UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR
DE INGENIEROS DE TELECOMUNICACIÓN

CONTRIBUTION TO OPERATION SUPPORT SYSTEMS AND SERVICE MANAGEMENT ARCHITECTURES FOR USER-CENTRIC TELECOMMUNICATIONS SERVICES OVER NEXT GENERATION NETWORKS

TESIS DOCTORAL

JOSÉ MARÍA DEL ÁLAMO RAMIRO
Ingeniero de Telecomunicación
2009

DEPARTAMENTO DE INGENIERÍA DE SISTEMAS TELEMÁTICOS

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN

UNIVERSIDAD POLITÉCNICA DE MADRID

CONTRIBUTION TO OPERATION SUPPORT SYSTEMS AND SERVICE MANAGEMENT ARCHITECTURES FOR USER-CENTRIC TELECOMMUNICATIONS SERVICES OVER NEXT GENERATION NETWORKS

AUTOR: JOSÉ MARÍA DEL ÁLAMO RAMIRO
Ingeniero de Telecomunicación

DIRECTOR: JUAN CARLOS YELMO GARCÍA
Doctor Ingeniero de Telecomunicación

2009

Tribunal nombrado por el Magfco. y Excmo. Sr. Rector de la Universidad Politécnica de Madrid, el día 5 de junio de 2009.

Presidente: D. Gonzalo León Serrano

Vocal: D. Carlos Delgado Kloos

Vocal: D. Juan Ramón Velasco Pérez

Vocal: D. Paolo Falcarin

Secretario: D. Victor Abraham Villagrá González

Suplente: D. Carlos García Rubio

Suplente: Dña. María Teresa Ariza Gómez

Realizado el acto de defensa y lectura de la Tesis el día 19 de junio de 2009 en la E.T.S.I.T. habiendo obtenido la calificación de _____

EL PRESIDENTE LOS VOCALES

EL SECRETARIO

Agradecimientos

Llegado este momento, siempre es difícil agradecer su trabajo, compañía y ánimo a tod@s aquell@s que en algún momento de esta trayectoria han aportado su granito de arena. Sois tantos, y en tanta medida, que no encuentro las palabras para expresar mi más sincero agradecimiento por vuestro apoyo.

En primer lugar, quiero agradecer a mi director de tesis, Juan Carlos Yelmo, su trabajo y enseñanzas en todos estos años. Sin tu ayuda y dirección todo esto no hubiera sido posible. Gracias por darme la oportunidad de participar en este gran proyecto y permitirme aprender tantas cosas.

También me gustaría recordar a los compañeros del laboratorio C-215, donde tanto tiempo hemos pasado juntos. Mucha gente ha ido y venido, pero cada uno ha dejado su huella: Agustín, Alex, Álvaro, Antonio, Arciniegas, Bea (la chica *accesible)*, Bea, Boni, Cristina, Dani, Félix, Freakant, Hugo, Jorge, Jose, Jose Luis, Juan, Juan Carlos, Lo, Lorena, Manu, Marco, Marta, Paquito, Rodrigo, Rodrigo Cerón y Sandra. También quisiera acordarme de los compañeros de comida y partidas de Go-Stop, Jose y Leti. Gracias a tod@s.

Me gustaría mencionar de forma especial a aquellos que me han acompañado desde el principio, y que por ello tengo más presentes en este momento. A HugoX, gestor de nuestros fondos de capital-riesgo – tus negocios un día nos sacarán a todos de pobres. A July, esa brujilla que pone la alegría y juventud en el grupo. A Samuel, el chico *accesible*, por sus explicaciones de unos cuantos miniYods[1] que nos acercan cada día el conocimiento de la WikiSamu. Y a Rubén: Empezamos a la par esta aventura del doctorado y espero que continuemos codo con codo. Gracias por poner tu lado artístico a todo lo que hacemos.

Este trabajo tampoco hubiera sido posible sin la ayuda de mi familia, empezando por mis padres que siempre me han apoyado en todo lo que he hecho y que me han motivado para llegar hasta aquí. También a mi hermana y mis abuel@s, que siempre han creído en mí y me han arropado. Y a los buenos amigos: Aarón, Aitor, Beto, Boli, César, Chabo, Erica, Javi, Marta, Martita, Mónica, Noemi, Óscar, Pedre, y tod@s l@s demás. A tod@s, sinceramente, muchas gracias.

Y por último, a Arantxa, por su ánimo constante, sobre todo en los momentos difíciles. Sin tu alegría y motivación no lo hubiera conseguido. Gracias por estar siempre a mi lado.

Gracias a tod@s,

Chema

[1] Un Yod es la unidad de complejidad conceptual equivalente a una idea que se tarda en explicar 1 hora. Dada la magnitud de esta unidad de medida lo normal es usar el microYod (para Samuel usamos miniYods).

ABSTRACT

Supported by Next Generation Network realizations and by Service Oriented Architectures, the new IP-based ICT world is blurring the borders between the traditionally separated Internet and Telecommunications industries. This enables new competition to be introduced in the service creation and delivery domain, which was previously constrained to a selected set of operators' partners. To keep the pace with new entrants, telecom operators are introducing fresh paradigms that engage new actors in the value chain e.g. User-Generated Services. The so-called user-centric environments support the fast development and supply of innovative User-Generated Services by enabling non-technically skilled users to create, share, discover and enjoy their own designs. By involving users in the service conception process telcos aim to have customers environments revealed and come up with new unique ideas that fulfil users' latent needs and user-experience expectations. Additionally, these new paradigms may contribute to save development and marketing expenses, thus helping to increase the revenue per bit carried.

Although the benefits that user-centric service creation and delivery platforms bring to the Telecommunications domain are potentially enormous, there are many challenges that operators must solve first. To begin with, the business models that can be applied are not clear. Additionally, the fact that users are allowed to create their own services and drive their lifecycles pose great challenges to current operations and support systems. On top of that, user-centric services are expected to intensively make use of end-users personal information, which may arise many concerns regarding privacy and personal information protection.

This dissertation has met these challenges by proposing a set of original contributions that may help to solve the detected problems. First, the author has proposed a business model that describes the actors and relationships involved. In addition, a study has been carried out that assesses the potential target groups and that analyzes the value network and the revenue generation mechanisms. The business context description for user-centric platforms has been complemented with an explanation of the technological fundamentals.

Going deeper into technical details, the author has focused on the operation and management of user-centric service creation and delivery platforms. Traditional support systems do not consider the customer involvement in the services management, and thus a review of the business processes involved has been conducted following the TeleManagement Forum Next Generation Operations Systems and Software framework. As a result, an architecture for the management and operation of user-centric platforms has been proposed. The proposal includes several original contributions, among which we have focused on the information model that describes User-Generated Services and supports their management and operation, and the privacy infrastructure that allows users to govern and decide on the use and release of their identity information.

The original contributions have been validated in several prototypes developed during Master Thesis that the author has tutored or has collaborated with. Furthermore, validation has been possible also within national and international research projects the author has been involved in.

In addition, the original contributions have been used to provide further research and scientific results by means of publications in relevant journals and conferences. Some of the results of this dissertation have been also awarded after submission to different conferences and prizes. The contributions have also provided industrial results by means of an international patent application and contributions submitted to first class telecom-oriented standard development organizations.

RESUMEN

El incipiente despliegue de Redes de Próxima Generación que exponen sus capacidades de red siguiendo enfoques de Arquitecturas Orientadas a Servicios, junto con la regulación que libera el negocio de la provisión de servicios de telecomunicaciones, hace posible que las fronteras entre las redes de telecomunicación e Internet se difuminen hasta prácticamente desaparecer. Esto permite a nuevos actores competir libremente por la provisión de servicios convergentes, hasta ese momento limitada a un conjunto reducido de proveedores que firmaban complejos acuerdos de negocio con los operadores.

La creciente competencia está provocando que los operadores busquen a su vez nuevos modelos para la creación y provisión de servicios que les permitan ahorrar costes a la vez que incrementar el valor de los bits que transportan. Uno de estos modelos propone facilitar a los usuarios (no expertos) las herramientas para crear sus propios servicios convergentes, que después podrán compartir con otra gente. Las denominadas *plataformas de servicios centrados en los usuarios* apoyan de esta forma el rápido desarrollo y provisión de servicios generados por los propios usuarios. Dado que los usuarios participan en el proceso de concepción del servicio es más sencillo conocer sus necesidades exactas, a la vez que se dispone de una inteligencia colectiva (y muchas veces gratuita) que permite elaborar nuevas ideas únicas que cumplen con las expectativas de los usuarios. Además, estos nuevos modelos pueden contribuir a ahorrar gastos en el desarrollo y comercialización de servicios, contribuyendo al mismo tiempo a aumentar los ingresos por consumo de servicios y tráfico cursado.

Aunque los beneficios que las plataformas para la creación y provisión de servicios centrados en el usuario pueden proporcionar son potencialmente enormes, quedan todavía muchos desafíos por resolver. Para empezar, los modelos de negocios que se pueden aplicar no están claros. Además, el hecho de que los usuarios puedan crear sus propios servicios y manejar sus ciclos de vida plantea grandes retos para los actuales sistemas de soporte a la operación. A todo esto hay que añadir que una característica de los servicios centrados en el usuario es que hacen un uso intensivo de la información personal de los usuarios finales. Por tanto, habrá que proporcionar los mecanismos adecuados para salvaguardar la privacidad de la información personal de los usuarios finales.

Esta tesis doctoral ha abordado estos desafíos, proponiendo un conjunto de contribuciones originales que pueden ayudar a resolver los problemas detectados. En primer lugar, se ha elaborado una propuesta de modelo de negocio que describe los actores involucrados y sus relaciones. También se ha llevado a cabo una evaluación de los segmentos de mercado para este tipo de plataformas, y de los mecanismos de generación de ingresos que pueden contribuir a incrementar su valor. Adicionalmente, se han descrito los fundamentos tecnológicos que dan soporte a las plataformas de servicios centradas en los usuarios sobre redes de próxima generación.

Las contribuciones han profundizado en los aspectos técnicos, centrándose en los mecanismos necesarios para la operación y gestión de los servicios centrados en el usuario. Dado que los sistemas de soporte a la operación tradicionales no consideran la participación del cliente en la gestión de los servicios de telecomunicaciones se han revisado los procesos de negocio involucrados siguiendo el marco de trabajo propuesto por el TeleManagement Forum. Como resultado, se ha elaborado una propuesta de

arquitectura para la gestión y operación de las plataformas de servicios centrados en el usuario. Esta propuesta incluye varias contribuciones originales, entre las que destacan un modelo de información para la descripción flexible de los servicios y recursos de cara a su gestión dinámica y automática por parte de la plataforma, y una infraestructura para la gestión de la privacidad por parte de los propios usuarios que les permite controlar y decidir sobre la utilización de su información de identidad.

Las contribuciones originales han sido validadas en varios prototipos desarrollados en el marco de diversos proyectos fin de carrera que el autor ha tutelado o en los que colaborado. Además, se ha realizado una validación más extensa en proyectos de investigación de ámbito nacional e internacional en los que el autor ha participado.

Por último, las contribuciones originales se han utilizado para producir resultados científicos por medio de publicaciones en revistas indexadas y conferencias con índice de impacto científico. Cabe destacar que algunos de estos resultados han sido galardonados después de ser presentados a diferentes conferencias y premios. Las contribuciones también han proporcionado resultados industriales por medio de una solicitud de patente internacional en la Oficina Europea de Patentes y contribuciones a estándares de ámbito internacional.

Table of Contents

List of Figures

List of Tables

List of Acronyms

3G	3rd Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
AAPML	Attribute Authority Policy Markup Language
ACF	Autonomic Communications Forum
ACL	Access Control List
API	Application Programming Interface
APPEL	A P3P Preference Exchange Language
ARPU	Average Revenue Per User
AS	Application Server
ATIS	Alliance for Telecommunication Industry Solutions
B2B	Business-to-Business
B2C	Business-to-Consumer
BGCF	Border Gateway Control Function
BLA	Business Level Agreement
BMF	Business Mashup Framework
BPEL	Business Process Execution Language
BPM	Business Process Management
BSS	Business Support Systems
BT	British Telecom
C2C	Consumer-to-Consumer
CA	Certification Authority
CAMEL	Customised Applications for Mobile network Enhanced Logic
CAMEL SCP	CAMEL Service Control Points
CARML	Client Attribute Requirement Markup Language
CDMA	Code Division Multiple Access
CIM	Common Information Model
CN	Core Network
CORE	Computing and Research Education
CoT	Circle of Trust
CRM	Customer Relationship Management
CRM	Customer Relationship Management
CSCF	Call/Session Control Function
DIT	Departmento de Ingeniería de Sistemas Telemáticos
DMTF	Distributed Management Task Force
DS	Discovery Service
DST	Data Service Template
EPO	European Patent Office
EPR	Endpoint Reference
ESB	Enterprise Service Bus
eTOM	enhanced Telecom Operations Map
ETSI	European Telecommunications Standards Institute
EU	European Union
FIA	Future Internet Assembly

FIDIS	Future of Identity in the Information Society
FP6	6th Framework Programme
FP7	7th Framework Programme
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSMA	GSM Association
GUI	Graphical User Interface
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
I-CSCF	Interrogating CSCF
ICT	Information and Communication Technology
IDE	Integrated Development Environment
ID-FF	Identity Federation Framework
IdP	Identity Provider
ID-SIS	Identity Services Interface Specifications
ID-WSF	Identity Web Services Framework
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFIP	International Federation for Information Processing
IGF	Identity Governance Framework
IM CN	IP Multimedia Core Network
IMS	IP Multimedia Subsystem
IM-SSF	IP Multimedia Serving Switching Function
IN	Intelligent Network
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Networks
IPR	Intellectual Property Rights
IPSF	IPsphere Forum
IS	Interaction Service
ISDN	Integrated Services Digital Network
ISI WoK	Information Science Institute Web of Knowledge
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
JRG-NGN	Joint Rapporteur Group for Next Generation Networks
JSLEE	JAIN Service Logic Execution Environment
MGCF	Media Gateway Control Function
MGW	Media Gateway
MMS	Multimedia Messaging Service
MRF	Media Resource Function
MVNO	Mobile Virtual Network Operator
NAI	New Applications for Internet
NESSI	Networked European Software and Services Initiative
NGN	Next Generation Network
NGN-GSI	NGN Global Standards Initiative
NGOSS	Next Generation Operations Systems and Software

NGSON	Next Generation Service Overlay Network
OMA	Open Mobile Alliance
OPEX	Operational Expenditure
OPUCE	Open Platform for User-Centric Service Creation and Execution
OSA	Open Services Architecture
OSA-SCS	OSA Service Capability Server
OSE	OMA Service Environment
OSI	Open Systems Interconnection
OSPE	OMA Service Provider Environment
OSS	Operations Support Systems
P3P	Platform for Privacy Preferences Project
P-CSCF	Proxy CSCF
PCT	Patent Cooperation Treaty
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PET	Privacy Enhancing Technology
PII	Personal Identifiable Information
PIN	Personal Identification Number
PM	Privacy Manager
PR	Policy Repository
PRIME	Privacy and Identity Management for Europe
PRM	Partner Relationship Management
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RSA	Revenue Sharing Agreement
RSS	Really Simple Syndication
SAML	Security Assertion Markup Language
S-CSCF	Serving CSCF
SDF	Service Delivery Framework
SDK	Software Development Kit
SDP	Service Delivery Platform
SDP	Service Delivery Platform
SDPA	SDP Alliance
SeCSE	Service Centric System Engineering
SEE	Service Execution Environment
SID	Shared Information Model
SID	Shared Information/Data Model
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLEE	Service Logic Execution Environment
SLO	Single Logout
SMAC	Service Model and Catalogue
SMS	Short Message Service
SOA	Service Oriented Architecture
SP	Service Provider
SPML	Service Provisioning Markup Language
SRM	Supplier Relationship Manager

SSO	Single Sign On
TINA-C	Telecommunication Information Networking Architecture Consortium
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TMF	TeleManagement Forum
TMN	Telecommunications Management Network
UE	User Equipment
UGC	User-Generated Content
UGS	User-Generated Service
UMTS	Universal Mobile Telecommunications System
UPM	Universidad Politécnica de Madrid
URI	Uniform Resource Identifiers
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USA	United States of America
W3C	World Wide Web Consortium
WLAN	Wireless Local Access Network
WSC	Web Service Identity Consumer
WSDL	Web Services Description Language
WSDM	Web Services Distributed Management
WSP	Web Service Identity Provider
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XPDL	XML Process Definition Language

1 INTRODUCTION

During the last few years there has been a convergence process in the Telecommunications industry. Three main axes have driven this process: device convergence, multimedia convergence and network convergence. Devices have converged in the sense that now we can use a single device to do the things for what we needed different devices in the past e.g. television, computer, telephone, etc. Multimedia has converged in a way so that we can have voice, data and video in a single service.

Finally, networks have converged around the Internet Protocol (IP) so that nowadays there is a common IP core network with multiple access networks. Next Generation Network (NGN) is the term used to refer to these new IP-based network architectures. They provide multiple broadband, Quality of Service (QoS)-enabled transport technologies and separation between service-related functions and the underlying transport technologies.

This new IP and multimedia world has blurred the border between the Internet and Telecommunications domains. This has allowed new competition to be introduced into the telecom service provision business. Mobile virtual network operators (MVNO) or Internet companies threaten now the traditional business models of Telecommunications operators by providing their services directly to the operators' customers.

End-users are also placing pressure on telcos by pushing for innovative and attractive value-added IP services which include new applications, other than just browsing on the mobile. These new services increasingly need to be delivered in shorter time-frames and for shorter lifetimes. On the other hand, this new source of revenue may help telecom operators to improve their now-stalled average revenue per user (ARPU).

NGN architectures can help in this new landscape of innovation and competitiveness by simplifying and speeding up the creation and deployment of new service delivery platforms (SDP). SDPs link the different stakeholders in the provision process (service providers, consumers, and the operator itself), and allow operators to open up their telecom networks to collaboration. Therefore operators and their partners can create an assorted portfolio of convergent services, reducing the time-to-market, and fulfilling some of the end-users requirements. By playing such a role, the operator becomes again the central entity in the service provision process and not just a bit-pipe.

However, it is clear now that there is not a unique killer application but that it is a better approach to develop as many small and good ideas as possible to address the long tail of users with their specific needs and preferences. Opening up network capabilities just to a close set of professional developers constrains this approach though.

On the other hand, some advanced models come about initially on the Internet allows end-users to define new contents and applications (mashups) using open services and interfaces that could be quickly and easily built and deployed. User-Generated Contents and User-Generated Services platforms enable end-users (not necessarily the very technically skilled) to create their own contents and services and manage the lifecycle of those services autonomously. It also allows users to share these services within a community which will promote the most interesting ones at a minimum cost. This approach not only saves development costs, but it also reduces marketing expenses.

The importance of User-Generated Contents, and of User-Generated Services as a follow up, has been highlighted as a key emerging usage trend in the ICT domain during the latest European ICT event 2008 held in Lyon in November 2008 [ICT08].

Nevertheless, to take advantage of the user-centric model operators still have to address the challenges associated with creating and managing user-defined products, capturing and handling orders for them, managing the provisioning of underlying services, opening and sharing the owned resources, managing the relationships with their partners, enabling subscribers to administer relevant service parameters and settings, coping with the legal requirements for the collection, maintenance and processing of customers' personal information, and so on and so forth. Furthermore, the expected increase in the number, complexity and specialization of services pose even greater challenges.

In order to support the aforementioned approach, it has become imperative for telcos to change their rigid business and provisioning models, replacing them with much more agile processes. This could be accomplished by identifying the operators' assets that can be provided only in the core network such as end-user location and presence information, and then abstract and offer them through well defined interfaces. Users may use these resources to create new or personalized services, thus generating a powerful and self-increasing ecosystem around the telecom operators' core business - their networks.

However, nowadays there is a lack in the state of the art about how the operators could manage this new situation, and which are the tools and technologies that might help them in this process. The business models to apply in this new situation are not clear either. It is also worth noting that relevant services will need personal information of end-users to better fit their needs. However, poor attention has been paid to this issue even though national and European regulation explicitly obliges service providers to protect users' privacy.

This dissertation aims to cover these detected gaps proposing a set of methodologies and techniques, as well as business and reference models that may help Telecommunications operators to open up their networks in order to create a secure, dynamic and trusted user-centric service ecosystem. Much of the challenge arises from the introduction of new business models and the effective operational delivery of those services, which in turn is highly dependant on flexible and efficient Operations Support Systems (OSS) and management processes. This dissertation focuses on these later management concerns rather than the networking aspects.

1.1 Research methodology

Service delivery platforms in general, and user-centric ones in particular, are becoming a hot research topic in the Telecommunications domain. New entrants coming from the Internet bring disruptive business models and innovative paradigms that put higher pressure on telcos, especially when it comes to the management and operation of user-generated services. New service creation and delivery models compel operators to review their traditional operation and management processes since new actors are involved, the lifetime for new services is shortened, and the amount of services is increasingly higher.

The work carried out in the OPUCE project, a research project within the European Union Sixth Framework Programme for Research and Technology Development, was crucial for identifying these challenges. In particular the author participation in the

OPUCE Work Package 3, which studied the service lifecycle management in user-centric platforms, was very useful to detect major drawbacks of current solutions and to point towards areas for improvement.

In addition, the validation of a prototype of user-centric platform, which was coordinated by the author as leader of the OPUCE task 5.3, revealed that several requirements regarding the management and operation systems were not fulfilled either by OPUCE or the reviewed state of the practice. For example, privacy and identity management in user-centric platforms were not usually considered, even though the necessity of it was generally recognised and required by European legislation. That is how the requirement for a privacy management infrastructure in user-centric platforms came up.

Once problems and goals were identified next step was trying to find already existing solutions. The aim of this search was finding suitable methodologies and frameworks that provide a solution to fulfil the requirements set. A preliminary conclusion of this search was that user-centric platforms were really scarce, not to mention information about their operations and management systems. Therefore, we had to go to domains close to this such as the service delivery platforms and its management and operations systems. After evaluating different alternatives the TeleManagement Forum initiative Next Generation Operations Systems and Software [TMF-GB930] was selected as the best approach to follow for the definition of a management and operations environment for user-centric platforms. Additionally, the Service Delivery Framework initiative [TMF-TR139a] and the Open Mobile Alliance Service Environment [OMA-OSE] were particularly useful regarding service processes. None of these initiatives provide a holistic solution for the challenges faced by this dissertation. Most of them do not provide explicit means for inter-domain privacy management, and none considers user-centricity of services. As a result they provide a good starting point but there is still room for improvement.

After the related work research, the description of the context surrounding user-centric platforms was investigated. In particular the business and the technological contexts were described. Firstly current business models were assessed and then a proposal for a business model for user-centric service creation and delivery platforms was elaborated. This proposal was presented by the author in the Third International Summer School organized by the PRIMELife project and the IFIP WG 9.2, 9.6/11.7, 11.6 in cooperation with FIDIS Network of Excellence and HumanIT. Experts in the field provided comments and suggestions, which helped to improve the proposal.

The work conducted by the author in OPUCE Work Package 3 provided the ground for the overall picture of a management and operations environment in user-centric platforms. Further investigation was required to provide the whole description of the different business processes involved in services and resources lifecycle. The result was the proposal of a reference architecture for the management and operation on user-centric platforms over Next Generation Networks.

At the same time, the work carried out in OPUCE task 3.1 provided the knowledge and requirements for the service and resource specification. From this initial information a complete information model to describe services and resources that supports the whole end-to-end lifecycle was elaborated. The proposal was further refined after comments and feedback from OPUCE partners as well as its submission as a contribution to the specification of the Open Mobile Alliance Service Provider Environment architecture.

Finally, a first draft to the contributions on the privacy management infrastructure was made up during the author attendance to the aforementioned IFIP/FIDIS Summer School. This initial work evolved and has led to the elaboration of a proposal of management infrastructure and different mechanisms for privacy control and identity protection in user-centric platforms. The development of this infrastructure was partially framed in the context of the CENIT SEGUR@ project, which has allowed the author to gather feedback from experts in the field. This information has been used to further improve the original contribution.

To conclude this section it must be highlighted that the author has followed a research methodology that provides an European dimension to the work conducted. This European dimension is firstly demonstrated by the alignment of the dissertation goals with those of the European Strategic Research Agendas and Priorities (see section 2.2). Additionally, the author has elaborated part of his original contributions in the context of the OPUCE project. Moreover, the doctorate was prepared, in part, during a stay of three months in the *Dipartamento di Automatica e Information* belonging to the *Politecnico di Torino*, in Italy. In addition, the candidate has participated in two different pan-European Summer Schools. On top of that, some of the original contributions have been disseminated within European and International institutions, such as the ITU-T, IEEE, IFIP and OMA. All this together has provided to the author a wide European scientific context and has internationalised his work, which is the main reason for the author to apply for the *Doctor Europeus Mention.*

1.2 Structure of this document

After introducing the motivation and context of the research work the document follows with a more detailed description of the objectives of this research work. The objectives are compared to European strategic research agendas and priorities regarding service engineering to check their allignment.

Then, chapter 3 focuses on the state of the art of the different technologies and solutions supporting the results of this dissertation as well as the state of the practice. In order to get a complete perspective we will cover different aspects. First, an overview on the status of Next Generation Networks and its realization as the IP Multimedia Subsystem will be given. Then, the fundamentals of Service Oriented Architecture and its use in Telecommunications are explained. After that, an overview of current and new service creation and delivery models is provided, including those related to User-Generated Contents and User-Generated Services. Additionally, most relevant standards regarding service management and operation in Telecommunications, as well as software and equipment vendors' solutions, will be covered. The state of the practice section finishes with a critique analysis of the state of the art of identity and privacy management, and its appliance to user-centric platforms. For each group of technologies, an analysis has been done to highlight shortcomings regarding the management and operation of user-centric service creation and delivery platforms.

Chapter 4 covers the fundamentals of user-centric platforms providing details on both the business and technical basis.

Chapter 5 is dedicated to the description of the management and operations reference architecture. The main entities of the model are introduced, their responsibilities are described and an explanation is given on how they interact with each other during the different lifecycle process affected by the user-centricity of services.

Chapter 6 further details the information model that is proposed to support the different aspects that the management and operation of services and resources in a user-centric platform may require. Information about how this model has been validated is provided.

Chapter 7 finalizes the description of the original contributions by thoroughly explaining the architecture and mechanisms proposed to manage the privacy in user-centric platforms.

Although the validations efforts have been included in each chapter as needed, chapter 8 provides an extended summary of all the validation activities. Additionally, it gives an idea of the research impact of the contributions of this dissertation, by describing the different papers and communications to conferences that the author has carried out. The industrial impact is also depicted by enumerating the author's contributions to standardization bodies and a PCT[2] application that has been filed as a result of the dissertation.

The document finishes in chapter 9 with the conclusions of this work, a brief summary of the original contributions and a description of future research activities.

[2] PCT stands for Patent Cooperation Treaty. This international patent law treaty provides a unified procedure for filing patent applications to protect inventions in each of its Contracting States. A patent application filed under the PCT is called an international application or PCT application.

2 OBJECTIVES

The overall objective that this thesis proposes is to investigate and improve the current processes and mechanisms that support the operation and management of advanced and innovative Telecommunications services over Next Generation Networks.

The outcome of the work to be done will facilitate the introduction of new technical and business models that are coming about in the Information and Communication Technologies (ICT) convergence process, i.e. the user-centric model, which places end-users as the generators and also consumers of their own contents and services.

These new paradigms pose great challenges to the management and operation of the network infrastructures due to the short lifetime of the services they provide and the increasingly amount of them. Furthermore, new relationships with partners, suppliers or third parties collaborating to provide end-users with services need to be efficiently addressed taking into account the right of the users to protect their privacy information.

2.1 Specific Objectives

The overall objective described in the previous point may be divided into the following set of specific objectives:

- To assess existing business models for service provision in the Telecommunications domain and their feasibility for user-centric service delivery platforms over next generation networks. Should not the previous business models be feasible, new business models will be proposed and described.
- To analyze the challenges and potential problems that new user-centric service delivery platforms and their business models pose regarding operations support systems and service management over next generation networks. Should some entities and functions be affected, then new solutions or improvements will be proposed and described.
- To analyze the risks that user-centric platforms pose for end-users privacy and anonymity, and the protection of their digital identities. Innovative proposals will be done that contribute to solve the detected problems.
- To design an architecture and a set of tools that incorporate the results from the previous analysis and that contribute to solve the problems detected in the management and operation of user-centric services over next generation networks.
- To validate the results of this thesis with a working prototype.
- To contribute the results of this dissertation to national and international research projects as well as open source communities aligned with the context and objectives of this work.
- To disseminate the results of this thesis in relevant national and international conferences and workshops, as well as in international journals and magazines.

2.2 Objectives Alignment with European Strategic Research Agendas and Priorities

The major goal of a dissertation is to advance a new point of view resulting from a research work. However, to be truly useful the author considers that a dissertation must advance the research according to its surrounding context. In this sense, this section describes the strategic research agendas and priorities related to the objectives of this work at national (Spain) and European levels.

2.2.1 Spanish National Plan for R+D+i

The Spanish ministry for Education and Sciences (Ministerio de Educación y Ciencia) has launched a new National Plan for Research, Development and Innovation (Plan Nacional I+D+i) [PLANI+D] for the period 2008-2011. The plan focuses on five strategic areas which include Health, Biotechnology, Energy, Telecommunications and Information Society, and Nanotechnology.

The goals of the Telecommunications and Information Society strategic area are the proper development and use of technologies, applications, services and content of the Information Society to contribute to the success of a model of economic growth based on increased competitiveness and productivity, to promote social and regional equality, the universal access to service and the improvement of welfare and quality of life of citizens.

Some of the specific topics that this strategic area addresses are:

- ***Information Technologies***, which include software engineering and service management.
- ***Telecommunications services***, systems and equipments, which include mobile networks, converged services, next generation network architectures, etc.
- ***Technologies for privacy and security***, which include digital identity, identity management, and privacy and data protection.

2.2.2 European Union 7th Framework Programme

The 7th Framework Programme for Research and Technological Development (FP7) [FP7] aims at strengthening the scientific and technological base of European industry and at encouraging its international competitiveness, while promoting research that supports EU policies. It will last for seven years from 2007 until 2013. There are five Specific Programmes within FP7, which constitute the major building blocks of FP7. The Information and Communications Technologies area is the most aligned with the objectives of this work.

The ICT Work Programme under FP7 is divided into seven Challenges of strategic interest to European society, plus research into *Future and emerging technologies* and support for horizontal actions, such as international cooperation. The Challenge that better fits the objectives of this dissertation is the number 1, *Pervasive and trusted network and service infrastructures*. It focuses on:

- New generations of software and service technologies that will allow ***services to be dynamically configured***, ***composed*** of ad-hoc coalitions of resources, dependable and reliable, and graceful in ***handling underlying complexities***.

- Architectures and solutions for ***integrated and interoperable organisations*** and enterprises.
- Complete user control over personal data and ***digital identity***, accompanied by strict protection of ***user privacy.***

2.2.3 Networked European Software and Services Initiative

The Networked European Software and Services Initiative (NESSI) [NESSI] aims to create a unified agenda, based on a multidisciplinary approach, for European research in Services and their foundations. This agenda defines and promotes the wide adoption of technologies, strategies and deployment policies fostering new, open, industrial solutions and societal applications that enhance the safety, security and well-being of citizens.

The research topics identified by NESSI that are aligned with the objectives of this work are:

- ***Service-oriented utility infrastructure***. The focus is to address the creation of new generation of infrastructures to provide all the capabilities needed for the dynamic management of the services distributed across the available resources. This research area includes the automation tools for IT service management.
- ***Service and system engineering***. Focus on dynamic composition, engineering automation, and management of complexity for both services and business processes. It includes topics on service management, service solution lifecycle management, and technology for networked and cooperating business ecosystem.
- ***Trust, security and dependability***. This area includes mechanisms and services to build end-to-end trust, security and dependability. In this context new business ecosystems shall be built respecting the basic democratic rights of modern societies such as privacy. It includes the deployment of Privacy Enhancing Technologies (PET), strong identity management, security mechanisms for services, trust management and assurance, etc.

2.2.4 European Future Internet Assembly

The European Future Internet Assembly (FIA) [FIA] is a forum for European industry and the research community to discuss and share ideas on Future Internet developments. It was launched in Bled, Slovenia, in March 2008, and since then has celebrated two meetings, the first one in Madrid in December 2008 and the latest one in Prague in May 2009.

One of the early results of the FIA was the Bled declaration, which described the challenges towards an European approach to the Future Internet. Among them, and aligned with the objectives of this dissertation, we can find:

- Create the conditions for the deployment of ***services and service oriented systems***;
- Communication through ***open standards*** for Future Internet technologies and architectures;
- Ensure the robustness and security of the networks, managing ***identities***, ***protecting privacy*** and creating trust in the on-line world;

- Design and develop capabilities for supporting the ***creation, sharing, locating and delivery of new-media content***.

3 STATE OF THE ART

Management and operation systems in Telecommunications have traditionally aimed at the service delivery at the network level (OSI stack layers 1 to 3) and the charging of the resources spent. However, as a result of the convergence process, Telecommunications service providers are moving up in the protocols layer opening up their networks to collaboration, applying new business and provision models, but also facing new competition and regulatory requirements. Thus also new problems are arising for the operations and support departments.

This chapter provides a twofold analysis of the state of the art. First, it aims to provide the reader with an overview of the different technologies, frameworks and architectures that support the contributions that this doctoral thesis proposes. Second, and even more important, it aims to clearly set the lacks and drawbacks of the current solutions that justify the original contributions that the following chapters detail.

With these goals, next section introduces the concept of Next Generation Network and provides an overview of its most common implementation, namely the IP Multimedia Subsystem. Then, the paradigm of Service Oriented Architecture is described focusing on the features that make it the choice to open up Telecommunications networks to collaboration and that enable the fast development of new services. After that, the chapter approaches the state of the art of service delivery in Telecommunications, introducing firstly the general concept of a Service Delivery Platform and moving on later to the latest and most successful paradigms enabling service creation and delivery over Next Generation Networks.

Since this doctoral thesis focuses on the management and operation of user-centric platforms a section is dedicated to this issue, analyzing the state of the art of service management in Telecommunications. For that, we first describe the initiatives within the main standard development organizations and compare them in terms of the features needed for a management and operations environment in a user-centric platform. Then, we also describe the related initiatives that leading software and equipment vendors are involved in.

One of the most important challenges that user-centric platform poses to the management and operation domain is related to the management and operation of users' personal information. The last section of this chapter focuses on this problem, and provides an overview of the processes related to identity management. The state of the art of both network- and user-centric identity management is described as well. To conclude, an overview of the European legislation that regulates the use and release of identity information is also provided.

3.1 Next Generation Networks

Telecom network architectures have evolved from the original Public Switched Telephone Network (PSTN), and nowadays several access and core networks coexist both in wireless and wired-line domains. The evolution process has been characterized first by the introduction of mobile technologies in the early 90ies, and the generalized access to the Internet later.

As a result of this process several kinds of access networks have been deployed. Nowadays they coexist and allow users to access to a huge set of Telecommunications services. Just to mention a few, there are fixed networks such as the aforesaid PSTN and

the Integrated Services Digital Network (ISDN), several radio networks such as the Global System for Mobile communications (GSM), the General Packet Radio Service (GPRS), the Universal Mobile Telecommunications System (UMTS) and the CDMA2000 networks (Code Division Multiple Access - CDMA), other wireless technologies such as Wi-Fi and WiMax, and so on. Core networks have also evolved from the original circuit switched networks to the packet switched networks.

At the beginning each network developed its own protocols with the aim of enhancing the previous ones. However, that means the coexistence of several network protocols that should communicate with each other, which produces both technological and business problems. Besides, each network followed a vertical approach where access entities, control systems and services where tightly coupled.

Some standardization organizations have begun to work on a convergence approach for Telecommunications networks, which has been named Next Generation Network (NGN). The work has been led by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Study Group 13 [ITU-T]. It has defined an NGN as "*A packet-based network able to provide telecommunication services and able to make use of multiple broadband, Quality of Service (QoS)-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users*" [Y.2001].

As stated in the Recommendation Y.2001, the fundamental characteristics of an NGN are:

- Packet-based transfer.
- Separation of control functions among bearer capabilities, call/session, and application/service.
- Decoupling of service provision from transport, and provision of open interfaces.
- Support for a wide range of services, applications and mechanisms based on service building blocks.
- Broadband capabilities with end-to-end QoS.
- Interworking with legacy networks using open interfaces.
- Generalized mobility.
- Unrestricted access by users to different service providers.
- A variety of identification schemes.
- Unified service characteristics for the same service as perceived by the user.
- Converged services between fixed/mobile.
- Independence of service-related functions from underlying transport technologies.
- Support of multiple last mile technologies.

- Compliance with all regulatory requirements, for example, concerning emergency communications, security, privacy, and lawful interception.

NGNs provide network operators with the possibility to share resources and infrastructure, facilitate the interoperability between networks, and simplify and unify the management, operation and maintenance of service offerings. In other words, a reduction of the expenses related to service management and operation.

And as for the end-users, NGNs allows for having services which were precluded to mobile networks due to signalling delays and latencies, low throughput, etc. Therefore, end-users can have now personal broadband mobile services at any time and any place and can begin to expect the flexibility, scope, and service variety they have experienced on the Web.

Next subsection provides the reader with an overview of the standardization status on NGN, the evolution of the ideas that surrounded it, and the future paths for standardization.

3.1.1 NGN standardization

In 1998 leading regional Telecommunications standard bodies agreed on create two 3rd Generation Partnership Projects (3GPP [3GPP] and 3GPP2 [3GPP2]) with the aim of evolving the circuit and voice based mobile networks into 3rd Generation (3G) multimedia packet-based mobile networks. The main result of these projects was the specification of the IP Multimedia Subsystem (IMS) which has been used as the cornerstone to support further NGN specifications.

IMS is an architectural framework for delivering IP multimedia services to end users. It was originally focused on evolving mobile networks beyond GSM and thus its original formulation (3GPP Release 5) represented an approach to delivering Internet services over GPRS. IMS is considered the first approach to the NGN concept.

Based on 3GPP/3GPP2 IMS, some other standardization bodies have worked around the idea of extending the NGN to both the wireless and wired-line domains. For example, in 2003 the ITU-T created a study group on NGN focused on advancing the specification. In 2004, the Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN) technical committee [TISPAN] of the European Telecommunications Standards Institute (ETSI) [ETSI] was created with the goal of standardizing an NGN for fixed network access, also based on IMS. At the same time in the United States of America, and again based on IMS, the Alliance for Telecommunication Industry Solutions (ATIS) [ATIS] created an NGN Focus Group to study the applicability of NGN to the USA fixed access networks.

To sum up, the initial approach to NGN of 3GPP IMS specification was subsequently updated by 3GPP itself, 3GPP2, TISPAN and ATIS by providing requirements for support of packet-based networks other than GPRS such as Wireless Local Access Networks (WLAN), CDMA2000 and fixed line. Finally, and due to concerns about possible overlaps, delays, and incompatibilities among future NGN standards, the ITU-T has coordinated the standardization process.

In order to do so, in 2003 a Joint Rapporteur Group for Next Generation Networks (JRG-NGN) was formed bringing together experts from ITU-T Study Group 13. JRP-NGN goals included to study NGN requirements, a general reference model, functional requirements and architecture of the NGN, and evolution to NGN. Its main results were two recommendations [Y.2001] and [Y.2011]. The former identifies a number of

characteristics considered necessary in an NGN and includes the definition for NGN; the latter provides a general framework for the architectural underpinnings required to obtain the basic characteristics.

To continue and accelerate NGN activities initiated by the JRG-NGN, ITU-T established a Focus Group on NGN in May 2004. This Focus Group addressed the urgent need for an initial suite of common, global standards for NGN, specifically concerning the following topics:

- NGN functional architecture.
- Generalized mobility.
- QoS.
- NGN control and signalling.
- Security capabilities, including authentication.
- Evolution from existing networks to NGN.

The main result of this group was the Focus Group NGN Release 1 [ITUT-ngn05] which includes contributions from ETSI TISPAN Release 1. It is a first step towards a comprehensive framework of services, capabilities and network functions that are considered to constitute an NGN (Figure 1). In fact, the concepts behind Release 1 are essentially the 3GPP IMS ones.

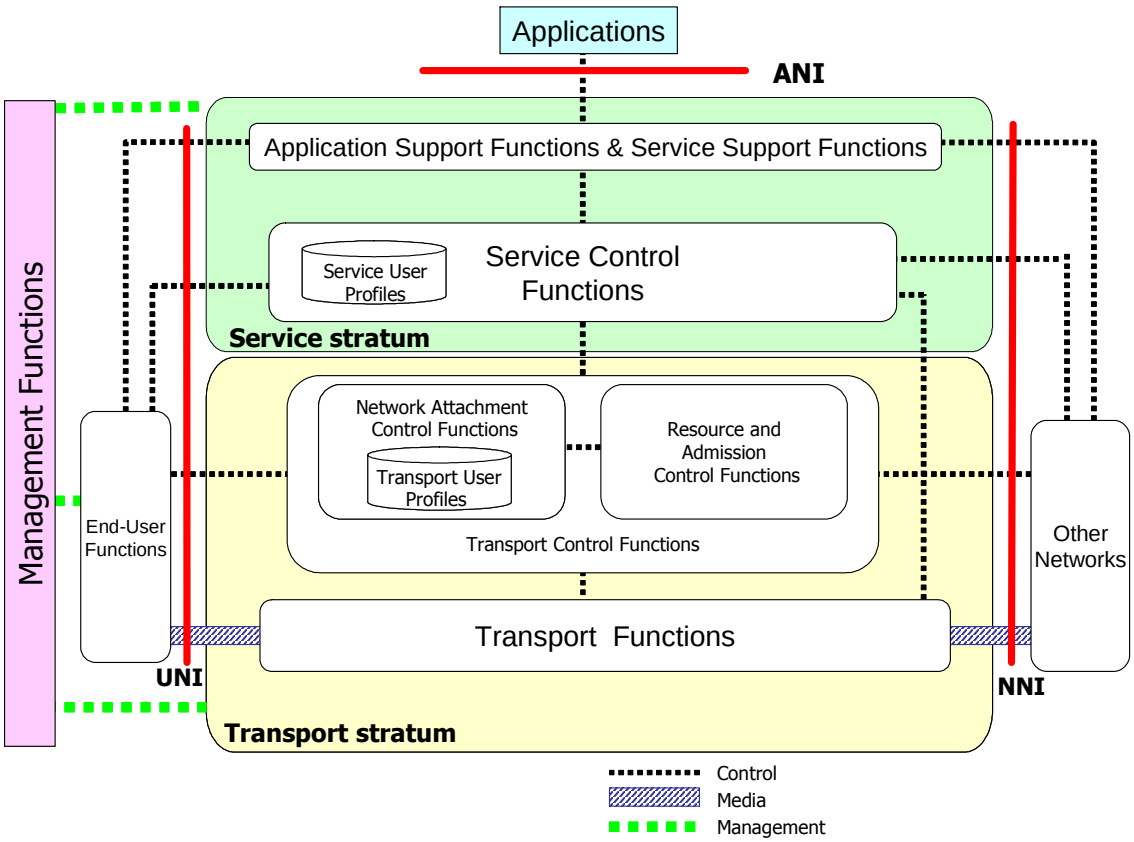

Figure 1 - ITU-T NGN Release 1 functional architecture [ITUT-ngn05].

ITU-T NGN Release 1 split the NGN functions into two strata, the service stratum and the transport stratum, and two set of functions, management functions and end-user functions. The transport stratum provides IP connectivity for all components and physically separated functions within the NGN such as end-users equipments outside

the NGN, and controllers and enablers that are located on servers inside the NGN. It also provides end-to-end QoS, which is a must for NGN as stated in [Y.2001].

Service stratum provides session-based and non session-based services, including subscribe/notify for presence information and a message method for instant message exchange. It also provides all the network functionality associated with existing PSTN/ISDN services and capabilities and interfaces to legacy customer equipment. The management functions enable the NGN operator to manage the network and provide NGN services with the expected quality, security, and reliability. It also includes charging and billing functions. End-user functions provide both physical and functional interfaces to the end users. End-user equipments could be either mobile or fixed. Further information on ITU-T NGN architecture can be found in [Knightson&05].

Eventually, as NGN was gaining momentum, and in order to encompass all the contributions that came from different ITU-T Study Groups, in 2006 the ITU-T created the NGN Global Standards Initiative (NGN-GSI). NGN-GSI focuses on developing the detailed standards necessary for NGN deployment to give service providers the means to offer the wide range of services expected in NGN. NGN-GSI harmonizes, in collaboration with other bodies, different approaches to NGN architecture worldwide.

3.1.2 The IP Multimedia Subsystem

IMS architecture [3GPP-ims] was first introduced by the 3GPP Release 5 and is being updated in onward releases. It defines a service provision architecture that can be seen as the Service Delivery Platform for NGN [Lee&05] because:

1. it provides access to services independent of the underlying connectivity network, and thus;
2. it has been incorporated by TISPAN and ITU-T into their NGN architecture. Moreover, the convergence of NGN Release 2 and 3GPP Release 7 is expected. Thus, there will be a unique IMS for the NGN (Although IMS specifications were initially developed for use with cellular networks, some extensions [Knightson&05] are expected to be made to the base IMS standards as part of future releases).

IMS is a collection of functions linked by standardized interfaces. It provides an abstraction layer above the underlying transport network technologies (transport layer). As long as the network access is provided via a suitable IP network, user equipments (UE) could access IMS.

Within IMS architecture, the transport layer could be split into IP-Connectivity Access Networks (IP-CAN) and Core Networks (CN):

- An IP-CAN is a collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities, e.g. GPRS.
- A CN is a collection of entities providing IP transport connectivity between an IP-CAN and another CN, between two IP-CANs, or between two other CNs. The CN also provides connectivity to service layer entities, such as IMS.

3GPP Release 8 states that the complete solution for the support of IP multimedia applications consists of UEs, IP-CANs, and the specific functional elements of the IP Multimedia Core Network (IM CN) subsystem (Figure 2). The IM CN subsystem comprises all CN elements for provision of multimedia services.

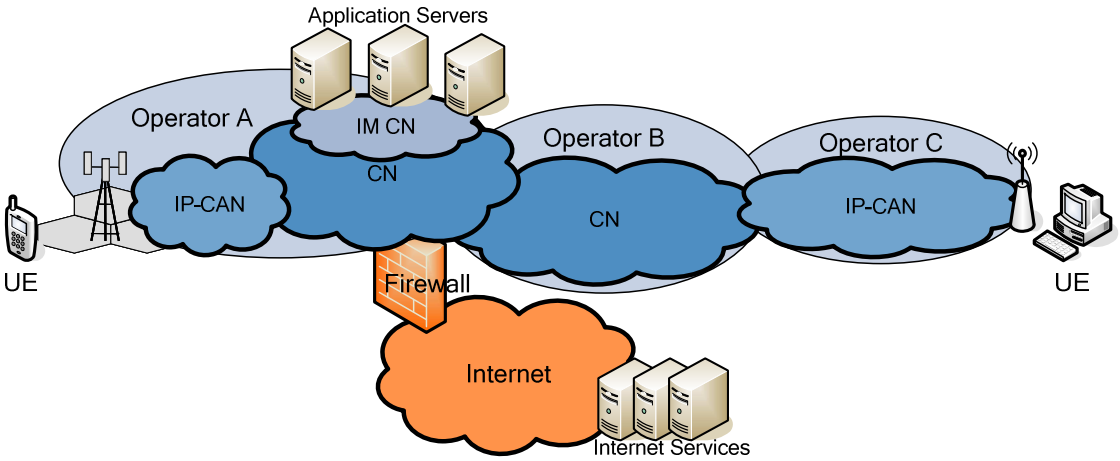

Figure 2 - IMS in a network partitioning.

IMS also supports the concept of a home and visited networks. The former is the CN supporting the IMS services that hold the IMS subscription. The latter is the network currently providing the users with connectivity to the IMS services.

3.1.2.1 IMS Architecture

Figure 3 shows a simplified vision of the IMS architecture. The dotted line has been used to represent the signalling flows. The full line is used to represent the media flows. It is important to notice that IMS deals just with the session signalling and control. It does not tackle with the actual transport of data or media flows of the sessions.

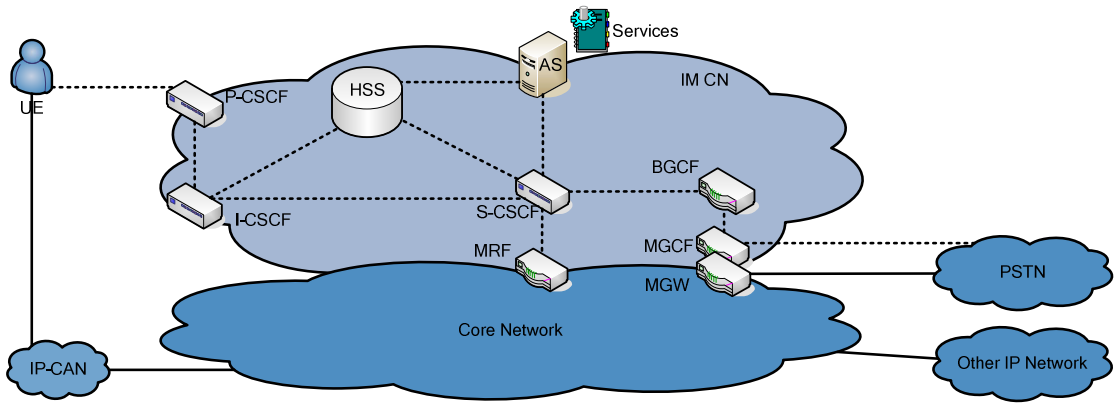

Figure 3 – IMS architecture.

There are three nodes of the IMS architecture that we are going to further discuss; the user database, the session control function, and the application servers.

The user-related information is stored in the Home Subscriber Server (HSS). It contains the user information required to handle multimedia sessions; i.e. location information, security information (authentication and authorization), user profile and subscribed services, and the session control function assigned to the user. Session control functions and application servers will be explained in next subsections.

The transport layer and the entities related to circuit-switched networks (Border Gateway Control Function – BGCF, Media Gateway Control Function – MGCF, and Media Gateway – MGW) are out of the scope of this document. We will not describe either the media-related functions such as the Media Resource Function (MRF). Further information about these and other IMS nodes can be obtained from IMS specifications,

some related specifications from 3GPP or from the specialized literature e.g. [Camarillo&06].

3.1.2.1.1 Session Control Function

The Session Initiation Protocol (SIP) [Rosemberg&02] has been chosen to control service sessions within IMS. SIP is a protocol specified by the Internet Engineering Task Force (IETF) [IETF] which allows establishing and managing multimedia sessions over IP networks. It is based on the Hypertext Transfer Protocol (HTTP) [Fielding&99], and thus it can be used in a similar way than this well-known Web protocol. For example SIP defines a set of methods e.g. ACK, BYE, INVITE, REGISTER, SUBSCRIBE, etc.

SIP specification defines three logical entities which participate in the communication (UEs, proxy and redirection servers, and SIP registrars), and a way to identify users, i.e. SIP Uniform Resource Identifiers (URI).

A SIP URI consists of a username followed by a domain name, e.g. sip:jmdela@midominio.es. SIP distinguishes between a public URI, the one used by other entities to contact me, and the URI used to reach me. The latter depends on where I am located at that moment, for example sip:686660776@mobile.company.com or sip:jmdela@cobi.dit.upm.es. A SIP registrar maps public URIs to the user's current location URIs. Every time I log in into a new location I must send a SIP REGISTER message to the registrar in my home domain. Thus, wherever I am, the registrar always knows how to forward incoming request to my public SIP URI.

IMS defines a Call/Session Control Function (CSCF), actually a SIP server, which processes all the SIP signalling. In fact, the CSCF is separated into three different entities depending on the role they take: the Proxy CSCF (P-CSCF), the Interrogating CSCF (I-CSCF), and the Serving CSCF (S-CSCF) (Figure 4).

The S-CSCF performs the session control services for the UEs and acts as a SIP registrar. It also knows the user's service profile and user's subscribed services (retrieved from the HSS). The SIP signalling from and to the UE goes through the S-CSCF and thus, whenever a SIP message contains triggering information for the subscribed services it routes that information to them. The S-CSCF is always located in the home network.

The I-CSCF is the contact point within an IMS home network from other networks. It knows user location and routes the received SIP requests to the S-CSCF serving the user. The I-CSCF also assigns an S-CSCF to the UE upon its initial registration.

The P-CSCF is the initial contact point within an IMS network (either visited or home) for a UE. It behaves like a proxy, i.e. it forwards registering requests from the UE to an I-CSCF in the home network, and then all subsequent SIP messages to the assigned S-CSCF. The P-CSCF also provides extra functionality such as checking and asserting users' identity, compressing and decompressing SIP messages, generating charging information, etc. Once a P-CSCF is assigned to a UE, it does not change for the duration of the UE registration.

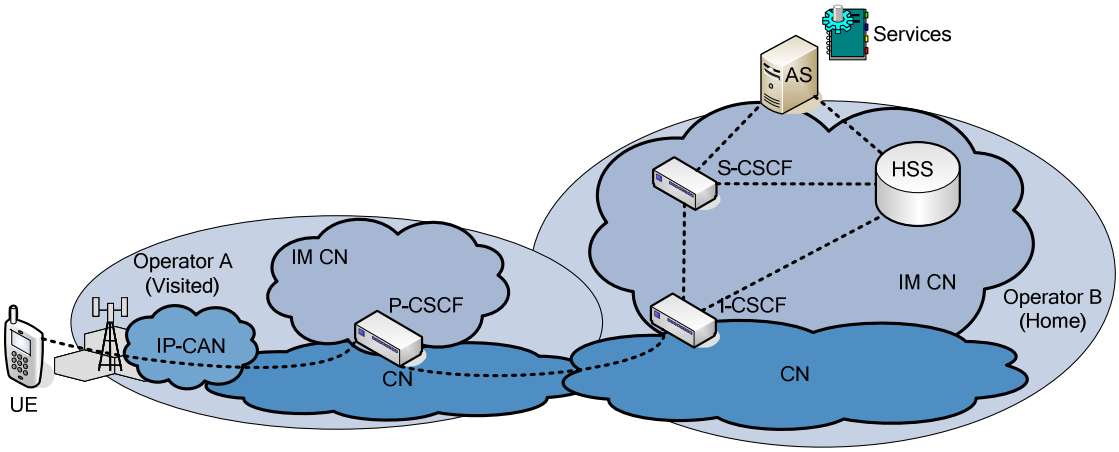

Figure 4 - Control session function roles in IMS home and visited networks.

3.1.2.1.2 Service provision

In IMS, services are hosted and executed within Application Servers (AS). There are three different types of AS (Figure 5):

- SIP AS. It hosts and executes SIP-based multimedia services.
- Open Services Architecture Service Capability Server (OSA-SCS). This kind of AS provides an interface to OSA AS. It also allows the access to the IMS from external networks via the OSA framework [OSA].
- IP Multimedia Serving Switching Function (IM-SSF). This kind of AS allows the reuse of CAMEL (Customised Applications for Mobile network Enhanced Logic) services via CAMEL Service Control Points (CAMEL SCP).

The AS may also interact with the HSS in order to obtain subscriber profile information as far as it is located within the home network. If it is located outside, e.g. in a third party provider network, it does not interface the HSS.

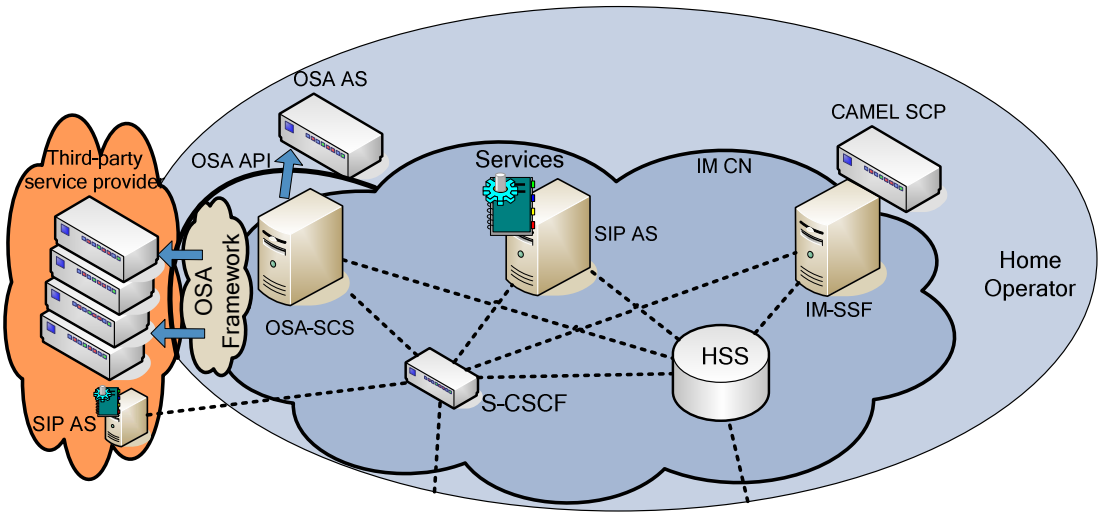

Figure 5 - Service provision in IMS.

As we have previously said, the S-CSCF performs the session control in IMS. To support the session control it first gathers the user profile from the HSS, which includes filter criteria that indicate the ASs providing service control for this user. During session establishment or modification the S-CSCF applies the filter criteria to involve ASs as needed in order to provide the services and features to which the user has subscribed.

The S-CSCF forwards SIP messages to each AS in the order established by the filter criteria. After the last AS is contacted, the SIP message is sent towards the intended destination. The filter criteria can be set on various service trigger points such as any SIP method, the presence or absence or any header, the direction of the request with respect to the served user, and so on.

3.1.3 Section summary and conclusions

This section has provided an overview on the evolution of the concept of Next Generation Network and the status of its standardization process. NGN proposes a layered architecture supporting the convergence of access networks around a packet-based core, decoupling the service provision from the transport and control functions. The IP Multimedia Subsystem specifies a service provision architecture that can be used to realize the NGN. This section has described the bases underpinning the IMS architecture and the entities and mechanisms that support the service creation and delivery over it.

NGN, and its realization as the IMS, is becoming the choice of Telecommunications operators to support the convergence process. Therefore, this dissertation assumes an underlying IMS architecture over which a user-centric service creation and delivery platform is built. However, to realize the idea of an open service creation platform the network resources must be offered to end-users to enable service creation and to third parties so that service delivery can be assured. Next sections provide details on how this can be achieved, describing the state of the art of Service Oriented Architecture and service creation and delivery in Telecommunications.

3.2 Service Oriented Architecture

As it has been described during the previous sections, there is an urgent need in the Telecommunications domain towards faster and cheaper service creation and delivery. These issues have already been faced in the Internet, and different mechanisms have been introduced to cope with them. From all the set of solutions that could be applied we focus within this section on Service Oriented Architecture (SOA) [Erl05] and Web services middleware [Chappell02].

SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains [MacKenzie&06]. These capabilities solve or support a solution for the needs that an entity or other collaborating face in the course of their businesses.

Services are the mechanism by which needs and capabilities are brought together. A service description contains the information necessary to interact with the service and describes this in such terms as the service inputs, outputs, and associated semantics. The service description also conveys what is accomplished when the service is invoked and the conditions for using the service.

In general, entities (people and organizations) offer capabilities and act as service providers. Those with needs who make use of services are referred to as service consumers. The service description allows prospective consumers to decide if the service is suitable for their current needs and establishes whether a consumer satisfies any requirements of the service provider.

The main drivers for SOA-based architectures are to facilitate the manageable growth of large scale enterprise systems, to facilitate huge-scale provisioning and use of services

and to reduce costs in organization to organization cooperation. Through this inherent ability to scale and evolve, SOA enables a service portfolio which is also adaptable to the different needs of specific problem domain or process architecture. The infrastructure SOA encourages is also more agile and responsive than one built on an exponential number of pair-wise interfaces. Therefore, SOA can provide a solid foundation for Telecommunications business agility and adaptability.

A Web services architecture is the most common way to implement an architecture according to SOA concepts. As described by the W3C *a Web service is a software system designed to support interoperable machine-to-machine interaction over a network* [W3C-WS]. There are many ways for a service consumer entity to engage and use a Web service. In general, the following broad steps are required:

1. the requester (consumer) and provider entities become known to each other (or at least one becomes known to the other);
2. the requester and provider entities somehow agree on the service description and semantics that will govern the interaction between the requester and provider agents;
3. the service description and semantics are realized by the requester and provider agents; and;
4. the requester and provider agents exchange messages, thus performing some task on behalf of the requester and provider entities.

Web service architecture involves many layered and interrelated technologies, but mainly XML [W3C-XML], SOAP [W3C-SOAP] and WSDL [W3C-WSDL]:

- Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behaviour of computer programs which process them. XML solves a key technology requirement that appears in many places: by offering a standard, flexible and inherently extensible data format, XML significantly reduces the burden of deploying the many technologies needed to ensure the success of Web services.
- SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It provides a standard, extensible, composable framework for packaging and exchanging XML messages. SOAP messages can be carried by a variety of network protocols; such as HTTP, SMTP, FTP, RMI/IIOP, or a proprietary messaging protocol.
- The Web Services Description Language (WSDL) is a language for describing Web services. WSDL describes Web services starting with the messages that are exchanged between the requester and provider agents. The messages themselves are described abstractly and then bound to a concrete network protocol and message format.

3.2.1 Service composition

Sometimes, the execution of a business process requires the composition (combination) of a set of lower-level independent building blocks. The logic of this process is defined by the invocations between the building blocks and how the data flow among them. The way those invocations are performed can be seen from two different points of view: orchestration and choreography [Peltz03]:

- Orchestration is defined as an executable business process that can interact with both internal and external services. Thus, orchestration refers to the definition of the business logic and the order of the execution of the required task during the execution of a service. It can be concluded that, in an orchestrated process, one party rules the execution of the process.
- Choreography follows a more collaborative approach, and it is each party of the process that describes its role in the service, tracking the sequence of messages among different parties, instead of a specific business process that a single party executes.

When it comes to modelling and describing business processes there are different alternatives. For example, the XML Process Definition Language (XPDL) [XPDL] allows for specifying the declarative part of a workflow or business process. However, the Business Process Execution Language (BPEL) [OASIS-BPEL] is the most successful and supported orchestration language for Web services. BPEL allows defining abstract processes, writing executable specifications of processes and executing the processes descriptions. Furthermore, it is widely supported by many products that allow creating and executing BPEL code.

Apart from the service logic an integrating layer is sometimes required, or at least desired, for the implementation and execution of these processes. For this, Business Process Management (BPM) and Enterprise Service Bus (ESB) [Rademakers&09] are used.

The activities that constitute BPM can be grouped into five categories: design, modeling, execution, monitoring, and optimization. BPM technologies provide the tools to design and implement business processes in such a way that the execution of the resulting software artifacts can be managed from a business process perspective. It also allows users to monitor the execution of individual processes, to analyze the overall behaviour of a set of business processes, to verify their successful performance, and to provide input for process optimization.

ESB provides technological solutions to intercept messages between Web services and to translate or route them to help the integration of business applications. An ESB is actually a middleware providing integration facilities built on top of industrial standards such as XML, SOAP, WSDL, an other WS-* specifications. Among other features, an ESB usually provides:

- A *transport service* that ensures the delivery of messages among the business process interconnected within the enterprise bus. It usually provides transactional, secure (e.g. cryptography and authorization) and managed capabilities.
- An *event service* that provides event detection, triggering, and distribution capabilities.
- Some *mediation services* that ensure the necessary protocol matching to integrate heterogeneous systems. In addition to transformation functionalities, mediation also includes the dynamic routing and dispatch of requests potentially to multiple receivers in order to perform load balancing or to respond to failure of a data source for instance. It also includes other non-functional actions related to QoS management such as incomplete data management, quality measurement, tracing, caching, or failure detection and recovery.

3.2.2 Applying SOA to Telecommunications networks

Telecommunications networks are evolving towards building-blocks-based architectures where lower-level reusable components can be easily and loosely composed into higher-level services [Jorstad&05]. The most widespread SOA technology, namely Web services, provides the features needed to support these new architectures and thus Web services is becoming a hot topic when it comes to apply SOA to Telecommunications networks [Pollet&06] [Griffin&07].

However, the efforts to realize the idea of a programmable and loosely-coupled Telecommunications network can be initially dated as early as the 1980s with the standardization of Intelligent Networks (IN) [Garraham&93]. IN is an architecture by which customized service logic programs can be created by a service provider for enhanced features on calls in the PSTN.

IN introduced a set of functional entities comprising the distributed functions that need to interact during call origination and call termination in the provision of IN call-related services, thus decoupling the service development from the network infrastructure. From that, the IN infrastructure has evolved to support some of the new features and requirements of the evolving networks. For instance CAMEL, which is the technology used in GSM networks to enable services such as roaming and international pre-paid, is based on IN [Zuidweg06].

However, IN is not able to fulfil some of the requirements that new converged networks impose such as shorter time to market of new services and the development of value-added, network independent services. To cover this gap IP-based NGN architectures such as the IMS have been specified. Initiatives such as the OSA/Parlay, OMA or the JAIN Service Logic Execution Environment (JAIN SLEE or JSLEE) [Boom&04] have also been developed in different contexts.

JSLEE defines a component model for structuring application logic of communications applications as a collection of reusable object-orientated components, and for composing these components into higher level, richer services. The specification also defines the contract between these components and the container that will host these components at runtime.

JAIN SLEE provides support for asynchronous applications supported by an event model. Application components receive events from event channels that are established at runtime. Network resource adapters create representations of calls and pass events generated by the calls to the SLEE. Application components are in turn invoked by the SLEE to process these events in a transactional context.

The specification of the OSA/Parlay [ETSI-OSA] is a joint effort between ETSI, 3GPP and The Parlay Group [PARLAY]. It is an open API for application access to telecom network resources. OSA/Parlay technology integrates telecom network capabilities with IT applications via a secure, measured, and billable interface. The APIs are network independent, and applications can be hosted within the telecom network operator's own environment, or by external third party service providers.

A Web services API is also available, known as Parlay X [ETSI-ParlayX]. This is also standardized jointly by ETSI, Parlay and the 3GPP. Parlay X is a simplified Web services interface to telecom network functionality. It may be used in conjunction with the base OSA/Parlay APIs, or on its own.

Within the mobile domain, OMA [OMA] is the focal point for the development of service enabler specifications. OMA does not deliver platform implementations, but it provides specifications of service enabling functionalities such as location, instant messaging and presence, device management, etc. It is left to others to implement the platforms and functionalities that they describe, specially using Web services technologies [OMA-OWSER].

Recently, a Telecommunications Service Member Section has been created at OASIS, named OASIS Telecom [OASIS-Telecom]. The goal of this new group is to bring the full advantages of SOA to the Telecommunications industry while solving its main pitfalls. This is expected to boost the convergence of Telecommunications networks and SOA, but results are not available yet.

Quite in the same line, the GSM Association (GSMA) [GSMA] supported by 10 global operators has launched an initiative called 3rd Party Access [GSMA-Access] which aims to identify and provide means for 3rd parties to more effectively and efficiently utilise operator network and service capabilities. 3rd parties in this context are Web content and service providers, namely Websites and client applications that access services over HTTP. The goal is to stimulate innovation; facilitate development and deployment; and increase portability between operators. The APIs define functionality for messaging, location, charging, data connection and user profile. This initiative will provide its first live implementations during 2009.

As it can be seen, several are the initiatives that have tried to provide the principles of a Service Oriented Architecture, being the latest the Web-services-oriented APIs. The use of a set of ubiquitous and open technologies gives Web services the capability of functioning over heterogeneous network, hardware, and software topologies. It must be said that this adaptability comes at a significant performance cost [Saiedian&08] as the data and communication protocols must be translated from compact proprietary formats to the often inefficient text-based standards used by Web services. Furthermore, Web services used in telecom networks have a number of constraints related to issues of trust when it comes to collaborating with third parties and other operators, as well as the protection of access to the network and to customer-identity resources [Yelmo&09a].

3.2.3 Section summary and conclusions

Service Oriented Architecture delivers the promise of enabling faster and cheaper service creation to the Telecommunications domain. By means of Web services technology network resources can be exposed as independent building-blocks (enablers) that can be combined with external resources provided by third parties collaborating. This section has described the bases underpinning SOA, service composition technologies and network resources exposure using Web services. This dissertation leverages on these areas in order to describe the fundamentals of user-centric service creation and delivery platforms over Next Generation Networks.

However, the application of Web services to the Telecommunications domain, and thus to the platforms that this dissertation focuses on, still have some constraints to be solved such as the protection of privacy when offering and releasing consumer-identity resources. Some of the original contributions of this dissertation points to that direction.

3.3 Service creation and delivery in Telecommunications

As a result of the convergence and deregulation processes in Telecommunications markets new competition has been introduced in the service delivery arena. Hence,

telcos are under increasing pressure to offer new and innovative service portfolios which fulfil customers' expectations and thus reduce churn.

New entrants coming from the Internet make this situation even worse, threatening traditional Telecommunications business models by providing their telecom-oriented services directly to end-users. As voice becomes just another application that can be delivered over an IP environment, the potential for new competition is enormous e.g. Jajah [JAJAH] or skype [SKYPE].

Recently, even traditional device manufacturers have launched their own initiatives for mobile devices that connect users with content and service providers. Nokia's Maemo platform [MAEMO] provides an operating system and a Software Development Kit (SDK) for the development of applications for Nokia devices; meanwhile Nokia Mosh [MOSH] supports the sharing of multimedia content between mobile users.

In response to the strong competition, telcos are evolving their service environments in order to offer a wider range of new value-added products faster and cost efficiently, and to collaborate with partners. In this sense NGN architectures, which provides an IP-based service infrastructure, enable easier deployment of new converged services that can be delivered over different access networks. Furthermore, the evolution of Telecommunications networks towards SOA approaches allows operators to open up their network resources to collaboration with third parties by means of reusable telecom services enablers.

These architectures simplify and speed up the creation and deployment of new service capabilities, using a component-based approach. Therefore operators and their partners can create an assorted portfolio of convergent services, reducing the time-to-market, and fulfilling some of the end-users requirements.

However, it is clear now that there is not a unique killer application but that it is a better approach to develop as many small and good ideas as possible, some of which may become mainstream thus increasing operators' revenue. Opening up network capabilities just to the professional developers constrains this approach though. On the other hand, the user-centric service creation paradigm set out on the Internet allows users to create and share new contents and applications.

This section describes the state of the art of the convergence process of open Telecommunications service platforms, IP-based NGN architectures and the new user-centric paradigms. With this aim we first provide an overview to the current status of Telecommunications service delivery platforms. Then we focus on the new paradigms that have come about on the Internet and how they are being applied to the Telecommunications area. To exemplify our description we analyze and compare several platforms that support some of the aforementioned ideas.

3.3.1 Service Delivery Platforms

The concept of Service Delivery Platform (SDP) has evolved over the past few years. Although there is no a single agreed definition for this term, it usually refers to a system architecture that enables the efficient creation, management, execution, and operation of one or more classes of services [HP-sdp07]. These systems have emerged as a consequence of telecom network evolution towards an all-IP solution, aiming at substituting numerous network-specific ‘stove-pipes’ with a common and horizontal service architecture.

Based on the definition given by the Moriana Group [MORIANA], we describe the common features for an SDP:

- An SDP provides a complete ecosystem for the rapid deployment, provisioning, execution, management and billing of value added services.
- An SDP supports the delivery of voice and data services and content in a way that is both network and device-independent.
- An SDP aggregates different network capabilities and services as well as different sources of content and allows application developers to access them in a uniform and standardized way.

As technology and the convergence process evolve, SDPs often require integration of telecom and IT capabilities and the creation of services beyond technology and network boundaries. In this sense, SOA adoption into SDPs allows service-oriented applications to be easily constructed through a collaboration of autonomous specialist enablers.

Lately, the growing number and complexity of services deployed on SDPs, as well as new specialized SDPs, has lead to the concept of the Service Delivery Framework (SDF). It refers to a set of principles, standards, policies and constraints used to guide the design, development, deployment, operation and retirement of services delivered by a service provider with a view to offering a consistent service experience to a specific user community in a specific business context. An SDF Reference Model is currently being defined by the TeleManagement Forum [TMF-TR139a], focusing their efforts on the management of the platform and the services it provides. As long as the author knows there are no results available for this initiative.

Nevertheless, although many advances have been done in the field of service delivery platforms they are still aimed to provide a developer-oriented infrastructure, thus constraining the service creation and delivery process to selected third parties and professional programmers. However, new successful, Web-originated paradigms have highlighted the importance of involving end-users in the development process. Next sections provide details on these new paradigms and how they are applied to the service creation and delivery in Telecommunications.

3.3.2 When users become producers

Tim O'Reilly described the Web 2.0 principles in September 2005 [O'Really05]. From his first ideas other paradigms have come about in other contexts, such as Telecommunications, under the umbrella of the buzzword 2.0: Telco 2.0[3], Mobile Web 2.0 [Jaokar&06], and so on.

The main concepts under these new paradigms are:

- ***The idea of a platform***; i.e. there is no hard boundary for the company business, but rather, a gravitational core around which the business is created.
- ***Harnessing collective intelligence***; i.e. turn your customers and providers into a global brain, which could be used to enhance your business.
- ***Data is one of the assets a company owns***; notice that most of the time this information is about the company's customers i.e. identity information.

[3] Telco 2.0 is a trademark of Simon Torrence Limited (STL) [TELCO2.0]. However, as the general principles underpinning the Telco 2.0 approach have been spread so that the Telco 2.0 term has been coined as a general word.

Regarding the first point, there is nowadays a trend towards partnership and the need to build open technology platforms that enable third party providers to collaborate. Relevant examples of this trend are the Amazon Web services [AMAZON]. They allow external developers and businesses to build their own applications with a set of Web services interfaces.

The most innovative case though, is the so called user-centric platforms [Caetano&07], which add the second concept of the 2.0 paradigms. User-centricity refers to the approach that is built around the needs and requirements of the end-users. User-centric platforms extend this approach to allow end-users (not necessarily the very technically skilled) to create and share their own User-Generated Contents (UGC) [OECD-ugc07].

This idea has been initially used in the Internet within Web-based user-centric environments such as Yahoo! Pipes [YAHOO!], IBM's QEDWiki [QUEDWIKI] or Microsoft's Popfly [POPFLY]. These tools allow end-users to create their own contents from the easily and quickly combination (composition) of different sources.

Mashup is a powerful concept behind the Web 2.0 paradigm that is starting to be applied to user-centric environments. A mashup is an application or service that aggregates multiple services and contents to achieve a new purpose. Yahoo! Pipes is mainly used to create mashups from the aggregation and filtering of several Really Simple Syndication (RSS) and Atom feeds. QEDWiki allows end-users to create new widgets from the combination of different services and data sources.

The possibility of adding functionality and a programmatic logic to users' products drives the evolution from UGC to User-Generated Services (UGS) [Jensen&08]. Leveraging on their users, user-centric environments support the fast development and supply of innovative UGS, which benefits the different parties involved. Development expenses are cut down while customers' expectations are fulfilled because they develop their own personalized services that better fit their needs.

Nonetheless, the combination of user-centric environments with social networks that allow for sharing and recommendation provides even greater advantages:

- When users are allowed to share their products within a community, the most interesting ones would be promoted at a minimum cost with mechanisms such as the Viral Marketing. Viral Marketing refers to marketing techniques that use pre-existing social networks to produce increases in brand awareness, through self-replicating viral processes, analogous to the spread of pathological and computer viruses. It can be word-of-mouth delivered or enhanced by the network effects of the Internet. This eliminates one major disadvantage of the traditional Telecommunications business models i.e. marketing expenses.
- When users are allowed to recommend services, the set of high value services will success from among the great amount of services that are to be created within a user-centric platform. These frequently recommended, high value services will actually provide added value to users, and might turn out to become a kind of killer services in the long tail [Anderson06].

The benefits of the 2.0 paradigms are clear, but the obvious question now is why any end-user should choose my platform rather than someone else's. The answer points to the third idea of the 2.0 approach: data is one of the main assets of a company.

Telecommunications companies have been collecting information about their customers. It has been kept in information silos just for their own use. However, they

can now use this information to boost their service delivery platforms and take advantage of the benefits the user-centric approaches provide, thus leveraging new and profitable business models. On top of that, being the mobile phone a personal device which subscribers wear everywhere and every time, it has the potential to act as a significant reporter of profitable, personal information. Moreover, in most cases they have even established a trust relationship with their customers, which may be also used as a powerful asset. Nonetheless, customers can also benefit from the use of their identity information with features such as personalization, customization, improved usability, better user experience and enhanced security.

On the other hand, in most countries there are laws which require companies to ensure security and privacy when revealing personal information about a customer. Thus, we have arrived at a point where we could create platforms that greatly improve the traditional service creation and delivery approach as far as users' privacy and identity information is protected. Unfortunately, little attention has been paid to this issue up to now.

The end-users' privacy protection in user-centric service creation and delivery platforms is one of the focuses of this work. Section 3.5 further describes this situation and the state of the art regarding privacy and data protection.

3.3.3 Status of User Generated Services in Telecommunications

This dissertation focuses on user-centric, telecom-oriented and IP-based service environments enabling the creation and delivery of UGS. These environments have recently begun to be introduced, and thus Telecommunications mashups, unlike Web-based mashups, are rather limited. Yahoo! Pipes [YAHOO!] and Google Mashups Editor [GOOGLE] are example of Web-based mashups tools. British Telecom (BT) toolkit Web21C [WEB21C] was one of the earliest Telecommunications examples.

BT Web21C allowed external developers and businesses to build their own applications using a small set of Telecommunications services, e.g. messaging, voice call and conference call. However, in this case the creators must be technically skilled, because the means chosen to compose services was through Java and .NET APIs. Following BT platform launch other telecom operators began to provide developers with community portals and open APIs for network access e.g. Telefónica's Open Movil Forum [OPENMF], Vodafone's Betavine [BETAVINE], Orange Partner [PARTNER] and AOL Developer Network [AOLDN].

Microsoft and BT launched together the Connected Services Sandbox [MS-CSS], merging the Microsoft Connected Service Framework [MS-CSF] (focused on service aggregation of Microsoft services) and the aforementioned Web21C. The result was a Telco 2.0 solution where Telecommunications services can be part of a service mashup. However, this solution lacked the required variety of telco services required to achieve real value added services, especially since third party providers could not introduce their own services for composition. Another drawback was the lack of an event-oriented model for service triggering, which prevents creating real telecom-oriented mashups that can be initiated by an SMS or a voice call. Recently, the standalone Web21C initiative was discontinued after Ribbit [RIBBIT] has been acquired by BT, which is a step forward towards real User Generated Services.

The Open Platform for User-centric service Creation and Execution (OPUCE) [OPUCE] is a research project within the European Union Sixth Framework Programme for Research and Technology Development. OPUCE aims at creating a telecom-

oriented user-centric SDP that supports the whole service lifecycle i.e. from creation, to management and execution of user-centric Telecommunications services. As long as the author knows OPUCE is the first SDP where real end-users are allowed to create, share and execute telecom-oriented services.

Table 1 summarizes the aforementioned initiatives and compares them in terms of some features: whether they provide Internet- and telecom-oriented services, if third parties are allowed to introduce new services, the existence of visual tools to allow non-skilled users to create their services, etc.

Table 1 - User-Generated Service creation and delivery platforms.

Feature \ Platform	Yahoo Pipes	Google Mashup Editor	Ribbit (former BT Web21C)	Betavine	Connected Services	Movil Open Forum	Orange Partner	AOL Developer Network	OPUCE
IT Services	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telco Services	No	No	Yes	Few	Yes	Few	Yes	Few	Yes
Graphical Mashup Editor	Yes	No	No	Yes	Yes	No	No	No	Yes
Open to Third Parties	No	Yes	No	Yes	No	No	No	No	Yes
Context Adaptation	No	No	No	No	No	No	No	No	Yes
Users' Community	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

3.3.4 Section summary and conclusions

This section has provided an overview of the status of service creation and delivery in Telecommunications. First, the concept of service delivery platform has been defined. Then the foundations for User-Generated Contents and User-Generated Services have been described as well as the benefits UGS can provide to telecom-oriented service delivery. Finally, a summary of the state of the art of UGS in the Telecommunications domain has been provided.

The main conclusion we derive from this section is that SDPs will become increasingly important as the convergence between Telecommunications and Internet worlds accelerates. Additionally, we think that this convergence process will include new Internet-originated paradigms, such as UGS.

Nevertheless, to take advantage of the user-centric model operators still have to address the challenges associated with opening up their service platforms, creating and managing user-defined products, capturing and handling orders for them, managing the provisioning of underlying services, enabling subscribers to administer relevant service parameters and settings, managing third parties relationships, and how to leverage identity resources while protecting customers' privacy. Furthermore, the expected increase in the number, complexity and specialization of services pose even greater challenges. This dissertation proposes contributions aiming to solve some of these issues.

3.4 Service management and operation

IP has been the chosen protocol to drive the convergence process of the telecom industry. NGN is the standardized architecture for these new IP-based networks. Over the NGN a new application-enabling layer is growing, which is supported by the IMS, SOA and standardized service enablers to abstract the different access networks and to decouple the business and service logic from the underlying network implementation.

In this context several tools and development environments are being created that allow for fast and cost effective service creation and delivery, which have roughly been named as Service Delivery Platforms. Nowadays telecom operators have got SDPs to create new services, but they are highly tied to the underlying layers and their own OSS/BSS processes. Therefore, although services can be fast created for a network operator they cannot be seamlessly ported to other operators' SDPs, or provisioned to other environments. Furthermore, the idea of an SDP that allows creating enterprise-grade applications using services from external domains and exchanging sensitive information with them is not feasible nowadays, as there is a lack in the state of the art about how these domains can securely interoperate or manage their relationships in a standardized way.

When it comes to user-centric SDPs these problems are even more important, as all the end-to-end processes involved in the service creation, provision and execution must be fully automated along all the participating providers. For that, a common understanding of the processes involved, their interfaces and an agreed vocabulary is a must. These activities are somehow being addressed within standardization bodies and industrial fora, though it has not provided clear results yet. On the other hand, some software vendors provide partial solutions to specific problems, most times with no standard-based interfaces though, which do not help to provide a holistic solution either.

This section analyses the relevant initiatives that partly provide solutions for the described problems and requirements all in the management domain, the Telecommunications standardization bodies and relevant vendors' initiatives.

3.4.1 TeleManagement Forum

The TeleManagement Forum (TMF) [TMF] is the most important body in the Telecommunications management domain. TMF best known specification is the Next Generation Operations Systems and Software (NGOSS) [TMF-GB930] framework, which sets the basis for separation of business process from component implementation, loosely coupled distributed systems and contract defined interfaces. It includes the enhanced Telecom Operations Map (eTOM) [TMF-GB921] and the Shared Information Model (SID) [TMF-GB922].

The focus of eTOM is to help service providers to define and describe the business processes they use (Figure 6), to understand the linkages between these processes, and to identify interfaces and external entities collaborating, as a way of structuring operations. It provides a business framework with hierarchy, relationships and individual process decompositions, as well as linking process flows that allow the business to be modelled in detail and end-to-end. It makes available a standard structure, terminology and classification scheme for describing business processes and their constituent building blocks.

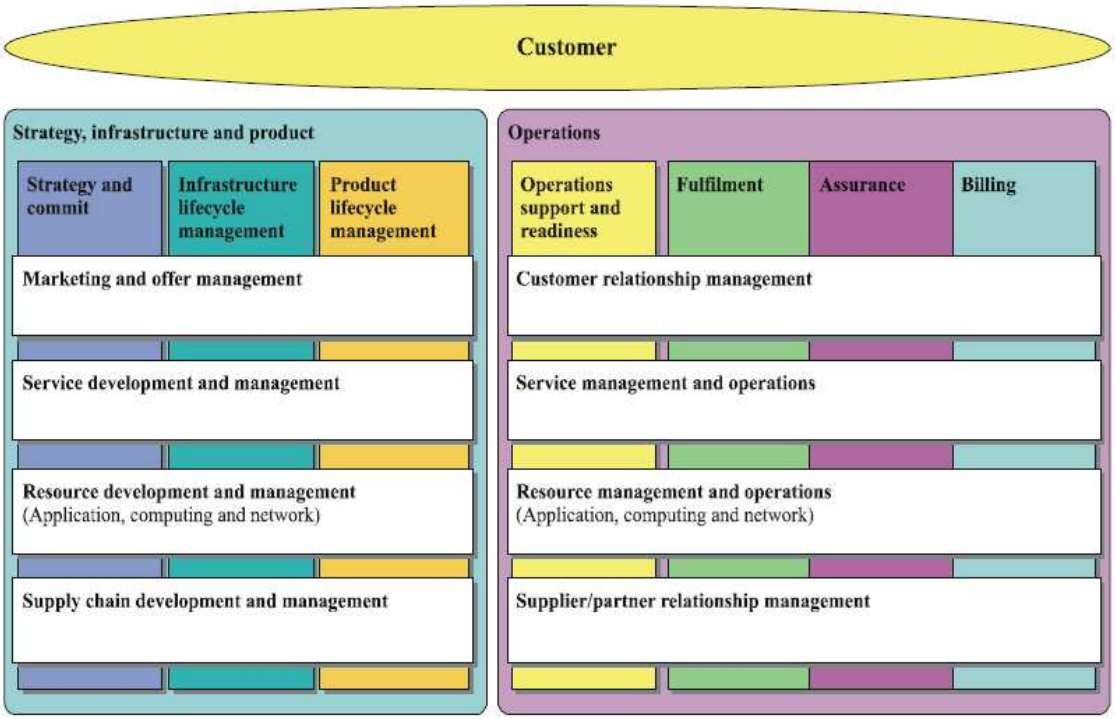

Figure 6 – eTOM business process framework Level 1 [M.3050.1].

SID complements eTOM providing a vocabulary for communications across the entire business and operational systems of a service provider as well as a standard format for exchanging information with partners and vendors. Therefore, eTOM and SID are useful tools to achieve B/OSS integration and distribution.

Using both eTOM and SID a service provider gets a clear view of its business processes, which facilitates the automation of several service lifecycle activities, mainly those related to service and product Fulfilment and Assurance, within the eTOM Operations area. However, poor attention has been paid to the automation of the Product Lifecycle Management processes defined by eTOM, which map the early stages of the product lifecycle such as product development. It was considered that one thing was the product development, which could be done off-line, and another one the deployment, activation and operation, which were considered real-time processes.

Moreover, the user-related activities are rather constrained to Customer Caring, which can trigger some product management processes in the Operations area on behalf of the customer. However, end-users are not allowed to control new products creation and deployment processes. Therefore, TMF needs to extend its eTom work to address the fast and automatic service creation, service deployment and service operations aspects required for user-centric SDPs.

Lately, the TMF has also realized the lack of specifications or standards that address the management of SDPs and the content/media services that are created and delivered within them and has decided to work on the standardization of a *Service Delivery Framework* (SDF) [TMF-TR139a] seen from a service provider point of view. Together with other industry groups, TMF will work on getting to a commonly agreed terminology and functional view of such an SDF. This will then serve as the base for further work on management interfaces and on identifying new operational processes that allows for service management across SDPs in distributed domains and linkages to B/OSS.

Unfortunately, this work is still in its early stage, namely requirements gathering, and no many results are publicly available (Some results are expected by the end of 2009 [Greene&08]). However, a number of essential SDF architectural features have been identified so far:

- *Product Lifecycle Model*: A standardised model and a unified view are needed to ensure that all products and services follow a common lifecycle model: service design, creation/composition, deployment, activation, provisioning, sale and campaign management, execution, operations, charging, billing and revenue management, retirement, monitoring and trouble resolution etc.
- *Management Reference Model:* Agreed services and interfaces are also needed in the different stages of the lifecycle to interact with the end-to-end product (SDF services), the supporting B/OSS processes, and the infrastructure (Figure 7).
- *Metadata Model*: Metadata descriptions must be defined as the reference base for all specifications of products and services. This facilitates consistent and compatible specifications that can be readily combined.

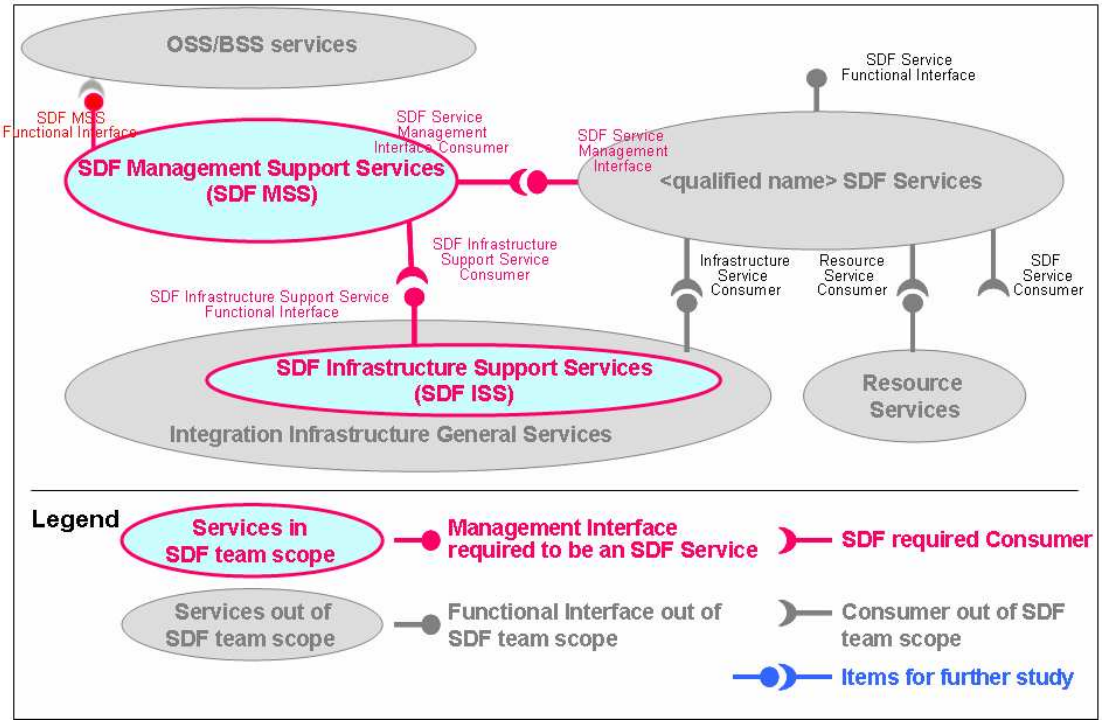

Figure 7 - TMF SDF reference model (working draft version 2) [TMF-TR139b].

TMF has also recognized the need to manage across both IT and communications domains in a truly converged ICT scenario, and thus it has addressed [M.3050.s1] the need to integrate eTOM with the Information Technology Infrastructure Library (ITIL) [ITIL], which is the reference standard for IT management. Quite in the same line, some efforts are being done [TMF-CIM] to align SID and the Distributed Management Task Force (DMTF) Common Information Model (CIM) [DMTF-CIM]. Although very interesting, this work is out of scope of this dissertation.

Nevertheless, although TMF SDF will provide a standard agreement to support interoperable and B/OSS-aware SDPs it will not address the user-centricity of services

neither the automation of the whole end-to-end service lifecycle processes, which are essential requirements for the work we propose.

3.4.2 IPsphere Forum

The IPsphere Forum [IPSF] is an international non-profit consortium of network equipment manufacturers, IT companies and communications service providers. It was established in 2005 with the aim of developing an open multi-stakeholder Web services framework for the rapid creation and automated deployment of IP-based services, supporting the flexible distribution of service revenues so that stakeholders may be recompensed when services are consumed.

The IPsphere Framework [IPSF-TS] is based on the concepts of service abstraction and decomposition: *Services* are structured via their decomposition into constituent *Elements* that represent the capabilities of a set of technology resources. The introduction of service templates for service descriptions provides the means for the translation of an abstract service offering into a set of concrete resource commitments across providers to meet the overall service goals.

The framework also defines interfaces for existing systems to participate in the interaction between service-based views and resource-based views. Moreover, it also provides interfaces to critical business functions such as billing systems, ordering systems, technology management systems and other sub-systems. Although this approach allows for a great degree of flexibility and processes automation, its realization is not clear as it has not been further documented yet.

Figure 8 depicts the IPsphere in the context of a typical network service provider's operating environment.

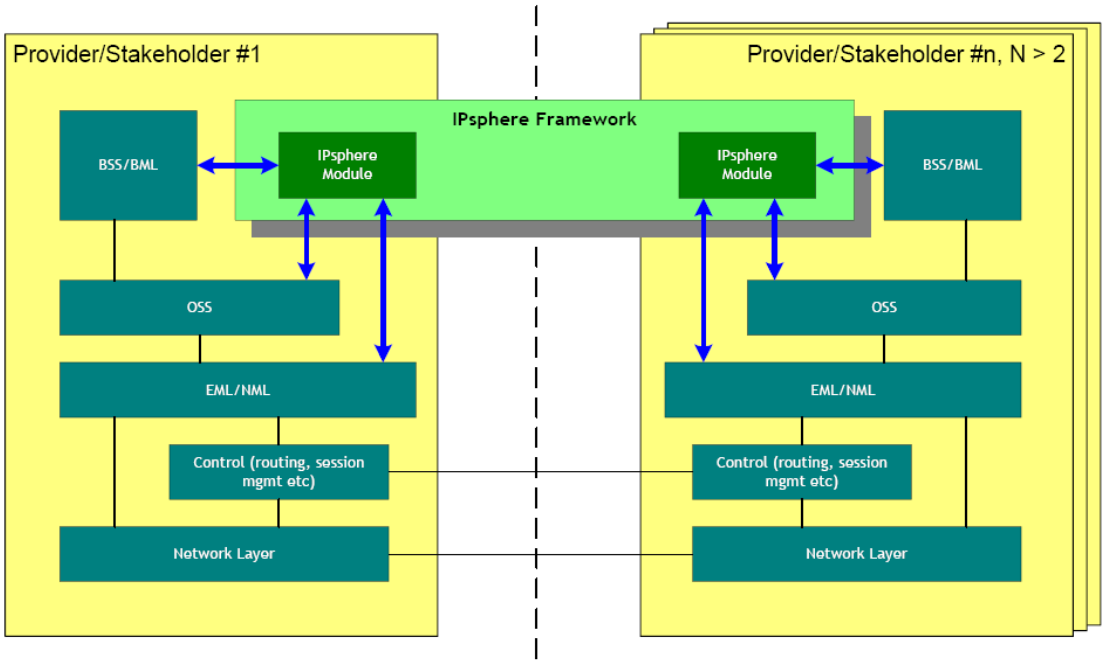

Figure 8 - IPsphere Framework [IPSF-TS].

At a functional level, the IPsphere Framework identifies the entities required, mainly *Service Owners* and *Element Owners*. At the highest level the Service Owners and Element Owners communicate for the purpose of provisioning, activating and monitoring services. Communications are bi-directional: A Service Owner orchestrates the provisioning and activation of a service by sending messages to the partnering

Element Owner and, once a service has been activated, an Element Owner may communicate faults, performance and other SLA related data by sending alerts back.

The framework also defines an information model to capture the requirements of a structured service; defines the flows for distributing the configuration information to the participating elements so they can be configured to deliver the service; allows for fault and performance monitoring both in structured service and the underlying resources so that the service owner can take preventative action or inform the customer of a violation in the contracted service level agreement; and generates events to support auditing, notification, billing and settlement, etc.

IPsphere, as a standards activity to define the process of decomposing service features into resource capabilities, is in fact a kind of flow management definition that specifies the features of various application components and the way that information flows between those components to create and support a service. Actually, the IPsphere Service Owner and Element Owner entities both are themselves service providers that individually have business processes as per the eTOM specification, where the latter is part of the supply chain of the former. The details of such cross jurisdiction relationships are not completely defined by eTOM today, and thus the work undertaken by the IPsphere Framework may be used to further refine eTOM. Nevertheless, IPsphere has not mapped its processes with eTOM blocks neither has employed SID vocabulary and data structures.

Summarizing, IPsphere major achievement is the specification of a set of processes needed to allow cross-domain providers collaboration. It is based on an abstract, layered model that allows for decoupling of services from their elements implementations, and the underlying networks and infrastructure. It also defines the means for some lifecycle management automation, supported by the use of service templates and a set of agreed components and interfaces. However, no information is provided about the rules to create these templates neither their specifications.

From the viewpoint of the goals of this dissertation, IPSphere Framework does not address the user-centricity of services at all, and the lack of information about the templates makes unclear the possibility of automation of the whole end-to-end service lifecycle processes from creation to retirement. Besides, as no details are available about the information model, except that it is not based on SID, its extensibility is not clear either. On top of that, IPSphere does not seem to address the exchange of personal information between different administrative domains.

3.4.3 Open Mobile Alliance

The Open Mobile Alliance (OMA) [OMA] focuses on the communications service layer independently of the underlying network technologies, which are specified by other organizations such as 3GPP [3GPP], 3GPP2 [3GPP2], TISPAN [TISPAN] and Parlay [PARLAY]. OMA works on specifying enablers, which provide standardized components to create an environment in which communications services may be developed and deployed.

Enabler implementations abstract the underlying network technologies and are realized on network resources using adapters. An OMA enabler is defined in terms of three types of interfaces, namely the *functional interface*, the *resource facing interface* (out-of-scope of OMA specifications) and the *lifecycle management interface*.

The OMA enablers, the decomposition into these components and the interactions between them comprise the OMA Service Environment (OSE) [OMA-OSE]. Within the OSE, applications are built by composing or delegating to OMA enabler implementations through the functional interfaces. Policy enforcement, through the *Policy Enforcer* architectural element, applies policies on any request to/from/among any resource in the OSE thus providing a generic mechanism to expose service providers' assets to third parties.

The *Policy Enforcer* intercepts all messages across the service provider service layer. Using this approach allows factorization of business rules from enablers and services: enablers or services provide only intrinsic functions using the functional interface (functions that are essential in fulfilling the intended task of the specified enabler e.g. Messaging) while the service providers can set policies for security, charging, SLAs, logging, QoS, privacy etc. that are enforced at the level of the Policy Enforcer.

Figure 9 provides a high overview of the OSE architectural model.

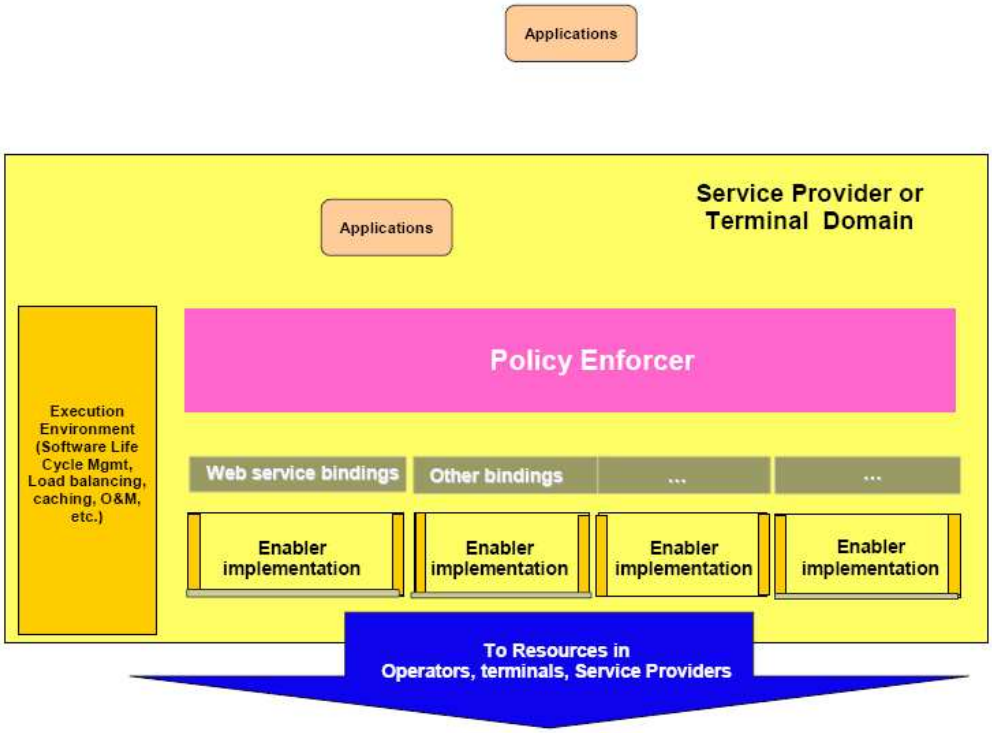

Figure 9 - OMA Service Provider architectural elements [OMA-OSE].

The OSE fulfils our first requirement as it abstracts the network resources and implementation from the services and applications that use them. It also allows for a certain degree of extension, as long as it is done following the OMA specifications for enablers implementations.

As for lifecycle management automation, the OSE specification states that the *Execution Environment* will support lifecycle management functions such as creation, deployment, operations, management, maintenance, removal, etc, through the enabler *lifecycle management interface*. However OSE does not specify any lifecycle for applications and enablers, and just refers to the eTOM for the definition of the service lifecycle phases. Therefore, although B/OSS integration can be achieved through the *Execution Environment* no processes have been specified so far. Furthermore, since

end-to-end services are out-of-scope of OMA specifications no interface has been specified to make possible an inter-*Execution Environment* integration and thus allow interactions among distributed OSE deployments. For the same reason user-driven features are not devised.

Nevertheless, OMA is working on a new enabler definition, the OMA *Service Provider Environment* (OSPE) [OMA-OSPE], which aims at implementing lifecycle management and service level tracing functions for OMA enablers and services within the OSE. These management capabilities will be exposed through the enabler functional interface and will help to solve some of the detected shortcomings for lifecycle management automation.

3.4.4 The SDP Alliance

The SDP Alliance [SDPA] is the result of a collaboration agreement between a set of software product companies that aim at defining an SDP architecture to support end-to-end ICT products delivery. The main difference with other initiatives is that instead of being supported by abstract enablers, interfaces and functions the SDP Alliance architecture is supported by its members' products, which are pre-integrated with internal and external enablers to define an end-to-end architecture.

The SDP Alliance provides solutions for the major part of the products lifecycle management and also for the integration with existing B/OSS solutions. However, although this is one of the firs efforts to define an end-to-end SDP for the ICT domain it clearly lacks the openness necessary for other organizations to adhere, and thus the extension is quite constrained to the members' products.

Moreover, even though the decoupling and abstraction from underlying networks and implementations could be achieved by means of world wide standards such as ParlayX, OMA enablers or IMS, these advantages are hidden by the use of specific proprietary products. Therefore, the decoupling and abstraction are somehow lost and the solution is now tight coupled to a reduced set of software products.

Last but not least, the support for user-driven actions is constrained to what the SDP Alliance members' solutions provide, which currently is nothing.

3.4.5 IEEE

IEEE Next Generation Service Overlay Network (NGSON) [IEEE-NGSON] working group aims at developing a standard to define and specify an overlay network architecture to support information and communication services. This (collaborative) service inferred overlay network is independent of underlying transport networks. The purpose of this standard is to facilitate the timely and efficient deployment of solutions that enable network operators, service/content providers, and end-users to create, deploy, and access collaborative services.

The project was approved by the IEEE Standards Board on 27th March 2008. Therefore, it is an on-going project which results will take time to arrive.

3.4.6 Autonomic Communications Forum

The Autonomic Communications Forum (ACF) [ACF] was established at the end of 2004 following an initiative by the EU funded Autonomic communication Accompanying Action project. ACF addresses autonomic principles for the management of service compositions, and its final goal is to "*develop a set of*

mechanisms allowing the self management of service compositions". In order to get this target, ACF intends to develop a framework covering technologies and mechanisms necessary to give NGN the following self-management capabilities:

- Self-configuration of service choreography.
- Self-monitoring and -testing of composite service and service component parameters.
- Self-awareness of context, environmental information.
- Self-healing and -optimization of composite service and service components.
- Automatic, dynamic service discovery.
- Automatic, dynamic service composition.
- Automatic lifecycle management, from service activation to service retirement.

Although most of their objectives could fulfil the requirements set for this dissertation up to now there are no available results, and it remains unclear whether there will be. Besides, the lifecycle management approach does not cover some important stages of the product lifecycle such as service creation and service deployment. Moreover, it does not address the user-centricity of services.

3.4.7 Telecommunications Management Network

ITU-T Recommendation M.3010 [M.3010] defined a Telecommunications Management Network (TMN) reference model to manage traditional Telecommunications networks. TMN defined a hierarchical OSS architecture organized in four logical layers of abstraction (Business, Service, Network and Element) across which multiple management functions or services apply [M.3200] [M.3400]. Under the element management layer there is a Network Elements layer, which includes all the network equipment that constitutes a single resource e.g. servers, routers, etc. (Figure 10).

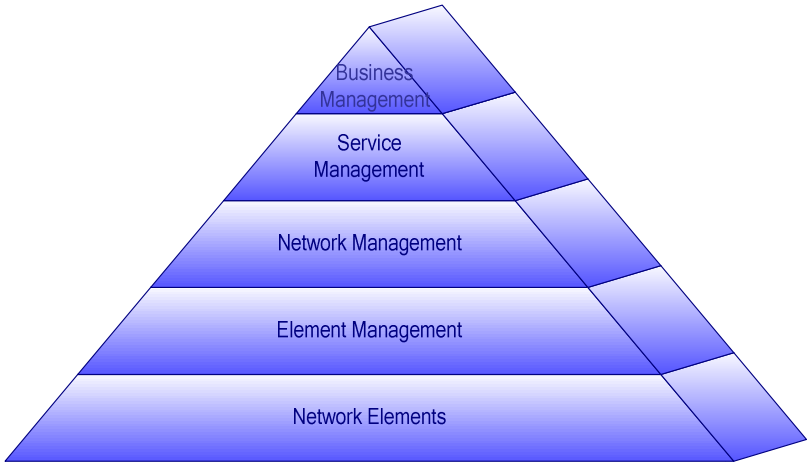

Figure 10 - ITU-T's TMN architecture.

The TMN model is simple and its strength is that it provides the capability to reach a level of abstraction that is increased through the layers. In theory, it could be possible to manage any network, services and products using it. However, NGN requirements to provide better support for network services, business process automation and to reduce

operational costs, made it clear that major changes were required. Furthermore, TMN standards were mainly concentrated in the element management and network management layers, paying poor attention to the service and business (product) one. Thus, the product and service lifecycle management is not possible, let alone any kind of user-driven actions.

The TMF's NGOSS framework has tried to cover this gap, as its specifications have been adopted in the major Telecommunications standardization bodies such as ITU-T [M.3050.0] and ETSI TISPAN [TISPAN-oss05] [TISPAN-oss06a] [TISPAN-oss06b]. For example, following the hierarchical model defined by TMF's eTOM, TISPAN NGN OSS Functional/Information View has defined three horizontal top-level NGN OSS Service Interface Groups, which map the homonym eTOM functional areas.

However, the *Market, Product and Customer Management Service Interface Group* has not been specified yet. It is worth noting that they address the definition of the products, the management of instances of products during their whole lifecycle, the management of interactions with the customers through business interfaces, and the administration and management of functionality that uses information from the layers below.

Two other extra Service Interface Groups are also included: the Basic Framework Services Service Interface Group, which provides common services (e.g. security, directory, etc.) supporting the other Service Interface Groups, and the Supplier/Partner Management Service Interface Group.

Figure 11 shows the whole ETSI NGN OSS Functional/Information View. On the left side it also shows the TMN model (simplified from Figure 10), and the correspondence between its logical layers and ETSI NGN OSS Service Interface Groups.

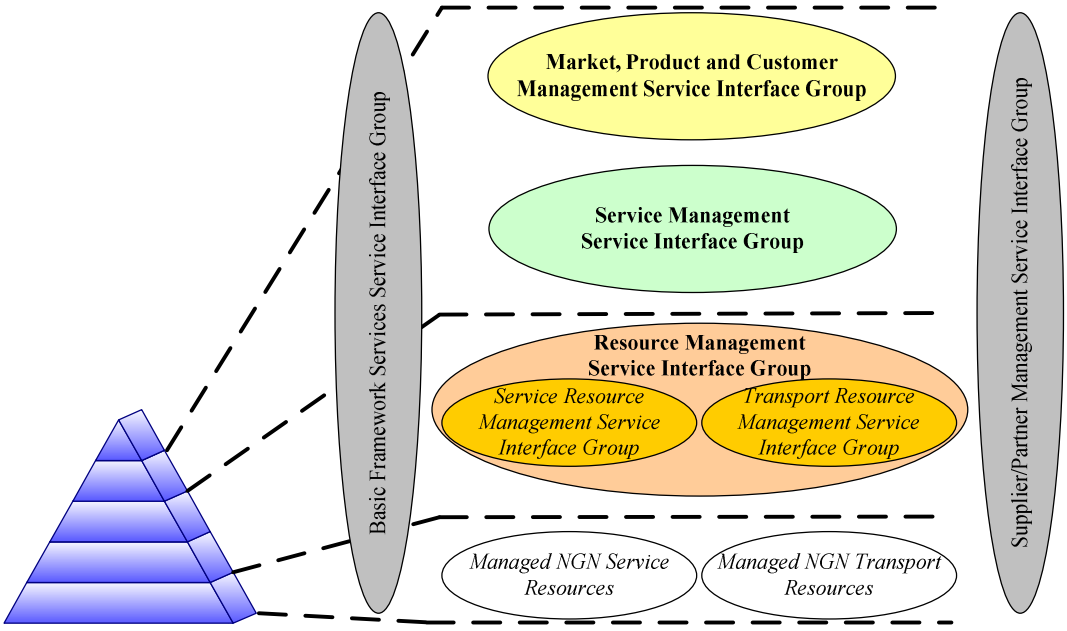

Figure 11 - ETSI NGN OSS Functional/Information View.

Although the TMF NGOSS framework provides the Telecommunications networks with the means for the definition of a management infrastructure that fulfils some of our requirements, this infrastructure has not been defined yet. Moreover, some of the key process enablers for the success of this infrastructure such as the customer facing interfaces have not been addressed either in the NGN standardization bodies.

3.4.8 Software and Equipment Vendors

Software and equipment vendors have been already developing and deploying user-centric technologies on the Internet, where the introduction of this new paradigm has followed a faster pace than in the telecom domain. Thus, they have taken advantage of its knowledge and expertise on this field and have extended their products to the converging ICT domain. Therefore, in some specific aspects, software vendors' products are ahead of the standardization processes. However, unless a globally agreed specification governs their developments the interoperability and interconnection aspects will be a difficult problem to tackle.

Nevertheless, and acknowledging the importance of the pressure that these companies' lobbies can bring on the standardization bodies, a brief summary of their main developments in the user-centric service creation, management and execution environments is provided focusing on those aspects related to operations and management. This can be seen as a partial view of the direction towards the ongoing standards can move on. For a deeper description the reader can refer to [Mendyk07].

3.4.8.1 Alcatel-Lucent

Alcatel-Lucent is working, among other fields, on exposing enablers to third parties and the business models that might accompany such exposure i.e. how such service functions can be publicized, how they can be secured, and which charging implications are associated in the mashups value chain. It also recognizes the increasingly importance of the client side developments, and thus it is working on exposing device capabilities as service enablers.

3.4.8.2 BEA Systems

As one of the top software vendors in the Internet and Enterprise domain, BEA tries to reuse its existing products to the telco domain. For instance, the mashups creation tool is based on the AquaLogic family, which also provides tools for mashup governance such as Web resource management, application usage monitoring and integration with existing BEA's security and runtime infrastructure based on WebLogic Application Server. This application server is also extended to the telco domain to support telecom service enablers.

3.4.8.3 IBM

IBM was one of the earliest companies to research the user-centric service creation field. As a result, it has developed its own mashups creation environment: QEDWiki [QUEDWIKI]. However, the integration of QEDWiki with telco environments is not clear though and IBM is doing some efforts to improve this area.

IBM service execution environment is supported by its own enterprise-level application server, WebSphere, which is being complemented with its Telecom Web Services Server providing a policy server to enforce SLAs and security functions on request to services, and its own service platform for network enablers.

3.4.8.4 Microsoft

Microsoft can be considered today as the most relevant software vendor regarding user-centric service mashups for Telecommunications. Its early launch of the Connected Services Framework [MS-CFM] allowed it to begin composing applications that

combine telco enablers with Internet-provided Web services. Microsoft mashups for the telecom domain are based on the idea of *managed network mashups* i.e. the mashups are created from services exposed through an SDP, which provides the management and operations functions needed to discover, control and monetize them. Thus, Microsoft envisages telcos playing a broker role in bringing their own and third-party services together. The contributions of this dissertation are aligned with these principles.

In 2006 Microsoft launched the Connected Services Framework Sandbox [MS-CSS], which provides a user-centric, Web 2.0 approach to its previous developments. In collaboration with BT, who provides its Web21C service development kit, it has been running an open competition for the best-of-breed mashups. The winners are allowed to deploy their services on BT's infrastructure.

3.4.8.5 Oracle

In early 2007 Oracle released its own mashups creation environment, WebCenter Suite, addressed to professional developers (and thus not feasible for user-centric environments). It is an add-on to the Oracle's Java Enterprise Edition Application Server which provides the service execution environment and some management and support functions. Although the WebCenter is not specifically aimed at the telco domains Oracle provides some other products that could complement it with communications features, CRM, billing and revenue management. Nevertheless, there is a gap to cover for the integration of Oracle's vision into the telco domain. Moreover, the lack of user-centricity on its products is also a major drawback.

3.4.8.6 Red Hat

Red Hat provides an Integrated Development Environment, the JBoss Developer Studio, which supports Java Enterprise Edition, SOA and Web 2.0 developments. It also provides a service execution environment based on its JBoss Application Server. Recently, Red Hat also completed the acquisition of Mobicents, an open source, SDP server technology certified for JSLEE compliance. Through the combination of the Jboss and Mobicents middleware offering, Red Hat has created the JBoss Communications Platform for the telecommunications industry, which can be seen as Red Hat's ICT service execution environment.

3.4.8.7 Sun Microsystems

Sun provides a service creation environment through its NetBeans suite of tools, which allow for Java, scripting languages, SOA, Ajax, and other Web 2.0 developments. Its service execution environment is supported by its open source application server, GlassFish. Lately, Sun has joined efforts with Ericsson, who has provided its SIP application server, to create the project SailFin, which aims at developing a complete ICT-grade service execution environment.

3.4.9 Section summary and conclusions

This section has thoroughly explained the state of the art that may be useful in fulfilling the requirements set for the management and operation of a NGN-based user-centric service creation delivery platform. Therefore, the major standardization initiatives in the management and the Telecommunications domains, as well as the latest software and equipment vendor products, have been described.

Table 2 shows a brief summary of the results of the analysis of standardization initiatives under the viewpoint of our requirements.

Table 2 - Standards analysis under the view of user-centric SDP requirements.

	Abstraction & Decoupling	**Lifecycle management automation**	**B/OSS integration & distribution**	**Model extension**	**User-driven support**
TMF	Well achieved Based on SOA Layered approach with increasingly abstraction	Partially eTOM (focused on operations) SDF improves cross-domain & product creation	Well achieved eTOM+SID (definitions & vocabulary)	Well achieved Supported by SID (enhanced with ITIL)	Partially eTOM, but focused on Operations
IPSF	Well achieved Based on SOA Layered approach with increasingly abstraction	Well achieved Major developments support this requirement	Partially A limited set of functions has been defined	Unclear Templates to support service description There is no specifications available	NO
OMA	Well achieved Abstracts network resources from services/products	Partially No lifecycle management processes are defined OSPE could improve this	NO No relationships among different OSEs are specified at this level	Partially Based on OMA enablers	Not applicable
SDPA	Constrained to the particular specifications of the members products				NO
IEEE	Work in progress. No results have been published yet.				
ACF	Well achieved Based on SOA principles	Partially Service creation & deployment not addressed	Unclear No description is provided	Not applicable	NO

After analysing the above table, it can be said that TMF specifications are the best prepared to address the requirements set for this work. However, since the eTOM considers the Product Lifecycle Management as an off-line process it cannot possibly fulfil the whole lifecycle management automation needed within a user-centric environment. This is also the major reason constraining the user-driven support of management processes in an end-to-end service.

Furthermore, eTOM provides just an abstract business process framework i.e. it can be used (with some changes) to formalize the end-to-end business processes needed, but from that point on, some other solutions must be used to realize the design. In that

sense, the work being conducted within TMF SDF initiative will provide some solutions to these problems. In the meantime, OMA OSE might be used as a good starting point, as it already defines an architecture to support the decoupling and abstraction from the underlying network resources, and provides a common model for services interactions.

Nevertheless, OMA OSE does not provide support for the whole product lifecycle management requirement either. IPsphere Framework does, based on the use of templates to support the service creation process and the subsequently lifecycle stages. However, no information about the IPsphere templates is available as for the time of this writing.

To conclude, it can be said that nowadays there is no standard solution that address the management and operation that end-to-end products and services in user-centric service creation and execution environments need. Furthermore, when it comes to the management of users' personal information and their privacy protection the lack of solutions is even worse.

3.5 Identity management and privacy control

In its widest definition a ***Digital Identity*** [Camp04] [Windley05] refers to the set of permanent or long-lived temporal attributes associated with a digital entity. In the context of this work, a digital entity usually represents a human being or user of the digital world.

When users want to interact with a service in the digital world (e.g. Internet) they have to demonstrate their identity very often. For this purpose, the user usually registers a new account with the service provider providing it with a login, a password and some identity attributes that may be required to personalise the service or to set user preferences. In that sense, this account is a partial expression of the user's digital identity.

Once the digital identity has been registered it can facilitate the following operations that are related to access management to services:

- ***Authentication***. It is the process of validating that it is indeed the owning entity that is using or deploying the owned identity in an interaction. The stronger the authentication is, the higher the confidence that the user of the identity is its owner.
- ***Authorization.*** The process of determining, by evaluating applicable access control information, whether an entity is allowed to have the specified types of access to a particular resource e.g. a service.

Registering an account, authenticating users and granting authorizations are all common and vital management processes in the daily business of any service provider. These processes are often thought of as a part of information security, but they are also closely related to the digital identity of the users. Furthermore, digital identity has greater utility than just protecting information. For example, trust and privacy are two features equally as important as security when it relates to service management:

- ***Trust*** may be defined as an evaluation, by an entity, of the reliability of an identity when the identity is involved in interactions. The level of trust is typically based on the technical strength of the identity.
- ***Privacy*** is the ability of a person to control the availability of information about and exposure of him or herself. The level of privacy that a system allows for is

directly related to the capability of the user to control the flow of identity attributes and the number of attributes. Two terms related to privacy are anonymity and pseudonyms.

- A ***pseudonym*** is a fictitious name used by an individual as an alternative to their legal name. Practically, a pseudonym is an identifier which is not immediately associated to an entity.
- ***Anonymity*** is an attribute of an identity which allows it not to be bound or linked to an entity.

Nowadays, user accounts (and the identity information they contain) are scattered in multiple Telecommunications networks and Internet sites, where isolated services are provided with no cohesion among entities and user preferences. The current uncontrolled accounts proliferation means a bad user experience, reduces user trust on ICT services and represents serious scalar problems. Thus, it reduces the e-commerce services expansion and user attention, and might represent a substantial risk of fraud for identity theft. In an increasingly digitalized and collaborative world, a means to facilitate the management of user's identity is a must.

Identity management is the discipline that deals with the technical, legal and business processes involved into the management and selectively disclose of user-related identity information into an institution and between some of them, while preserving and enforcing privacy, data protection and security needs [Radhakrishnan07].

After this brief introduction to the main definitions of the digital identity domain, this section describes the lifecycle of an identity, and the related features that make it necessary to the management and operation of Telecommunications services. A short overview of privacy management is also provided.

3.5.1 Identity lifecycle

The operations performed on an identity start with the creation of the identity of a user when an individual joins an organization i.e. identity provisioning. The information initially set must be maintained during the lifetime of the identity within the organization i.e. identity maintenance. Once the identity information exists and is accurate, it may be used for different purposes within the organization e.g. access management to services. From time to time and due to business requirements, it may be also necessary to share it with other organizations outside the initial organization boundaries, i.e. cross-domain identity management. Eventually the identity information must be disabled or removed when the individual leaves the organization i.e. deprovisioning. All these steps could be done by the organization staff but they may be also controlled somehow by the end-users themselves, which is called user-centric identity management. Next subsections give more details on all these topics.

3.5.1.1 Identity Provisioning/Deprovisioning

The OASIS Provisioning Services Technical Committee [OASIS] has defined provisioning as the "*preparation beforehand of IT systems' materials or supplies required to carry out some defined activity*". From the perspective of digital identity, identity provisioning is the creation of the identity record and its population with the correct attributes.

Identity provisioning can be done by the system administrator but also by the end-users themselves (self-provisioning). Self-provisioning is common in Internet, where end-

users sign up for new accounts. However, it is a bit more difficult when users' credentials (identity) must be verified.

Sometimes the identity information must be provisioned in multiple systems within the same organizational domain, and thus automated provisioning is necessary. The Service Provisioning Markup Language (SPML) [OASIS-SPML] is an OASIS standard protocol for the integration and interoperation of service provisioning which supports the automation of all aspects of managing an identity throughout its entire lifecycle, including creating, amending, or revoking the identity.

3.5.1.2 Access Management

Access management consists of the processes and technologies for controlling and monitoring access to resources consistent with governing policies. Access management in Internet typically includes authentication, authorization, trust and security auditing. Access management in Telecommunications is also related to accounting, which may include auditing, and is usually referred to as AAA (Authentication, Authorization and Accounting) [Nakhjiri&05].

To lay claim to a set of attributes (e.g. an identity), a subject presents credentials that can be authenticated. The most common credentials in the Internet are the pair username/password. In the Telecommunications domain we usually introduce a Personal Identification Number (PIN) to access to our mobile phone. These credentials are grouped under the category 'something the user knows'. Some other kinds of credentials, also known as authentication factors, are 'something the user has' and 'something the user is'.

An example of 'something the user has' is a digital certificate. A digital certificate typically includes the public key, information about the identity of the party holding the corresponding private key, the operational period for the certificate, and the Certification Authority's (CA) own digital signature. In addition, the certificate may contain other information about the signing party or information about the recommended uses for the public key.

A CA is similar to a notary. It may issue certificates to users, to other CAs, or both. When a CA issues a certificate, it is asserting that the subject (the entity named in the certificate) has the private key that corresponds to the public key contained in the certificate. If the CA includes additional information in the certificate, the CA is asserting that information corresponds to the subject as well.

Once the users have been authenticated, their rights to access a resource must be checked. The simplest form of authorization is based on authentication: if the user has been successfully authenticated, then the user is authorized to use the resource. Other traditional Web authorization schemes, a bit more elaborated, are based on users and groups, roles and access-control lists (ACL). In the Telecommunications domain, authorization is sometimes coupled with accounting. If the network provider knows it can charge the user for the use of the service, then the user will be authorized for that service.

In any case, the abstract authorization architecture is based on two main entities: A Policy Decision Point (PDP) and a Policy Enforcement Point (PEP). The PEP is the point in the system where the user requests access to a resource. For example, if a user attempts to download a ring tone, the PEP is the server that the user accesses. The PDP is the point in the system where the decision is made as to whether or not the user will

be allowed to access a resource. In many cases, the PDP is part of the same system that houses the PEP, but it is not needed. The server could, for example, send the resource prize and the user identity to the network provider AAA system and simply get back a "yes" or "no" answer.

One feature related to authentication and authorization processes is Single Sign On (SSO). It is the ability to use one set of credentials to authenticate a user and allow him or her to access information across a system, application and even organizational boundaries without bothering him or her again with authentication processes during the access session. This feature enhances security and usability of ICT services because it allows users to have a single set of credentials that are easier to manage. The complementary process to SSO is Single Logout (SLO), which consists of the synchronize session logout across all sessions that were authenticated by a particular SSO session.

The third major process for access management in Telecommunications is accounting. Accounting is concerned with the collection of information on resource consumption at all or specific parts of the network. Sometimes accounting is confused with billing due to their close relationship; billing is the preparation of the invoice for the total amount of resources consumed within a given period of time. As we have previously said, accounting may include auditing, which is the act of verifying the correctness of an invoice submitted by a service provider.

In Telecommunications, the most widespread AAA protocol is Remote Access Dial-In User Service (RADIUS) [Rigney&00]. RADIUS was originally designed as the authentication protocol to manage the connection of dial-up users. It was later evolved to support authorization and accounting procedures.

When wireless and IP networks began to appear it was clear that RADIUS was insufficient to cope with the new requirements that the new architectures imposed. Thus, the Diameter protocol [Calhoun&03] was selected as the replacement of RADIUS, with a lot of improvements in different aspects such as reliable transport, support for security and audibility, capability negotiation, server-initiated messages, fail-over enhancements, better roaming support, etc. Diameter is widely used in the IMS architecture for IMS entities to exchange AAA-related information, and thus it is nearly a must in the access management for next generation Telecommunications services.

3.5.2 Cross-Domain Identity Management

Some models have been proposed to share identity information between different domains. The two most important are the centralized and federated approaches. The former proposes the creation of a central identity infrastructure where all the identity information about an entity is stored. Every single entity that requires identity information will store and retrieve it from this repository. This implies one single point of fault and the need to have one organization managing all the identity information of each user. This architecture was proposed by Microsoft with its Passport initiative for instance, but was fast rejected by the whole community.

On the other hand, the federated approach defines processes and supporting technology so that disparate companies can cooperatively solve identity tasks. If they have established trust relationships between themselves the process does not require a common root authority and is called Federated Identity Management. Each company maintains its own repository with accounts and its identity attributes, and identifies each user properly when required.

Some of the benefits of the federated approach are:

- Enhanced User experience - simplifies and enriches user experience through SSO, SLO, account linkage and service integration.
- Privacy protection - prevents exchange of sensitive credentials and user attributes.
- Service aggregation - enables access to multiple service partners.
- Content delivery - enables delivery of content from multiple sources.
- Advanced advertising - increases ad value through analytics of data from multiple sources.
- Rapid time to market - enables rapid linkage to service and content sources.
- Leveraged business expansion - enables accelerated growth in delivery capacity and subscriber demand.
- Foundation for future innovation - enables advanced automation.

Some models have arisen that propose a federation with a central well-trusted and reliable third party organization that both parties collaborating know and rely on. This federation model is proposed, for instance, by the Liberty Alliance [LIBERTY], among others. Next subsections describe some of these initiatives and also a lighter but similar approach that has recently come about in the Internet, OpenID [OPENID].

3.5.2.1 Security Assertion Markup Language

The Security Assertion Markup Language (SAML) [OASIS-SAML] is a specification from the OASIS Security Services Technical Committee. It defines an XML-based framework for communicating security and identity (authentication, entitlements, and attributes) information between computer entities.

It consists of a number of components that, when used together, permit the exchange of identity, authentication, and authorization information between autonomous organizations. The first component is an assertion that defines the structure and content of the information being transferred. How an assertion is requested by, or pushed to, a service provider is defined as a request/response protocol: ***SAML protocol***. A binding defines the underlying communication protocol i.e. HTTP Redirect, POST and Artifact, or SOAP, over which the SAML protocol can be transported. Together, these three components create a profile (such as Web Browser Artifact or Web Browser POST).

3.5.2.2 Liberty Alliance

The Liberty Alliance offers a comprehensive standards portfolio that enables identity federation and the providing and consuming of identity-enabled services. These features can be realized by using either traditional HTTP communications and Web browsers, or Web services technologies, and servers and clients based on Web services [Hirsch&06].

The Liberty approach associates service providers into trusted domains called ***circles of trust*** that are supported by Liberty technology and by operative agreements in which trust relationships are defined among providers (Figure 12). Inside a circle of trust, users can federate (link) isolated accounts that they own across different service providers (SP), also known as relying parties. Some entities could be especially prepared to

manage these federations, as well as providing some other ancillary services. They are called identity providers (IdP) and play a central role within the Liberty architecture.

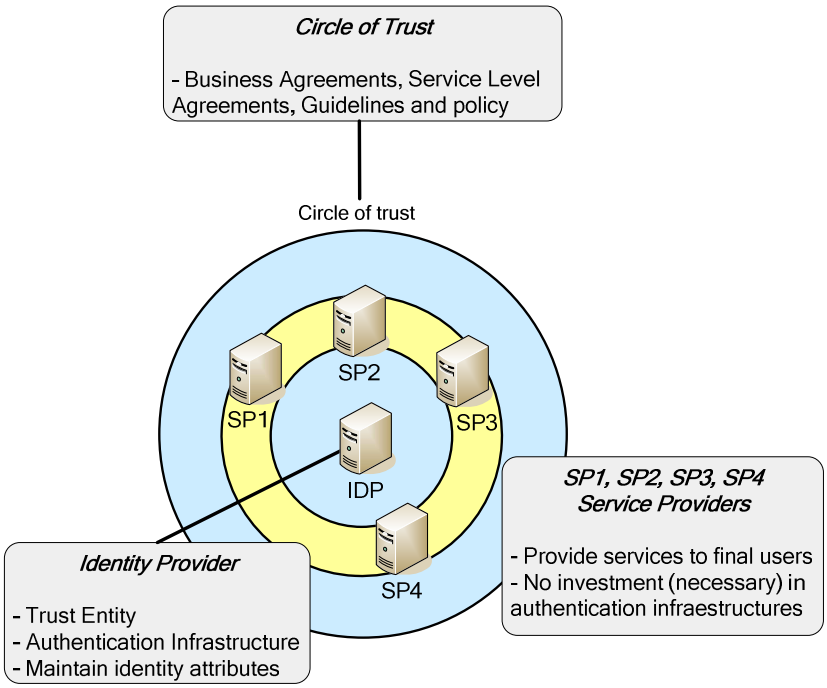

Figure 12 - Circle of Trust in Liberty Alliance Architecture.

Liberty Alliance divides the development of the standards and recommendations in three phases:

- ***Phase 1 – Identity Federation Framework (ID-FF)***. Protocols specification for identity federation, SSO, SLO and global name registration.
- ***Phase 2 – Identity Web Services Framework (ID-WSF)***. A Web services based framework specification for developing identity services: service description and discovery, authentication, shared attributes access, user interaction for privacy guidelines, etc.
- ***Phase 3 – Identity Services Interface Specifications (ID-SIS)***. Identity based specific services that make use of the framework defined in phase 2: personal profile, employee profile, contact book, geo-location, presence, and so on.

Liberty ID-FF version 1.2 was submitted to OASIS for inclusion in SAML 2.0 specifications. Additionally, support for SAML 2.0 was added in the second version of Liberty's ID-WSF specifications.

3.5.2.3 WS-*

OASIS and W3C have developed a set of standards under the denomination of WS-* that aim at providing a stack of specifications to create secure and reliable Web services, and also at providing support for identity management [Rosenberg&04]. Among others, the most important ones are WS-Security, WS-Trust, WS-Policy and WS-Federation.

Web services security (WS-Security or WSS) [OASIS-WSS] is a communications protocol providing a means for applying security to Web services.

WS-Trust [OASIS-WSTrust] is an OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security

tokens, as well as with ways to establish, assess the presence of, and broker trust relationships between participants in a secure message exchange.

WS-Policy [W3C-WSPolicy] is a W3C recommendation that allows Web services to use XML to advertise their policies (in different aspects such as privacy, security, Quality of Service, etc.) and for Web services consumers to specify their policy requirements.

Finally, ***WS-Federation*** [Lockhart&06] defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities are managed in other realms.

Both SAML and WS-Federation provide similar characteristics regarding federated identity and access management. The main advantages to choose one instead of the other are based on the organization guidelines and principles. However, it is worth noting that there are several industrial and open source implementations of SAML specifications while products supporting WS-Federation are beginning to appear. Moreover, SAML and Liberty specifications have converged in SAML 2.0 which is another advantage.

3.5.2.4 OpenID

OpenID is a new identity management system that has recently come about in the Internet. It proposes an approach for identity management lighter than the federated model but with some of its advantages. It is based on the same model than a circle of trust (there are an identity provider and some relying parties), but there are no established trust relationships between them.

To be authenticated a user signs on into an OpenID-enabled service provider using a Uniform Resource Identifier (URI). The service provider will redirect the user to the OpenID identity provider identified by that URI where the user will authenticate his or her identity. Once authenticated the identity provider will redirect the user to the original service provider. OpenID framework also provides the means for users to share their identity attributes.

The main advantage of the OpenID model is that it is very simple, and thus it could be easily used in Web sites where security considerations are not very important e.g. blog commenting in a controlled manner to protect against spam and misattribution. The main drawback of this model is that if the user provides the same URI to multiple relying parties then the user can be tracked. Nevertheless, the last version of OpenID (version 2.0) has solved this privacy risk.

For an in depth comparison among OpenID, WS-Federation, SAML and Liberty the reader can refer to [Ping07].

3.5.3 User-Centric Identity Management

User-centric identity management aims at enabling users to take a larger control of their digital identities and the processes related to them. Basically, these systems try to enforce user privacy and data protection. They could be based on two main models:

- Contractual: the authority promises the user not to misuse the data. Liability agreements and terms of use are related to this model.

- Technical: the software used to store and transmit user data encrypts and digitally signs it in such a way that is hidden from everyone except the sites at the endpoint with a need to know, and ***user decides*** when to allow this use.

In this work we will pay attention to the technical models. They can provide the following features among others:

- All user identities/attributes are self-asserted and provisioned. When a user provides a relying party with some attributes, the disclosure of these attributes to third parties requires user permission.
- All user identities/attributes are self-selected within the context of each interaction, and these interactions are engaged in by the user with full knowledge, transparency, and non repudiation of the relying parties.
- The user has a consistent user experience by using the same identity agent over and over for each identity transaction. Currently each service provider shows its own user interface which means the user is learning a new interface, sometimes just for one-time use (e.g. site registration).

Recently a set of technologies and tools have come about in the Internet to support the user-centric identity management paradigm. The next subsection describes the most relevant one, Windows CardSpace. Then, some other efforts are briefly mentioned.

3.5.3.1 Windows CardSpace

Windows CardSpace [Chappell06] is part of Microsoft's vision of an identity metasystem [MS-IDM]. It provides four main aspects about identity management: support for different digital identity systems, consistent user control of digital identity, replacement of password-based Web login and improved user confident in the identity of remote applications.

The basic use case for CardSpace is shown in the figure below (Taken from [Chappell06]):

1. First, the application (commonly a Web browser) gets the security token requirements of the relying party that the user wishes to access. This information is contained in the relying party's policy, and it includes things such as what security token formats the relying party will accept, and exactly which claims those tokens must contain. In a Web site, this relying party's policy is expressed with HTML tags.
2. Once it has the details of the security token this relying party requires, the application passes this information to CardSpace, asking it to request a token from an appropriate identity provider. CardSpace also includes a self-issued identity provider which runs on the local Windows system and can produce information cards just like any other identity provider.
3. Once this security token has been received, CardSpace gives it to the application, which passes it on to the relying party. Windows CardSpace is entirely agnostic about the format of the security token that is requested from an identity provider and passed on to a relying party. Therefore, CardSpace can work with any digital identity system.

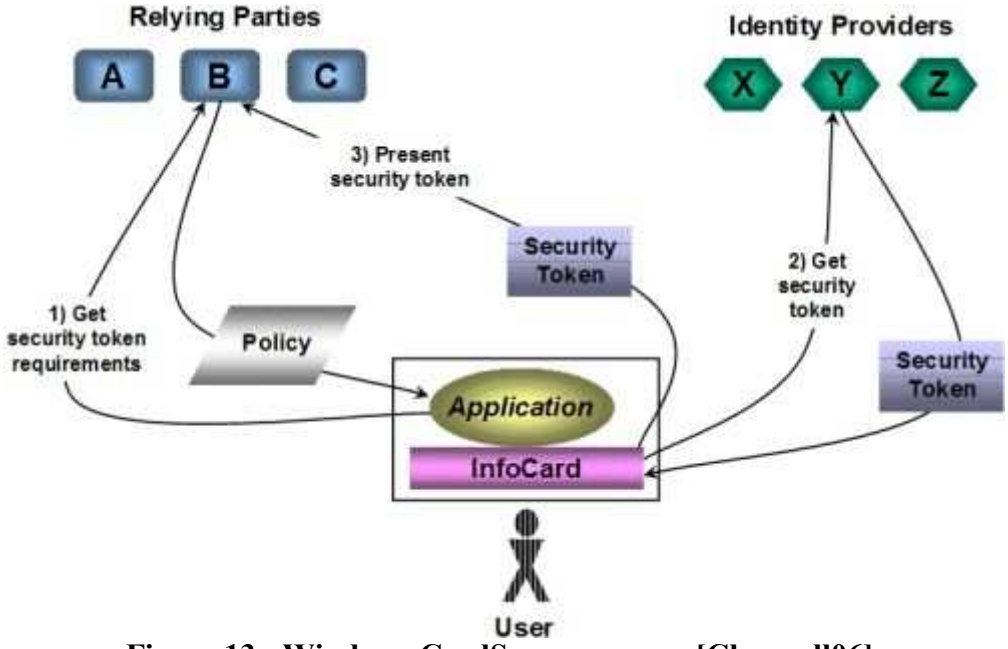

Figure 13 - Windows CardSpace use case [Chappell06].

3.5.4 Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. In a digital world, privacy is related to digital identity, and thus with the ability to protect or selectively disclose digital Personal Identifiable Information (PII), and to govern what others can do with that information.

Recently, user privacy has become one of the hot topics of the identity management arena. However, it lacks comprehensive frameworks in spite of the fact that all the identity management frameworks include built-in privacy features. For instance, when it comes to network-based schemas such as those of the Liberty Alliance, privacy is supposedly handled by the user at each service provider and, from that point on the service providers are responsible for meeting the user privacy settings and preferences.

Some research work has been done in the field though. For example, [Hommel06] introduces an integrated approach to privacy-aware identity management on both the user and the service provider side. However, this solution is valid just for Web-based interactions (user-driven) and thus not suitable for our Telecommunications-oriented context because users could be offline at the time of privacy enforcement. Additionally, Ahn and Ko [Ahn&07] proposed another solution for user-centric privacy management for federated identity management. Unfortunately, this proposal does not define mechanisms to centrally handle privacy policies by end-users themselves, which is a must in a user-centric environment.

Next subsections describe the state of the art regarding privacy management. First, different means to represent privacy information are analyzed and compared. Then, the Liberty and CardSpace approaches to privacy management are introduced and they feasibility for user-centric service creation and delivery platforms is assessed.

3.5.4.1 Expressing privacy information

There are different means to express privacy, but in a digital world privacy is usually expressed by means of privacy policies. For the goals of this dissertation we focus on

XML-based languages that can be used in a Web-services context to express these privacy policies e.g. XACML, WS-Policy, P3P, CARML, etc.

XACML stands for eXtensible Access Control Markup Language [XACML]. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies. XACML is used to describe general access control requirements and conditions. Lately, a WS-XACML profile has been specified.

WS-Policy [W3C-WSPolicy] is a W3C specification that allows Web services to use XML to advertise their policies and for Web service consumers to specify their policy requirements. WS-Policy also describes how to associate policies with services and end points. WS-Policy main advantage is that it is able to describe any kind of policy (privacy, security, QoS), but for the same reason there is no specific description of privacy information. Thus, using WS-Policy alone implies that we should create our descriptions for privacy constraints.

The P3P (Platform for Privacy Preferences Project) [W3C-P3P] is a framework that allows PII consumers to declare, in a XML-based language [P3P], what information they collect about users and their intended use. P3P is complemented by APPEL (A P3P Preference Exchange Language) [APPEL]. Using APPEL a user can express her preferences in a set of preference-rules, which can then be used by her user agent to make automated or semi-automated decisions regarding the acceptability of machine-readable privacy policies from P3P enabled Web sites. The main disadvantage of P3P/APPEL is that it is focused on Web development. However, some APIs are available which allows using P3P in a Web-services context.

Oracle, through the Liberty IGF initiative [LibertyIGF], has proposed two draft specifications that allow expressing complementary privacy information: the Client Attribute Requirement Markup Language (CARML) [Hunt06] and the Attribute Authority Policy Markup Language (AAPML) [Mishra06]. A CARML document is an XML document format that allows applications consuming identity-related data to declare identity data requirements and intended usage for PII. On the other hand, AAPML is a XACML profile designed to allow identity service providers to specify conditions under which information under management may be used (and possibly modified) by other applications. The combination of CARML and AAPML allows for a great control on the flow of PII between providers and consumers.

Next table summarizes an assessment of the suitability of the evaluated policy expression languages to 5 different types of privacy policies, as categorized by [Madsen&06].

Table 3 - Comparative between XML-based privacy expression language.

	User privacy preferences	Service privacy statement	Service acceptance rules for identity attributes consumption	Service governance rules for the use and release of identity attributes	Service conditions upon attribute release
P3P	No	Yes	No	No	No
APPEL	Yes	No	No	No	No
XACML	No	No	Yes	Yes	Yes
CARML	No	Yes	Yes	No	No
AAPML	No	No	No	No	Yes
WS-Policy	Yes	No	No	No	Yes

3.5.4.2 Liberty Alliance approach to privacy

Liberty specifies that each entity is responsible for the privacy of the information it stores, understanding privacy in this case as the service governance rules for the use and release of identity attributes. For example, it is stated that a Liberty entity will verify the entity requesting identity information against an access control list to ensure that it has been granted access to the requested attribute. As for the information custodians, they must check whether the resource owner has given consent to return the requested information.

Although the specific means to specify such consents are not described some initial guidelines based on a multi-level labelled approach have been described in [LibertyPrivacy]. Users and attribute requestors can describe their privacy policies using labels; each label corresponding to a specific privacy policy described using P3P vocabulary (although the policy itself does not have to be a P3P policy). Labelling defined privacy policies allows users for easier understanding and selection of their policies. And as for the custodian it is easier to compare a limited set of policies which are labelled following a hierarchical structure.

Additionally, in the Liberty ID-WSF dialogue participants may indicate the privacy policy associated with a message by adding one or more <*UsageDirective*> header blocks to the SOAP header. Essentially, the usage directives header contains elements that describe the privacy policy associated with the request (privacy statements made by the information requestor) or the response (conditions upon information release). The usage directive in a request from a client can be understood as "*intended usage*" or "*policy promise*" (Requestor's privacy policy). The usage directive in a response can be understood as a directive which governs subsequent use and release and describes how data is to be used (Custodian's obligations).

Lately, some drafts have been added to the Liberty site regarding the Liberty Identity Governance Framework (IGF) [LibertyIGF]. IGF aims at describing in depth a small set of privacy constraints and the mechanisms to interact with them. Privacy constraints describe fundamental constraints on the propagation, usage, retention, storage and display of identity data both on the consumer and the provider sides. Liberty IGF uses WS-Policy as the means to describe privacy constrains and provides some specifications to describe obligations imposed by the provider and promises offered by the consumer.

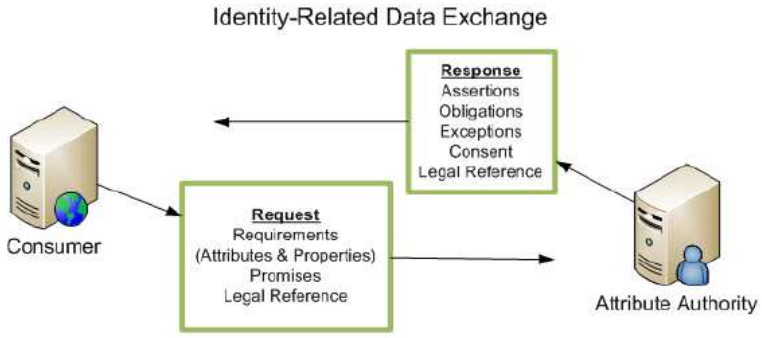

Figure 14 – Liberty IGF basic scenario [LibertyIGF].

3.5.4.3 Windows CardSpace approach to privacy

CardSpace delegates all the privacy decisions to the user. Information Cards are designed so that before a user acquires a particular card, he will see a link to the privacy policy of the identity provider describing how any personal data submitted will be used. Similarly, before a particular card is deployed to a relying party, the user will see a link to the relying party's privacy policy and can learn whether the relying party intends to use the data for purposes beyond identity verification.

The parameters to the OBJECT and XHTML Information Card objects are used to encode information in HTML that is otherwise supplied as WS-SecurityPolicy information via WS-MetadataExchange when an Identity Selector is used in a Web services context. For the privacy policy they are:

- *privacyURL (optional)*. This parameter specifies the URL of the human-readable privacy policy of the site, if provided.
- *privacyVersion (optional)*. This parameter specifies the privacy policy version.

CardSpace approach to privacy forces users to check the privacy policy of every single site they are visiting. While this approach ensures user control, it is probable that most users skip this checking because of its nuisance.

3.5.5 Regulatory requirements regarding identity information

Proper identity management is essential in every new Telecommunications service that is implemented or provided in Europe. Furthermore, it is obligatory because of restrictions and legal constraints derived from several European Directives:

- European Union Data Protection Directive [EU2006-24];
- European Union Electronic Communications Privacy Directive [EU2002-58];
- European Union Data Retention Directive [EU1995-46].

Within the Data Protection Directive, personal data is defined as information that relates to an identified or identifiable natural person. The processing of personal data is defined as any operation or set of operations that is performed on personal data, such as collecting, storing, disseminating, and so on. The different dimensions of data protection are:

1. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

2. Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. This can be seen as part of the privacy principle of data minimization, which can be seen in two ways:
   - Avoid that private date might appear scattered in multiple places in the network.
   - Ensure that a unique unit of private data is provided to a certain requester, and not a set of it which may include more private information that the one that is needed.
3. Personal data may be processed only if the data subject has unambiguously given her or his consent.

The aforementioned requirements from the main European Directives regarding identity management must be considered when designing any Telecommunications service and, of course, when designing the systems that will manage those services.

3.5.6 Identity Management Forums

There are a huge set of organizations that work on different aspects of identity management. In this section we just describe a small subset that includes those which are related with the aim of this work.

ITU-T Identity Management Focus Group [ITUT-FGIdM]**.** The scope of the Focus Group is identity management for Telecommunications/ICT in general; and specifically to facilitate and advance the development of a generic identity management framework and means of discovery of autonomous distributed identities and identity federations and implementations. Part of the work involves the creation of a list containing details of identity management work in standards bodies, forums, and consortia.

3GPP [3GPP]**.** 3GPP has developed specifications related to subscription management, user profiles, and Liberty specifications and 3GPP security interworking.

Liberty Alliance Project [LIBERTY]**.** Liberty has specified an open standard for federated network identity that is intended to support current and emerging network devices, offering a secure way to control digital identity information.

OASIS [OASIS]**.** It has developed several specifications related to identity management including SAML, SPML and WS-Security.

Open Mobile Alliance [OMA]**.** It has developed a document containing requirements for an identity management framework which will allow integrating existing efforts relating to identity within the OMA to create a single identity management enabler to be used by all OMA enablers.

World Wide Web Consortium [W3C]**.** It has developed some recommendations for XML aspects of identity management such as P3P.

Concordia [CONCORDIA]. The Concordia project is a global initiative designed to drive interoperability across identity protocols in use today. It does this by soliciting and defining real-world use cases and requirements for the usage of multiple identity protocols together in various deployment scenarios, and encouraging and facilitating the creation of protocol solutions in the appropriate "homes" for those technologies.

Future of Identity in the Information Society (FIDIS) [FIDIS]. This European Network of Excellence aims at shaping the requirements for the future management of

identity in the Information Society and contributing to the technologies and infrastructures needed.

Privacy and Identity Management for Europe (PRIME) [PRIME]**.** PRIME aims to develop a working prototype of a privacy-enhancing identity management system. The PRIME project receives research funding from the EU's Sixth Framework Programme and the Swiss Federal Office for Education and Science.

3.5.7 Section summary and conclusions

User-centric service creation and delivery platforms face great challenges when it comes to the management and operation of the information associated to the digital identities of their users. This section has provided the reader with a description of the bases underpinning identity management and privacy control, which are the disciplines needed to deal with these challenges.

A description of all the processes involved in the management of a digital identity has been provided. The state of the art of the solutions that address cross-domain identity management has been detailed as well as those relevant solutions for user-centric identity management. An assessment of these technologies has been conducted too, in order to select those that better fit the requirements of a user-centric service creation and delivery platform. In addition, the technologies that support privacy protection have been analysed, and the different solutions have been compared. Finally, a summary or the regulatory requirements that must govern the use of identity information has been provided.

Due to the nature of user-centric platforms some consumer's identity attributes must be shared with the providers collaborating and some specialized providers may deliver services with identity-based information. As we have seen legislation states that users must be informed and provide consent on the use of their attributes when shared among different companies and therefore there is a need in user-centric platforms to provide mechanisms that support sharing identity information while allowing users to control and govern its use and release i.e. identity and privacy management. As long as the author has checked these requirements have not been properly addressed in the literature, and thus they will be among the goals of this doctoral thesis.

3.6 Chapter summary and conclusions

The new converged, NGN- and multimedia-based world is very different from the one in which traditional Business and Operations Support Systems (B/OSS) managed just connection-oriented services within a single administrative domain. Management of new products and services is also more complicated due to shorter lifecycles, the user-centricity of new services, the openness and sharing of the owned resources, partnership management, legal requirements for the collection, maintenance and processing of customers' personal information, and so on, and so forth. Therefore, current management and operation systems are not just in charge of network and hardware management, but also of a huge multimedia service ecosystem and its support systems and processes, some owned by the company but many other belonging to third parties such as partners or even the users themselves.

Summarizing, the focal point of service management is now shifting from traditional network service management to the management of the user-experience. Therefore, provisioning and fulfilling next-generation converged products and services across communications and IT domains requires next-generation management and operation

systems and processes combined with organizational transformation. As stated in [Dickerson&04], "*The OSS of the next generation network will provide a radically enhanced customer experience in which customers can provide and manage their own services in an easy-to-use environment*".

Motivated by this context this chapter has described, assessed and analyzed the different technologies and solutions that can support user-centric service creation and delivery platforms over NGN. For that, the state of the art of NGN and its realization as the IMS have been described. The bases supporting the openness of these networks to third parties have been detailed focusing on SOA and its use in Telecommunications, the current status of Service Delivery Platforms, and the new Web paradigms for service creation such as User-Generated Content and User-Generated Services.

The requirements that these new paradigms pose to the management infrastructure have been used to analyze and assess the state of the art of current solutions for the management and operation of service creation and delivery environments in Telecommunications. The standardization initiatives in this field have also been considered but unfortunately their current status does not provide solutions for our requirements. This is especially important when it comes to the management of identity information and the privacy protection of users, since current technologies and solutions do not properly address how to let users govern the use and release of their identity information when different entities are collaborating in a SOA environment. The original contributions of this doctoral thesis aim to cover the detected lacks.

4 USER-CENTRIC SERVICE CREATION AND DELIVERY

Traditional paradigms for digital service creation and delivery have usually involved specialized roles such as service producer, service aggregator and service distributor. Lately, new applications have come about in Internet within the so called Web 2.0 paradigm. These applications allow non-technically skilled users to create and manage their own digital contents i.e. User Generated Contents (UGC). The contents might be shared within a virtual community, where they are recommended and consumed by any user connected, promoting the most interesting ones at a minimum cost (viral marketing[4]), thus realizing paradigms such as The Long Tail [Anderson06].

Despite being relevant, UGC do not allow interactivity, and thus users are constrained to be just passive spectators of the provided information. The spread of technologies that allow contents mashups provides users with powerful means to aggregate and filter contents, thus obtaining the contents that better fit their needs. This process was possible due to the existence of open interfaces provided by Internet content providers.

Trying to emulate Web 2.0 success, the very same process has been ported to the Telecommunications domain. Nowadays, more and more telecom operators provide developers and third parties with interfaces to their network resources, thus allowing them to create advanced telecom services. Moreover, the convergence of Internet and Telecommunications networks around the Internet Protocol (IP) to create the Next Generation Networks (NGN) is fostering the emergence of environments where telecom features are available to Web services. Furthermore, since users *wear* mobile devices connected to telecom networks, these are able to provide reach context information about users such as location, presence status, and so on.

Following Web 2.0 evolution, it is feasible that the openness of telecom network does not stop with professional developers creating services but that it is extended to non-technically skilled end-users. This will allow users to develop and share their own next generation converged services: User Generated Services (UGS).

Under this new service creation and delivery paradigm the value chain is shortened, eliminating intermediation in the creation and distribution processes. This allows creators and consumer to be in contact. Service creation and delivery platforms provide an open marketplace where resource providers, service creators and service consumers can meet, thus enabling a dynamic ecosystem of services and resources. This provides benefits for all the actors involved.

Next sections describe the business and technology basis underpinning user-centric service creation and delivery platforms, and the paradigms they are based on. The chapter concludes with an overview of a high-level architecture of one of these platforms. We will use this architecture as a framework useful to explain the contributions that this dissertation aims to provide.

4.1 Business context

This section provides the overall business context needed to better understand the motivation and goals of this dissertation. With that aim we first introduce a business

[4] Viral marketing refers to marketing techniques that use pre-existing social networks to produce increases in brand awareness, through self-replicating viral processes, analogous to the spread of pathological and computer viruses. It can be word-of-mouth delivered or enhanced by the network effects of the Internet. [Source: Wikipedia].

motivation for user-centric service creation and delivery platforms. Then we analyze existing business models for service provision in Telecommunications. Since traditional business models do not fulfil the requirements we set for a user-centric service creation and delivery platform we propose and describe a new business model.

4.1.1 Innovation and user-centric service creation and delivery platforms

Open innovation is a term promoted by Chesbrough [Chesbrough05]. The key goal behind this concept is to help enterprises in advancing their business by making the most of their innovation processes. It is based on the idea that in a world of widely distributed knowledge, companies cannot afford to rely just on applying their own (limited) research to their own business model but they rather should be permeable to innovation both outwards (inside-out) and inwards (outside-in) (**Figure 15**).

The principles behind open innovation are twofold. On the one hand, enterprises practicing outside-in innovation work with external entities collaborating to bring new ideas into the company innovation process. For example, enterprises buy or license processes or inventions (e.g. patents) from other companies in order to incorporate them to their core business model, thus enhancing it. On the other hand, internal inventions not being used in a firm's business should be taken outside the company e.g., through licensing, joint ventures or spin-offs, thus monetizing the innovation activities carried out.

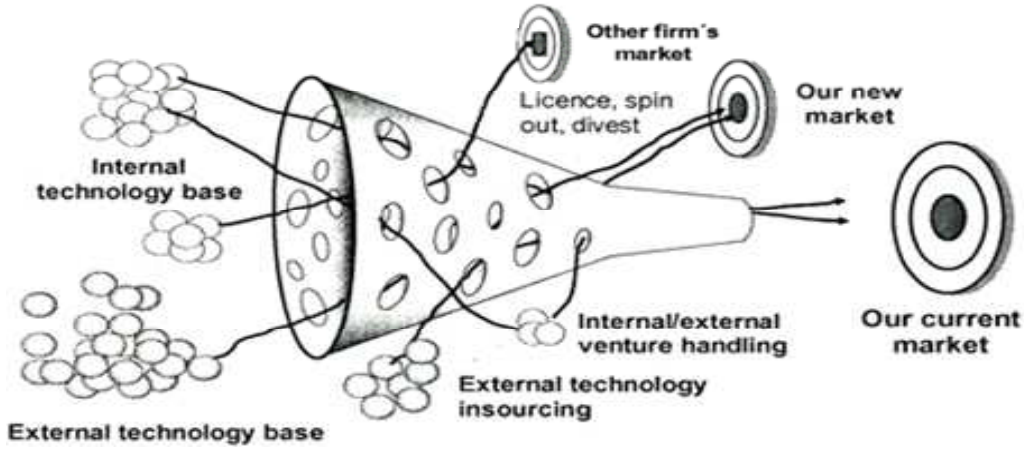

Figure 15 - Open Innovation [Chesbrough05].

User innovation is a concept introduced by Eric von Hippel [Hippel94] [Hippel06] that refers to innovations developed by consumers and end-users, rather than by enterprises. Von Hippel discovered that most products and services are actually developed by users, who then give ideas to manufacturers. Since manufacturers develop products to meet the widest possible needs, when individual users face problems that the majority of consumers do not they have no choice but to develop their own modifications to existing products, or entirely new products, to solve their issues.

Von Hippel refers to innovators as *lead users* and characterizes them. Lead users of a novel or enhanced product, process, or service face needs that will be general in a marketplace, but face them month of years before the bulk of that marketplace encounters them; and they expect to benefit significantly by obtaining a solution to those needs.

Sometimes, lead users can be identified and drawn into a process of joint development of new product or service concepts with a company. The innovations can be obtained by different means e.g. innovators can be provided with toolkits that directly allow them to innovate or they can provide feedback that may be used to improve processes, tools and products, or to gather new ideas for future developments. In any case, innovators provide invaluable inputs for outside-in open innovation. **User-centric service creation and delivery platforms** provide the means to incorporate user innovation into open innovation processes.

The motivations for lead users to join the platform might be as simple as that they get new services that can fulfil their specific needs. However, other lead users might need further incentive to innovate and thus voluntarily reveal their innovations e.g. a percentage of the revenue obtained by the services commercialization. Of course, integrating the new services benefits also the platform provider business since new innovative services will be commercialized.

4.1.2 Telecom business models

The Telecommunication Information Networking Architecture Consortium (TINA-C) [TINAC] states in [Yates&97] that ***a business model defines the different parties involved in service provisioning and their relationships***. Based on this definition, we analyze in this section different telecom business models. We assess them according to a general set of requirements to support user-centric service creation and delivery:

- ***End-user service creation*** – The first requirement is that the business model should support end-user service creation. This will allow end-users to compose their own services from the set of resources that is already offered within the platform.
- ***End-user service provision*** – The business model should allow extensions to accommodate end-users in the service provision. Once end-users create new services, they will probably want to provide end-users with them.
- ***End-user service execution*** – The next requirement is that end-user service execution should be allowed.
- ***End-user service recommendation*** – Finally, the business model should allow users to recommend services to other users. This will contribute to the success of a set of high value services from among the great amount of services that are to be created within the platform. These frequently recommended, high value services will actually provide added value to users, and might turn out to become a kind of killer services [Anderson06] in the long tail.

On the other hand, the following business models are commonly applied to service provision in Telecommunications.

Walled garden – Business models for telcos have traditionally followed the walled garden paradigm [Afuah&01]. The goal has always consisted of subscribers getting everything they wish (services and contents) in the operator's portfolio. Access to outer services is not allowed and third party service providers, if any, appear under the operator's brand name. All revenues go directly to the telco from its customers.

The rationale of this business model is that the user is served better and the service is more profitable for the provider. A Telecommunications operator has some elements that lend considerable power to do so i.e. a large customer base, knowledge of the

subscriber's location, billing relationship to the customer and customer services and marketing reach. In fact, this model is restricting the user experience, for instance restricting browsing out of the operator domain or choosing service position on the menu. Nevertheless, the walled garden reduces the number, and limits the activities, of participants in a marketplace.

Bit pipe – The bit-pipe approach [Cuevas&06] describes the operator network as bit pipes that allow its customers to access services with neither constrains nor added value. The operator gets its revenue from the use of the network. Users may choose from the set of services offered by third parties in the Internet. They pay for the services following the service provider terms and conditions, which may differ from provider to provider. Quality of Service (QoS) is not checked by the operator, and thus not ensured. The management of identity information and the privacy and data protection is up to each service.

Semi-walled garden – Within this business model customers stay inside the operator's walled garden but they are free to choose and enjoy third party services and contents. The revenue is divided between the operator and the provider.

The network operator and the service provider work together in a team to build a value chain that produces services which may be interesting to end-users, thus providing some revenue to each member in the chain. Similar to the walled garden case, it is the operator itself who carries out the service recommendation by suggesting as trusted and directly accessible from the service menu those services which belong to selected third parties. The order in which services are prompted to the users determines the actual service recommendation. This order is usually based on off-line agreements between the operator and the corresponding service providers.

Operators can also offer value-added service enablers that are attractive to third party providers thus encouraging the partnership between them: some are related to the Telecommunications infrastructure (e.g. QoS, SMS service or setting up calls), and other to users' identity (e.g. authentication, billing, presence, location or address books).

i-mode [Baker&01] is the best example of a semi-walled garden business ecosystem. It has some limitations though: there is just one billing and subscription model, and the service provider revenue from each service is limited. Nonetheless, there is an increasing movement in the Telecommunications service provisioning arena towards the semi-walled garden business model or some of its slight variations.

The previous business models are analyzed in **Table 4** with respect to the proposed requirements for a user-centric business model.

Table 4 - Analysis of Telecommunications business models.

Requirement	***Walled garden***	***Bit pipe***	***Semi-walled garden***
End-user service execution	Yes	Yes	Yes
End-user service creation	No	No	No
End-user service provision	No	No	No
End-user service recommendation	No	Yes (externally)	No

None of the main business models for Telecommunications satisfy the requirements related to end-user service creation and delivery. The best approach, the *semi-walled garden,* lets third parties to take part in the business by developing services that the customer could use within the framework provided by the *walled garden*, and that is a first step on the right path. However, the process to become a third party is long and tedious and is not feasible for end-users.

Nevertheless, an evolution of the business model is needed which will make it possible also for customers to create, share and recommend their own services. This is the particularity of the business model we present; the fact that the customer performs now other roles in the business model apart from the passive service consumer.

4.1.3 A business model for user-centric service creation and delivery

To begin with the description of the proposed business model we present the entities that participate, their roles and their relationships. For that we follow the business model definition given by TINA-C.

Once we have described the basis of our business model proposal, then we articulate the value proposition, identify the market segment, define the structure of the value chain, describe the value network and specify the revenue generation mechanisms. For that we follow Chesbrough's definition of business model [Chesbrough05].

4.1.3.1 Entities, roles and relationships

Three main entities participate in our business model: end-user, platform owner and third party provider. The platform owner provides and maintains the user-centric service creation and delivery platform. It may also provide some resources with basic functionality e.g. send a SMS, set up a call, retrieve a presence status or a location, and so forth. End-users may execute the services available, but also create and share their own services. Some third parties might also participate in this business model, providing specialized resources useful for composition on the operator's platform.

The relationships between the different entities and their roles in the business model are detailed in the following figure.

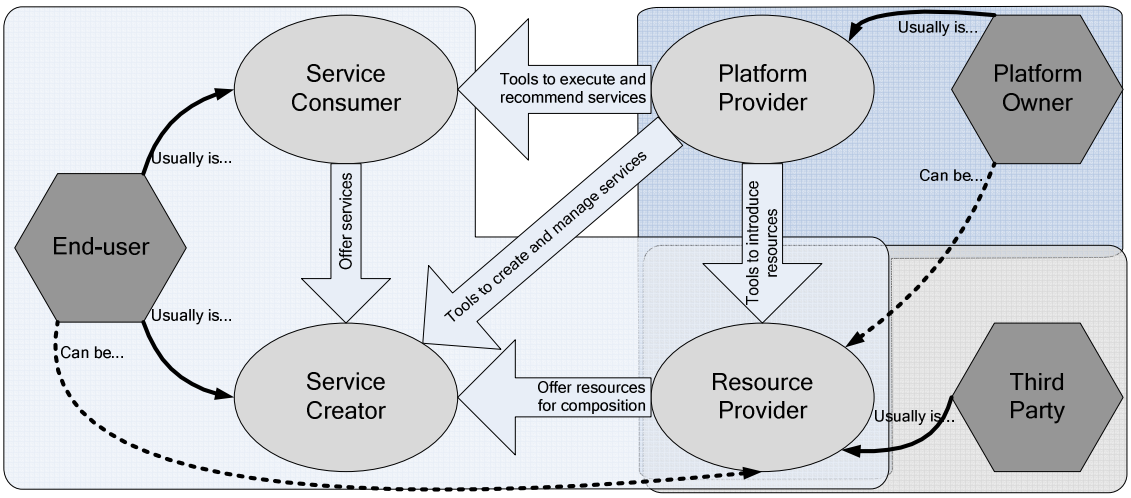

Figure 16 - Entities and roles in a user-generated service business model.

The roles played by the different entities are: platform provider, service consumer, service creator and resource provider. The end-user may play the role of service consumer, service creator and resource provider. The difference between service creator and resource provider is that the former offers services to consumers, while the latter offers its resources to other service creators for combination. The platform owner usually plays the role of platform provider, but as we have said it could also provide its own resource portfolio for combination thus becoming a resource provider too.

The platform provider supplies all the features that enable the creation, the management, the provision, the execution and the recommendation of services. It is also involved in the economic flows between the different members (creators, providers and consumers). Moreover, as any software platform it provides a marketplace for resource providers, service creators and service consumers to meet, acting as an intermediary and reducing the transaction costs for the two groups [Evans&06].

Service creators find that a service is needed and useful (for themselves or for any other member of the community) and have the necessary skills and tools to create it from the set of resources already available within the platform. Once the service is created and deployed on the platform it will be available to be used by service consumers. Successful services may also be used as resources in further compositions, thus service creators may become resource providers too.

It may be possible (probable) that the same end-user plays two roles at different times: end-users can execute services created by someone else and in this case they are acting as service consumers, but they can also create their own services that better fit their needs and in this case they are acting as service creators. Henceforth, we will use the term *prosumer* to refer to the actors that play this twofold role.

4.1.3.2 Value proposition

To articulate the value proposition wee need to define what the product offering is and in what form a customer may use it. In the context of a user-centric service creation and delivery platform the product offering is the platform itself, the services that are delivered through it and all the tools and applications that the platform includes.

Now we must define the customers of the platform and how they use it. In the previous section we have already defined the actors of the platform and their roles. We set the platform customers as all the roles that use the platform and get some benefit for it i.e. resource providers, service creators and service consumers.

Resource provider value – Resource providers use the platform to deliver enablers that can be used by service creators to compose new services. Thus, they use the platform as a distribution channel for their products and thus gain an intensive use of their resources at a low risk.

Service creator value – Service creators use the platform to create new services that fit their needs and fulfil their requirements. Service creators may also use the platform as a distribution channel thus selling their services through it. The platform provides an extensive base of consumers and low risk in the investment.

Service consumer value – Service consumers use the platform to look for new services, subscribe them and enjoy them. The two main factors for the value perceived by the customer are the prize and the response time. The level of personalization and the chance of sharing them are also taken into account. Other factors that can be identified are the service effectiveness and the service usability.

4.1.3.3 Market segmentation

To identify a market segment we need to profile the potential customers the platform targets. We base our findings for service creators and service consumers on Forrester's Research Technographics surveys [FORRESTER], which classifies customers into six overlapping levels of participation according to how they use social technologies. The six Forrester's groups are defined as follows:

- *Creators* – They make social content go. They write blogs, publish their own Web pages, and upload the contents they create e.g. video, music or text.
- *Critics* – They respond to content from others. They post reviews, comment on blogs, participate in forums, and edit wiki articles.
- *Collectors* – They organize content for themselves or others using RSS feeds, tags and voting sites.
- *Joiners* – They connect in social networks like MySpace and Facebook.
- *Spectators* – They consume social content including blogs, user-generated content, podcasts, forums, or reviews.
- *Inactives* – They neither create nor consume social content of any kind.

Next figure shows how participation varies among different groups of European customers according to the age. The chart in the right-bottom corner shows the average participation.

Figure 17 - Customers participation in social technologies [FORRESTER].

We have taken advantage of this information to profile customers of user-centric service creation and delivery platforms. We identify our service creators as Forrester's creators and our service consumers as Forrester's spectators, and thus we consider that they inherit the characteristics of Forrester's groups. However, service creators and service

consumers of user-generated services have an additional characteristic since they are in the context of a convergent network i.e. they are medium/advanced mobile users able to setup phone calls, send SMS and MMS, and use the device gadgets such as the camera or the multimedia player.

On other hand, we still have to profile resource providers, which is our third group of customers. We consider that any Internet and/or telecom service and content provider that provides its services currently in the Web might become a resource provider of user-centric service creation and delivery platforms.

4.1.3.4 Value chain

A value chain is required to create and distribute the offering, and to determine the complementary assets needed to support the platform owner position in this chain. Knowing the intended market and the value proposition, we can construct the value chain that will deliver these elements. The value chain must achieve two goals: first it must create value throughout the chain delivering that value to customers, and then it must allow the platform owner to claim some value from the chain to justify its participation.

In our case, the value chain allows providers to introduce resources, and supports creators in composing them into new services that are delivered to consumers. Therefore the roles that add value in this value chain are the platform owner that provides the platform, the resource provider that provides resources, and the service creator that creates services that can be delivered. There are no intermediaries between the service creator and the service consumer, except the platform. Therefore the traditional value chain for service provisioning has been shortened to put creators in touch with consumers via a simplified channel. This new channel should have the means and the tools to simplify the delivery of resources, the creation of services and their consumption.

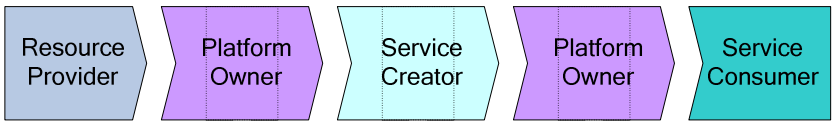

Figure 18 - User-centric service creation and delivery value chain.

4.1.3.5 Value network

A value network is an evolution of the traditional value chain. Value chains are quite simple, assuming a linear value flow and unidirectional relationships from raw material providers to manufacturers to suppliers and finally to customers. The real world is fairly more complex and there are many-to-many relationships among the actors involved in a business model that are not accurately described by a value chain. Therefore, value chains have evolved into value grids also known as value networks, which are characterized by a complex web of direct and indirect ties between various actors, all delivering value either to their immediate customer or to the end-consumer.

An example of use of the value network approach is *relationship management*: Relationship management typically just focuses on managing information about customers, suppliers, and business partners. However, a value network approach considers relationships as two-way value-creating interactions, which focus on realizing value as well as providing value.

[Basole&08] introduces a conceptual model for service value networks characterization. This model proposes the use of node-and-arc representation as a common method to visualize and describe value networks: nodes represent actors and arcs represent relationships or ties between actors. Value is created through a complex set of business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) relationships, and influenced by the social, technological, economic and political context in which it is embedded. We have followed this approach to characterize a user-centric service creation and delivery platform as a value network (**Figure 19**).

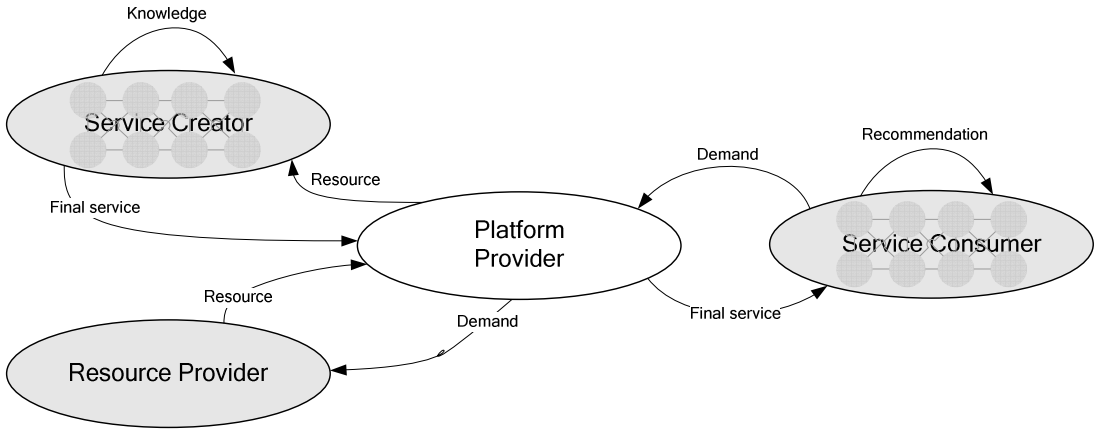

Figure 19 - User-centric service creation and delivery platform value network.

First we must note that value networks help to increase the supply of resources on the providers' side and the delivery of services on the creators' side. Traditional network businesses base their value on the number of participants that take advantages of their features. A user-centric service creation and delivery platform is a network business as well, and thus it is important for its success to have as many members as possible. This will allow the flow of services being shared between service creators and service consumers to increase.

However, end-users are the ones that play a fundamental role in our value network. First, consumers demand customized services thus driving the value creation. Additionally, they can be linked together through social activities such as knowledge sharing and service recommendation, thus creating the most benefit for the people involved in the network. Knowledge can be shared among creators to create the best situations or opportunities, and to stimulate user innovation thus improving open innovation. Service recommendation filters really valuable services from the huge amount of worthless (unprofitable) services, thus highlighting potential killer (profitable) services in the long tail [Anderson06]. On the end-user side, value networks enable ideas to flow into the market and provide the means to the people that need to hear them.

4.1.3.6 Revenue generation mechanisms

Now we are ready to define the architecture of the revenues i.e. how platform's customers will pay and how the value created will be apportioned between service consumers, service creators, resource providers and the platform provider itself. There are many options depending on the business policies of each actor.

Two models are usually applied to software platforms in order to distribute the cost of software development: either the user pays or developer pays. We think that user-centric service creation and delivery platforms will follow a similar path to PC operating

systems (the user pays) with slight variations: Unlike the operating system model, all consumers will be allowed to freely access the platform. Consumers will have to pay for some (premium) services consumption. Quite in the same way, resource providers will be freely allowed to offer their services, although they will be charged for the consumption of some specific features such as payment intermediation. Finally, creators will have to pay to use some special services in their compositions but they will be allowed to receive some revenues for the consumption of their services.

It is worth noting that the critical moment for the revenue generation mechanism, and also to the business model, is the launch of the platform as all the actors may be reluctant to invest in a new idea unless there is a substantial installed base of creators, consumers and providers. However, telecom operators have a privileged position to play the role of platform provider as they do already have this base of customers.

Figure 20 shows the flows of revenue between different roles. The consumer pays the platform under different billing plans (monthly fee, pay per use, etc). It could be determined by means of the nature of the service. Service creators and resource providers might pay the platform an engagement fee, which allows them to use the tools and mechanisms for service creation and resource delivery. This model is similar to the one successfully implemented by Apple, which charges an entrance fee to developers willing to create new applications for iPhone and to offer them in the AppStore.

Service creators might receive some revenue, which can be proportional to the number of consumers of their services (this is a revenue-sharing model, but their might be others depending on the service itself). In turn, service providers perceive their revenues from the platform, for example by agreements on percentages for each service they are part of.

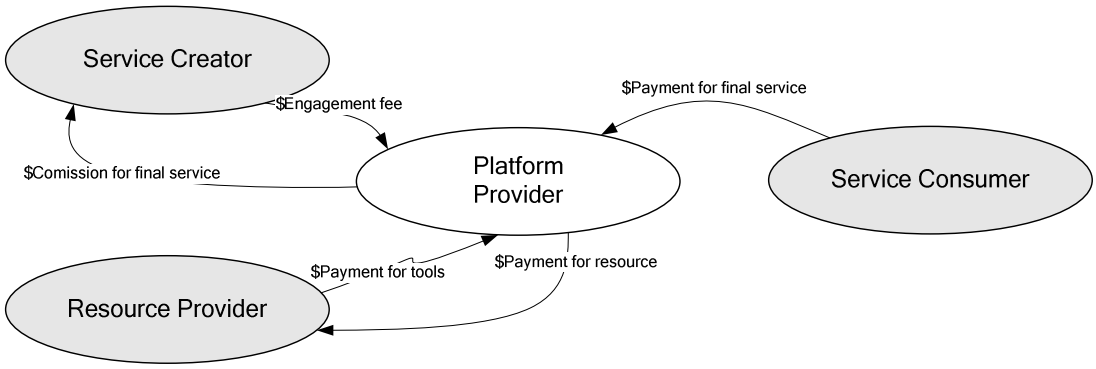

Figure 20 - Revenue flows in the proposed business model.

If consumers perceive the service as valuable, the platform provider and the service creator receive intangible benefits such as customer loyalty (the former), reputation (the latter) or trust (both). In turn, service creators find specific resources as valuable and thus some resource providers also benefit for better reputation and trust. It is worth noting that all these intangible benefits are received through the platform, which is the contact point for all actors, and therefore the platform provider always benefit for them too.

If tools are in place, consumers can also rate and recommend services to other consumers, thus increasing the knowledge among them. Besides, service creators might receive feedback from the consumers of their services that can be used to improve the services. Additionally, service creators might have tools that allow them to share their

expertise, thus increasing the global knowledge. All these benefits are increased by the network effects that the platform provides.

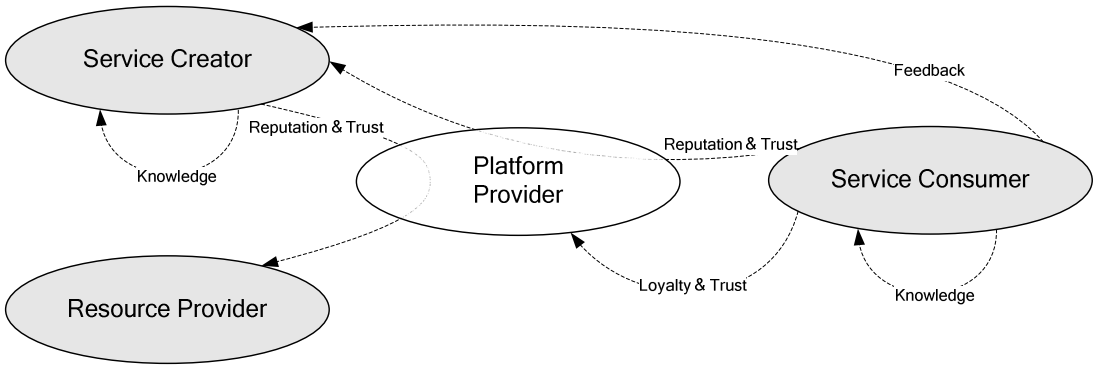

Figure 21 - Intangible benefits in the proposed business model.

4.2 Technological context

The key technological concept that supports user-centric service creation platforms is service composition: Service creators generate new services by the dynamic ad-hoc composition of available IT and Telecommunications resources. This section provides the reader with an overview of the technological context behind the terms *service* and *resource*. For that, we begin explaining the concept of resource and how it can be implemented in the platforms under study. Then, we describe how services can be created from resources.

4.2.1 Resource

In the context of this dissertation we define a resource as the functional unit available at the user-centric service creation platform that can be combined by service creators to generate a new service and that can be managed by the platform. Resources are atomic from the point of view of the service creator and the platform: they provide defined functionality but their implementation details are hidden.

A resource is made of two main parts: the resource adaptor or wrapper, and the resource implementation (**Figure 22**). The resource adaptor is the element that is introduced in the platform domain and that provides it with a common interface to the resource implementation. Resource adaptors will be used by the platform to invoke the resource functionality and to manage the resource lifecycle. Therefore, resource adaptors must provide a common interface to the platform even though each one deals with different resources and implementations: they homogenize the resources heterogeneity. Adaptors do not provide any functionality on their own, but they translate messages from the platform to the specific resource implementation and the other way around.

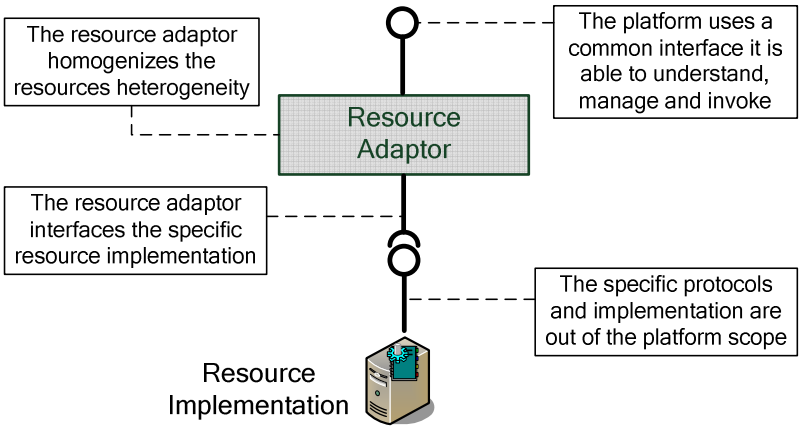

Figure 22 - Resource adaptor and resource implementation.

The minimum element that an adaptor must contain is a Web Service interface describing in WSDL the resource functionality. This technology has been selected due to its maturity and the availability of solutions. Complex adaptors might include software that translates the Web Service invocations from the platform into specific protocols used to communicate with the resource implementation. Adaptors may also install certificates that guarantee a secure communication between the resource adaptor and the resource implementation.

Resources are usually supplied by third parties both in the IT and the Telecommunications domains that open up their business to collaboration with the platform. Resources might be provided by the platform owner too, following the same rules applied to external resource suppliers. In the IT domain resources might be implemented for example using Java EE containers, .NET servers, or any other implementation technology, and the communication with the resource adaptor can be carried out by means of any desired protocol e.g. based on Web Services or REST technologies. In the Telecommunications domain resources may be implemented by means of JSLEE technologies, SIP application servers, or some other technologies that allow access to network capabilities such as IMS, OSA, CAMEL, etc. The communication with the adaptor could be supported by Web Services technology, SIP or some other protocol. In any case, the implementation and communications details are out of the scope of the platform.

From a technical point of view the inclusion of a new resource into the platform requires several steps. First the resource that provides the functionality must be created. This step is out of the scope of the platform. Then the resource must be introduced to the platform, creating a new resource adaptor. For that, the platform requests the provider all the information needed, and if required also specific components to install or deploy into the platform. Once all the information and components are available, the platform must validate the resource in different facets such as the interface, functionality, reliability and performance. If the validation is successful the platform prepares its modules for the management and operation of the new resource and it is made available. After that the resource can be published and promoted so that creators can easily find and use it in their compositions.

In order to allow the generation of a rich resource ecosystem the delivery of new resources must be easy, flexible and not expensive for resource providers. This process can be facilitated providing resource suppliers with a Resource Delivery Application, which guides and helps them throughout all the required steps.

4.2.2 Service

Services can be generated by service creators by combining resources in a syntactical correct way. Such combination may include sequences of components, conditional branches, forks and join operations, etc. The easiest way to generate a new service is using a Service Creation Application that allows creators to graphically compose their services from a set of resources represented as building blocks of the composition. Resources can be connected then so that *graphical logic* is created.

Note that graphical logic does not directly translate into service logic i.e. a graphical composition can be translated into several logic representations such as resource orchestration or resource choreography. The former requires a central entity, the orchestrator, which directs the service logic invoking resources as needed and receiving the outputs of these resources to invoke new resources again. The latter provides a more distributed execution in which each resource knows the role it plays in the composition and thus resources invoke each other to carry out the service logic. A user-centric platform does not preclude any specific service logic, but we have chosen resource orchestration for the sake of simplicity.

Although at first glance service composition might look like a matter of just creating the service logic, some other activities must be carried out. For example, if the platform is going to automatically manage and operate the new service throughout its lifecycle, then all the information needed for these activities must be generated. Even in the case of really simple service e.g. invoke a single resource and retrieve the answer, the platform must test it for compliance with platform rules, deploy it into the execution environment, and prepare it for subscription. Therefore, the graphical composition must generate a complete service description not only in terms of service logic, but also in any other aspects needed during the service lifecycle.

Since service creation is aimed at non-technically skilled end-users, the platform must provide creators with simple and usable tools that facilitate the user experience.

4.3 Architecture overview

Once we have described the basis underpinning user-centric service creation and delivery we provide in this section a high-level view of its architecture. It can be roughly divided into the following top-level entities: a Service Creation Environment, a Resource Delivery Environment, a Management and Operations Environment, and an Execution Environment.

Figure 24 shows the aforementioned environments as well as the stakeholders involved namely service creator, service consumer and resource supplier, and the underlying infrastructure.

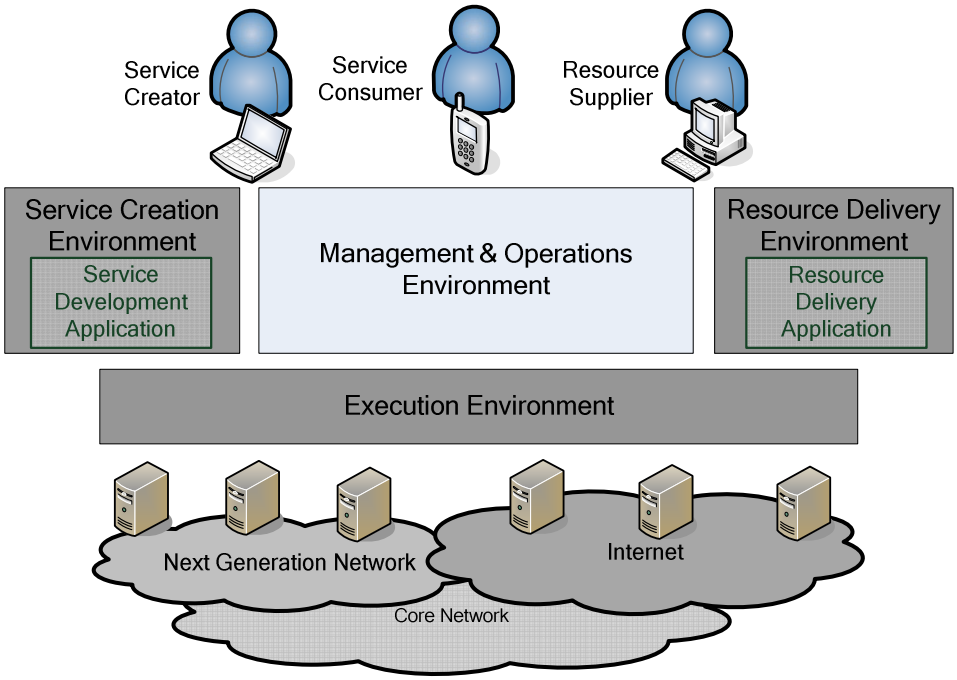

Figure 23 - High-level architecture for a user-centric platform.

This section provides an overview of each environment, describing also their components and interactions. We have highlighted the Management and Operations Environment as it is the focus of this dissertation and will be thoroughly described in the following chapter.

4.3.1 Resource Delivery Environment

This element allows resource suppliers to deliver their resources into the platform, so that service creators can begin to use them into their compositions and the platform can properly manage and operate them. Resource suppliers are provided with a Resource Delivery Application that supports them in the process of creating a wrapper to an existing resource that is implemented somewhere else. This application ensures that the resource and its wrapper comply with the platform quality and business levels and that they will not harm the platform.

During the delivery of a new resource the Resource Delivery Environment communicates with the Management and Operations Environment in order to prepare it for the new resource. After a successful delivery, the Execution Environment will include a new adaptor for the new resource.

4.3.2 Service Creation Environment

The Service Creation Environment may adopt different forms. It could be a simple Application Programming Interface (API) or an elaborated Software Development Kit (SDK). User-centric platforms usually provide Integrated Development Environments (IDE), which may include ancillary functionality such as Graphical User Interfaces (GUI) supporting the creation of new services and edition of existing ones, integration with resource repositories and testing mechanisms.

Whatever the infrastructure the Service Creation Environment provides, it must manage and carry out different activities that end up with the new service being available in the Management and Operations Environment ready to be deployed into the Execution

Environment. At the end of the creation state, the Service Creation Environment must signal to the Operations and Management Environment that a new service has been created. Then, the management environment takes control of the new service to go on with its lifecycle.

4.3.3 Execution Environment

The Execution Environment main goal is supporting the execution of services when consumers invoke them. In its simplest expression, an execution environment is made up of an **orchestration engine** that executes the service logic invoking one or several **resource adaptors**, returning the outcomes to the consumer.

The Execution Environment usually includes some ancillary modules to manage and control non-functional properties of the service such as security and privacy. For example, single sign on and identity sharing functionalities can be provided by an **Identity Provider** (IdP), and further authentication, authorization and accounting (AAA) mechanism are provided by the **AAA server**.

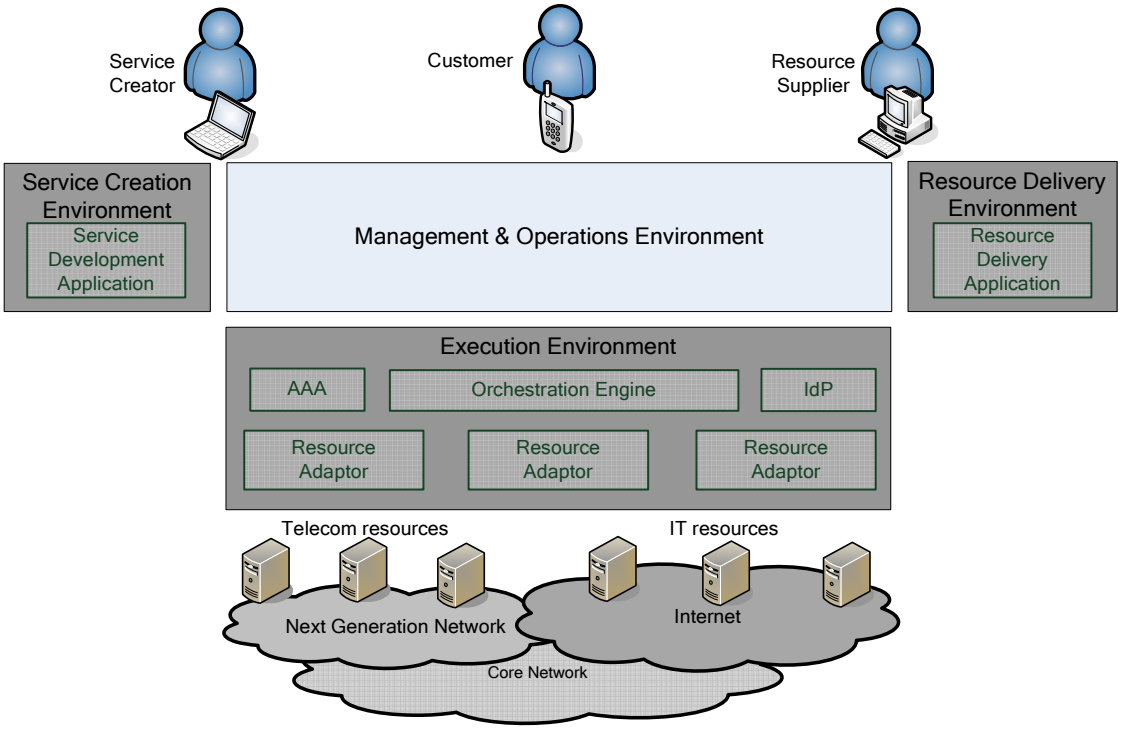

Figure 24 - Details of the Execution Environment.

The *orchestration engine* can collect execution information on behalf of the Management and Operations Environment:

- Current availability for the URL and port of the service, as well as an indication of whether or not a request on the service itself completes in an acceptable time period.
- Metrics for number of requests, number of responses, number of failure responses, number of invocations of each method, average response time for invocation of each method, total elapsed execution time, etc.
- Operations to enable and disable the ability to invoke the service i.e. activation and passivation operations.
- Events to signal lifecycle changes and request failures.

Other elements of the Execution Environment can also collect statistics to be used as a basis for usage monitoring and billing applications.

The description of a complete Execution Environment is out of the scope of this dissertation. We have described just those components that are interesting to demonstrate our contributions.

4.4 Chapter summary and original contributions

This chapter has described and analysed the foundations that support the new user-centric service creation and delivery platforms over next generation networks. For that, both the business and the technological contexts have been approached. First, the author has analysed the business context that motivates the need for such platforms. Existing business models for service provision in Telecommunications has been assessed and their feasibility for user-centric service delivery platforms has been checked. Then, the author has analysed the technological context that surrounds user-centric environments: The concept of resource has been explained, and then the concept of service as a composition of resources has been described.

As a result of the analysis carried out, the following original contributions have been proposed:

- A business model for user-centric service creation and delivery platforms. Since the analysed business model does not fulfil the requirements for these platforms the author has proposed an innovative business model.
- A high-level reference architecture for user-centric service creation and delivery platforms over next generation networks.

Next chapter will further detail the management and operations area of the reference architecture. For that, the business processes that occur in traditional management and operation systems will be described. Then they will be revisited from a user-centric point of view.

5 MANAGEMENT AND OPERATION IN USER-CENTRIC SERVICE CREATION AND DELIVERY PLATFORMS

Management in Telecommunications comprises the set of processes that manages individual resources, the network, and the offered services and products to meet customers' requirements whether the customer has explicit knowledge of these entities, including any delivery object, or not [TMF-GB924]. The previous definition is very general, but this also gives an idea of the wide coverage of the management concept in the telecom domain.

Management activities in Telecommunications are usually grouped into Operations Support Systems (OSS). OSS refers to a suite of management functions that enable an enterprise to monitor, analyse and manage systems, resources and services required to run a Telecommunications business [Koivukoski&05]. Traditional OSS deals with the Telecommunications network itself, supporting processes such as maintaining network inventory, provisioning communications services, configuring network components and resources, and managing faults.

OSS has paid poor attention to customer-facing management processes, to some extent because the traditional telecom business was focused on the network and the voice/data services that it could provide. To cover this gap the concept of Business Support Systems (BSS) was introduced. It refers to business systems dealing with customers, supporting processes such as taking orders, processing bills, and collecting payments. Although BSS is closer to the customers it has been somehow a glue that allows for the automation of some OSS processes which were related to customers such as self-service, billing and payments.

Lately, it has been realized that much of the telecom business is not just about carrying profitable bits on behalf of others, which was the focus of the network, but rather about adding value to them on the upper layers [Cuevas&06]. With this aim, the Telecommunications industry is moving towards Service Oriented Architectures (SOA) as a way to offer network resources and capabilities, and enable their use by others willing to collaborate. As a result, Web services and related orchestration environments are becoming the main complementary approach to delivering new services and products, building on and combining features available in telecom and enterprise networks with Internet types of applications. This is the case of Service Delivery Platforms (SDP) where different services from different domains, exposed using Web services interfaces, can be combined to get a new product.

Finally, with the convergence of telecom and Internet technologies, new paradigms are being introduced in the ICT service creation and delivery field. They allow for fast and cheap service creation based on allowing the end-users to create their own services. User-centric SDPs introduce even greater requirements as the services are created by end-users themselves. Besides, creators might need to decide about some steps of the lifecycle of their services. Moreover, the collaboration among operators and their partners to fulfil a service pose some risks to end-users privacy.

These problems have not been addressed yet and nowadays support systems do not consider the customer involvement in the management processes, which sometimes is required by customers and desirable to reduce operator's operational expenditure (OPEX). Moreover, the automation of all this processes is a must which will provide faster time-to-market for the new services. These are the main motivations of this

dissertation which targets at contributing to cover the detected gaps proposing innovative solutions based on standardized mechanisms and technologies.

This chapter analyses the needs and requirements of user-centric service creation and delivery platforms regarding its management and operation, and proposes a reference architecture to fulfil them. For that, the TMF NGOSS framework [TMF-GB930] [Reilly&05] [HP-ngoss08] has been followed. The previous chapter addressed the business view (why are we doing this?) analysing the internal and external drivers, the business model, the participants and the goals. This chapter addresses the functional view (What should the solution do?) and the technical view (How should the solution work?). With that aim we first analyze and describe the different business lifecycles that may occur in the context of a user-centric service creation and delivery platform. Then, traditional management and operation systems are revisited from this original point of view.

5.1 OSS/BSS lifecycles analysis

We analyze here what is needed to support the management and operation of a user-centric platform over NGN. We start by understanding the business processes that need to be supported, focusing on the lifecycles that may involve an OSS/BSS in a user-centric platform: resource supplier, resource, service creator, service and, market and consumer. These lifecycles provide a dynamic view of the related processes.

For our analysis we acknowledge that three external roles interact with the platform: service consumers, service creators and resource suppliers:

- Service consumers are customers that buy products (service offers) from the platform.
- Service creators use the platform to create new services from the composition of available resources. Then they provide the platform with these services. Service creators may propose or select a billing plan to apply to their services and thus they will be sold through the platform as a product. In this sense we can say that service creators are platform partners.

  On the other hand service creators might need to pay in order to use the service creation platform. Should this be the case, service creators would be customers of the platform. For the analysis we do in this document we do not consider service creators as customers but just as partners of the platform provider.
- Resource suppliers are third parties that provide resources onto the platform. Resource suppliers might be paid for the use of the resources they provide.

In our description we highlight those processes that are specially affected by user-centricity. For that, we focus on two concrete aspects: *user-driven* processes and *user-centred* processes. User-driven processes are triggered or controlled by end-users, whatever the role the end-user plays i.e. service creator or service consumer. User-centred processes support the management of information related to users, which is of utmost importance in user-centric platforms as it is needed for personalization and context-aware services. This information, namely personal identifiable information, is protected by specific legislation and end-users have the right to ultimately govern its use and release. In spite of the increasing relevance of these processes they are not properly addressed in the literature.

To support our analysis we use TMF's eTOM business process framework [TMF-GB921].

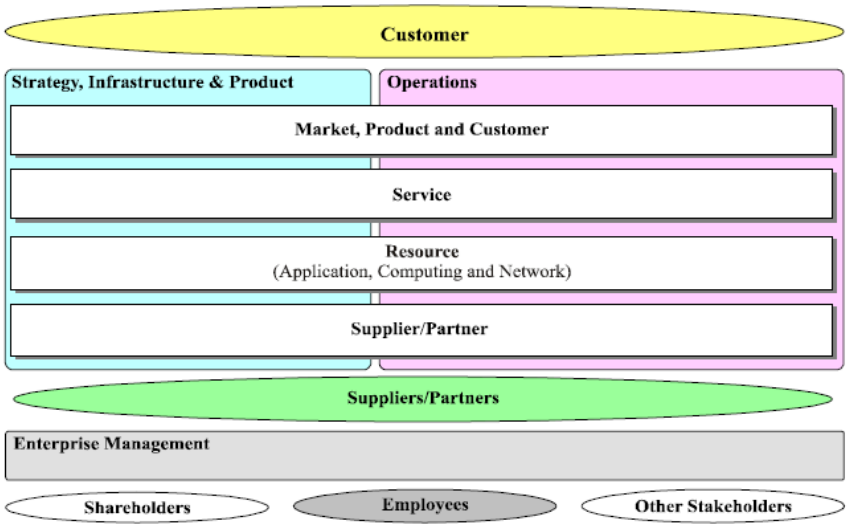

Figure 25 - TMF's eTOM business processes map [TMF-GB921].

5.1.1 Resource supplier lifecycle

The resource supplier lifecycle covers those activities involved in bringing a new resource provider to the platform, monitoring its business performance, paying it for the resources provided and finalizing the relationship. In the approach we follow, suppliers provide resources to the platform, which are used by creators to create and deliver new services to consumers. Suppliers are paid for the use of the resources they provide based on different business agreements (see section 4.1.3).

Note that this lifecycle should be traversed once per supplier even though a supplier can provide several resources.

Typical business scenarios are:

- ***Strategy and planning***: Develops the enterprise policies for engagement and interaction with new suppliers. These policies will be particularized for each resource and enforced during the interaction with every provider, and thus they drive the platform relationships with its ecosystem of suppliers.
- ***Capability delivery***: These processes initiate and complete business agreements with the resource providers. On completion of the contract arrangements, these processes can manage provision of the contracted resources or can ensure that other processes are able to make requisitions against the contract (e.g. during Fulfilment), according to the appropriate policy and practices of the enterprise. They set the basis for resource delivery and thus should be flexible enough to allow introducing as many suppliers as possible.
- ***Communications management***: This set of processes manages different type of communications with resource provider e.g. requests to fulfil some activity or passing on reports on detected problems. The business process usually includes tracking, monitoring and reporting on the communication.

- ***Settlement and payments management****:* Manage all settlements and payments to suppliers, including invoice validation and verification, and payment authorization. Payments are usually calculated based on resource usage records.

Next figure shows the processes involved in the lifecycle management of resource suppliers in a user-centric platform. Resource supplier lifecycle processes map to the horizontal processes grouping named as *Supplier* in eTOM (**Figure 25**).

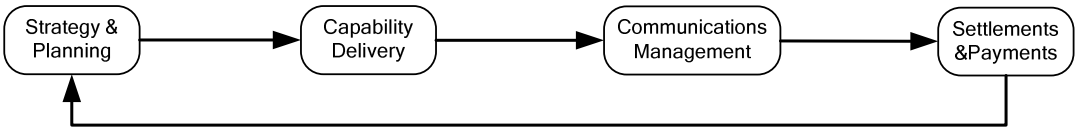

Figure 26 - Simplified resource provider lifecycle in user-centric platforms.

5.1.2 Resource lifecycle

This lifecycle addresses the development, operation and management of those resources directly involved in delivering the services. This description has traditionally focused on domain and element management, including network management for managing the network components and IT management for managing systems and applications that are part of the revenue generating infrastructure.

However, in the context of this work, we assume that resources are always exposed through enablers, whatever their implementation is. Thus, network resources are offered for example as OMA enablers, through ParlayX technology or by means of ad-hoc Web Services interfaces. The very same resource might be implemented using Java Enterprise Edition technology, SIP Application Servers, JSLEE containers, .NET framework, or any other implementation technology.

Resources are usually developed and provided by a supplier (third party resource provider) and distributed somewhere out of the platform provider domain. However, the platform still must manage and operate the resources according to its business needs. The fact that some information might be exchanged between the platform provider and resource suppliers (i.e. out of the platform administrative domain) poses some requirements on supporting processes regarding the treatment of personal information and privacy protection.

Typical business scenarios for resource management include:

- ***Strategy and planning****:* This set of processes supports planning for new resources. Therefore they might help to support long-term business, market, product and service directions of the platform provider.
- ***Development & Delivery****:* Since resources will be developed by an external resource supplier the platform must ensure their correct delivery and smooth integration onto the platform, including allocation, installation, configuration and activation of specific resource types. These processes support the delivery of new resource types onto the platform. They also introduce the new resource type to the OSS/BSS so that instances of the new resource can be properly instantiated, operated and managed as needed.
- ***Resource inventory management:*** Establish, manage and administer the platform's resource inventory. The resource inventory maintains records of all

resources available for composition as well as configuration, version, and status details.

- ***Provisioning**:* This set of processes deals with the resource operation to meet specific service requirements or to alleviate specific resource capacity shortfalls, availability concerns or failure conditions. Provisioning processes will vary depending on the resource features and even there could be no need for provisioning at all. Although these processes are invoked by the platform provider they must be implemented by the resource supplier so that they are requested as needed. The means by which the platform invokes these processes must be agreed between the parties, probably based on standardized specifications such as the ongoing work within the TMF Service Delivery Framework or the OMA Open Service Provider Environment.
- ***Fault and performance management**:* Monitoring the resources for any faults and performance issues. The monitoring might be based on the service level agreements agreed between the platform and the resource supplier. Once a fault has been detected, the platform provider can report and fix the problem, or even pass it on to the resource supplier in order to have it fixed.
- ***Data management**:* Managing the operational data of the resources. Data management usually refers to collecting the usage information with the aim of suppliers and partners settlement and consumer billing. Related processes include the collection of raw usage from the resources, the processing of this data such as filtering and summarization, the formatting of usage data as to bring the processed data in a form suitable for distribution to other processes, and the distribution of this data (called usage records) to the resource, subscription and service functions.

  In user-centric platforms data management might also include the management of sensitive information exchanged with resources e.g. consumer profile or identity information. These processes must address the increasing set of regulation that requires privacy protection when releasing personal identifiable information. Under this viewpoint, resource data management is a user-centred process and must be paid special attention.
- ***Evolution or retirement:*** Evolve or terminate the resource. Retirement is usually driven by business agreements between platform provider and resource suppliers.

Next figure shows the processes involved in the lifecycle management of resources in a user-centric platform. Resource lifecycle processes map to the horizontal processes grouping named as *Resource* in eTOM (**Figure 25**).

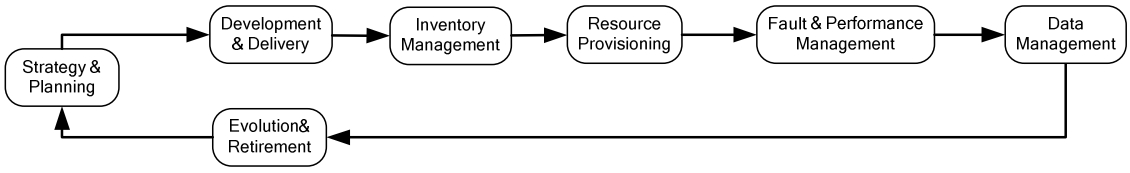

Figure 27 - Simplified resource lifecycle in a user-centric platform.

5.1.3 Service creator lifecycle

The service creator lifecycle covers those activities involved in bringing new service creators to the platform, communicating with them as needed, paying them for the

services provided and finalizing the relationship. In the approach we follow, creators provide services to the platform, which are subscribed by consumers. Creators might be paid by the platform based on different measures but usually they will be paid depending on the use of the services they have created. The payment will be calculated based on different business agreements (see section 4.1.3).

Note that this lifecycle should be traversed once per service creator even though a service creator can provide several services.

Typical business scenarios regarding service creator lifecycle are:

- ***Strategy and planning****:* Develops the enterprise policies for engagement and interaction with new creators. These policies will be particularized for each service and enforced during the interaction with every creator, and thus they drive the platform relationships with its ecosystem of service creators.
- ***Capability delivery****:* These processes initiate and complete business agreements with the service creator. On completion of the contract arrangements, these processes can manage provision of the tools and information needed to start creating services e.g. username and password or delivery of creation tools. They set the basis for service creation and thus should be flexible enough to allow a rich development of the platform service ecosystem.
- ***Communications management***: This set of processes manages different type of communications with service creators e.g. requests to fulfil some activity or passing on reports on detected problems. The business process usually includes tracking, monitoring and reporting on the communication.
- ***Settlement and payments management****:* Manage all settlements and payments to service creators, including invoice validation and verification, and payment authorization. Payments are usually calculated based on service usage records.

Next figure shows the processes involved in the lifecycle management of service creators in a user-centric platform. Service creator lifecycle processes map to the horizontal processes grouping named as *Partner* in eTOM (**Figure 25**). These processes are functionally similar to the *Supplier* business processes, as they both refer to external stakeholder from which the platform *buys goods*.

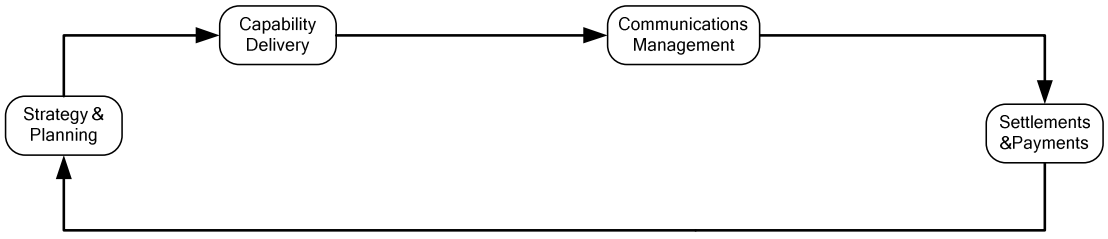

Figure 28 – Simplified service creator lifecycle in user-centric platforms.

5.1.4 Service lifecycle

The service lifecycle covers the activities involved in bringing a new service to the platform so that customers can subscribe it, and managing and operating it.

Typical business scenarios for service lifecycle are:

- ***Strategy and planning****:* Decide on a new service to provide and plan how to deliver it. In the platform under study this is a user-driven process since end-

users (service creators) decide on when and how a new service will be delivered. However, platform providers play an important role since they can influence the service creation process by promoting, recommending or advertising selected resources.

- ***Development****:* Develop and simulate a new service type. These are user-driven processes. However, since OSS and BSS must take control of the outcomes of this process for service deployment thus service development must be closely aligned with OSS and BSS systems.
- ***Deployment:*** Once the service has been successfully developed it can be deployed. These processes make necessary changes in the infrastructure as well as in the required support systems for the new service type. This is one of the key set of processes in user-centric platforms, as the success of the platform will depend on how easy it is to deploy a new service. OSS and BSS should support and automate deployment of new services as much as possible.
- ***Service inventory management:*** Establish, manage and administer the platform's service inventory. The service inventory maintains records of all service types, service infrastructure and service instance configuration, version, and status details. It also records test and performance results and any other service related- information.
- ***Service subscription****:* Once a new service subscription order has been delivered, these processes take care of that order and provision the service (determine the changes and configurations required to provide the service to the consumer) and activate it for the customer (make the necessary changes in the infrastructure).
- ***Service monitoring****:* Monitor the service to ensure that the customer's expectations are being met; resolve any incidents or problems that may occur; collect information about service usage, monitor personal identifiable information release.
- ***Data retention and compliance:*** The data retention and compliance processes address the increasing set of regulations that require both the collection of data for law enforcement and the increasingly protection of the data privacy. These processes are affected by specific requirements in user-centric platforms as services are created by end-users and automatically deployed. Therefore, data privacy must be automatically checked and enforced.
- ***Rating:*** These processes relate the usage records to a resource, service or service subscription. They aggregate usage records that relate to the same service instance (i.e. customer), apply the appropriate tariff or charging algorithm to parameters included in the usage records and insert it in the records, and finally distribute these records to the billing and collection management process. They also distribute usage records to service creators' and resource suppliers' payment and settlement processes.
- ***Service evolution or retirement****:* Evolve or retire the service. Service evolution might be a user-driven process: service creators decide about the evolution of their services. However, service retirement is also a platform-driven process since business agreements usually set all rights in hands of the platform provider. OSS and BSS must support service creator and platform provider in accomplishing these activities.

Next figure shows a simplified view of the service lifecycle in a user-centric platform. This lifecycle maps to the *Service* horizontal processes group in eTOM (see **Figure 25**).

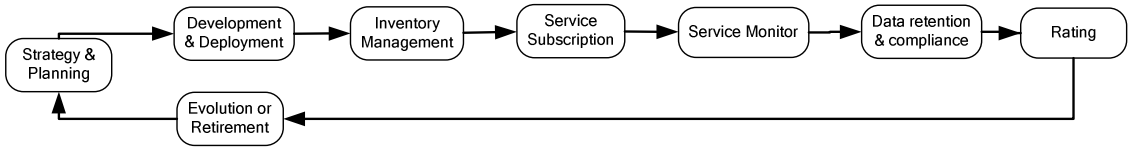

Figure 29 - Simplified service lifecycle in user-centric platforms.

5.1.5 Market and consumer lifecycle

This lifecycle covers those activities involved in bringing new consumers to the platform and managing their relationships with the platform. In the approach we follow consumers buy (subscribe) services from the platform.

Typical business scenarios are:

- ***Market strategy and planning:*** Market segmentation and analysis is performed to determine the platform's target and addressable markets, along with the development of marketing strategies for each set of target customers. These are usually off-line processes.
- ***Market capability delivery:*** Manage the delivery and build of new or changed market capabilities or customer-related capabilities. These processes create and deliver the processes that *Marketing, communications and promotions* will support.
- ***Marketing, communications and promotions:*** Deal with overall communications to customers and markets. In user-centric platforms these processes might support techniques such as viral marketing through recommendation and sharing of services among consumers, direct advertising based on preference matching and profiling, and so on.
- ***Customer inventory management:*** The customer inventory maintains records of all customers, their interactions with the platform, and any other customer related- information required to support the business. The purpose of these processes is twofold. First they establish, manage and administer the enterprise customer inventory with processes such as customer identity provisioning and withdrawal. Then they monitor and report on the usage and access to the customer inventory, and the quality of the data maintained in it.

  Customer inventory related processes have been platform-driven processes since the platform traditionally decides all aspects of the management of customer-related information. However, these processes are also user-centred since they support the management of information related to users. Since users would like to take an active role regarding the use and release of their personal information customer inventory management is quickly becoming also a user-driven process. Therefore customer inventory must be revisited in user-centric platforms.
- ***End-user self service and ordering***. Provide the means for a consumer to buy the service and take the order. Self-service is not a specific feature of user-centric platform, as it is currently used in several systems.

- ***Problem report:*** Responsible for receiving trouble reports from customers, resolving them to the customer's satisfaction and providing meaningful status on repair and/or restoration activity to the customer.
- ***QoS management***: Monitoring, managing and reporting of delivered vs. contractual Quality of Service (QoS), as defined in the platform's service descriptions, customer contracts or product catalogue.
- ***Billing and collections management***: Service charges are related to individual consumers depending on the details of the agreement and additional charging rules such as discounts. Bills are created and delivered to consumers, and payment collection is managed.

Next figure shows the process involved in the lifecycle management of market and consumers in a user-centric platform. Market and consumer lifecycle processes map to the horizontal processes group named as *Market and Customer* in eTOM (see **Figure 25**).

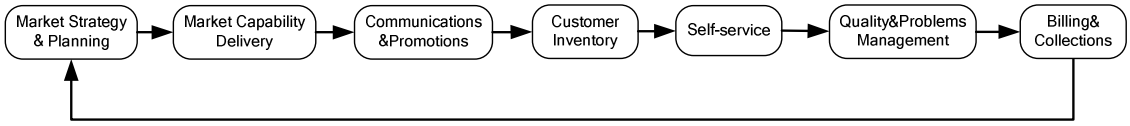

Figure 30 – Simplified market and customer lifecycle in user-centric platforms.

5.1.6 End-to-end lifecycles view

The described lifecycles span within the two major areas of the eTOM: *Strategy, Infrastructure and Product,* and *Operations* (Figure 31). To simplify the figure we have grouped the *Service Creator Lifecycle* and the *Resource Supplier Lifecycle* as they are functionally overlapped.

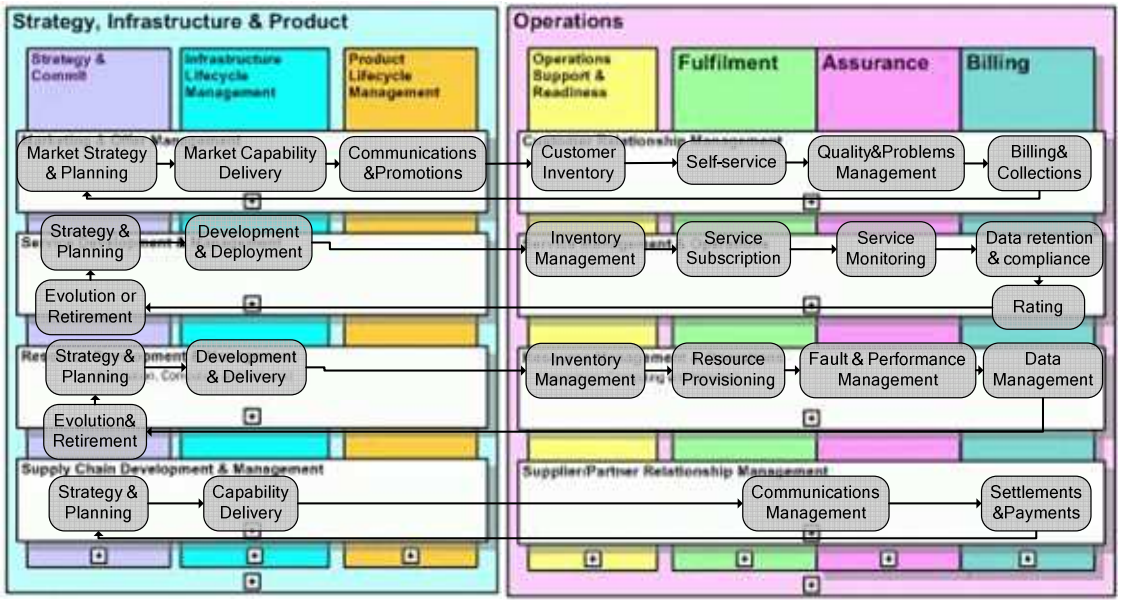

Figure 31 - OSS lifecycles and eTOM business processes map.

5.1.7 Interactions among the lifecycles

The lifecycles described are not independent of each other i.e. several links exist among them. For example, to successfully complete an order for a new service offer (self-

service) a new service instance must be subscribed and thus underlying resources must be provisioned. This is a usual link in traditional telecom systems.

There are two interesting links in user-centric platforms we pay special attention. The first one is that between a service and the underlying resources. Traditional services have a very direct and defined link between them since services usually have dedicated resources. However, in user-centric platforms new services are composed by end-users from a huge set of disparate resources and thus relationships are dynamically defined at the time of creation, setup at the time of deployment, used at runtime and finalized when the service is not needed anymore. These relationships are needed during the service lifecycle, for example, to successfully carry out an order for a new service subscription or to adequately share revenues between platform provider, service creator and resource suppliers. Therefore the platform must provide a flexible mechanism to support the description of dynamic relationships between services and resources.

On the other hand many services can share the very same resource, which might serve one service instance one day and a hundred the next one if successful. To support this fast changing environment the link between the service instance and the resource is becoming increasingly virtualized allowing seamless replication of resources as needed. This, in turn, introduces abstractions to the links between the service lifecycle and the resource lifecycle.

The second interesting link between lifecycles is that between the processes that manage customers' identity resources i.e. customer inventory, service data retention and compliance, and resource data management. They all support the management of identity information, but they work at different business times. Although functionally represented in different lifecycles all these processes are referred globally as identity management processes. Identity management deals with the technical, legal and business processes involved into the management and selectively disclose of user-related identity information into an institution and between some of them, while preserving and enforcing privacy, data protection and security needs [Radhakrishnan07].

Seen as a whole, these processes provide a new lifecycle on their own: identity lifecycle. The operations performed on an identity start with the creation of the identity of a user when an individual joins an organization i.e. identity provisioning. The information initially set must be maintained during the lifetime of the identity within the organization i.e. customer inventory. Once the identity information exists and is accurate, it may be used for different purposes within the organization e.g. access management to services. From time to time and due to business requirements, it may be also necessary to share it with other organizations outside the initial organization boundaries, i.e. cross-domain identity management. During these processes data retention and privacy protection laws must be enforced, which are supported by service data retention and compliance processes within the platform, and resource data management processes when the identity information is shared outside the boundaries of the platform provider. Eventually the identity information must be disabled or removed when the individual leaves the organization.

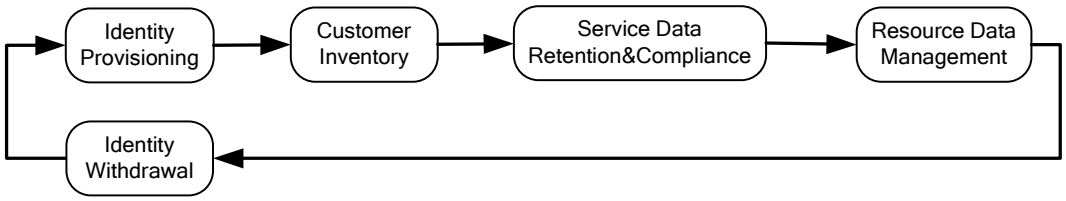

Figure 32 - Simplified identity lifecycle.

It is on the very roots of user-centric platforms the distribution of information among services and also to resources, and identity information is not an exception. To facilitate these activities and avoid overwhelming customers with details, identity management lifecycle processes should be automatically carried out by the platform. Besides, the identity information will be usually distributed in some nodes of the network including the consumer device itself. However, being user-centricity at the core of these platforms they must provide users with the opportunity of governing and controlling their privacy i.e. user-centric privacy control.

5.2 Management and operations revisited under a user-centric viewpoint

Now that we understand the business processes that the OSS/BSS need to support in a user-centric platform we can look at the functionality needed to implement them. With this aim this section first introduces a high-level view of the OSS functionality explaining its different modules. Then we detail each one, highlighting those modules that this dissertation targets.

5.2.1 High level view of the OSS functionality

Traditional architectures for the management and operation in Telecommunications services usually focus on the areas of Fulfilment, Assurance and Billing. Lately, also the Customer Relationship Management is being covered, which addresses the business processes related to service consumers. These functional areas were enough for traditional Telecommunications services, where the major actor was a passive consumer of services and information provided always by the Telecommunications operator. However, since end-users increasingly perform more active roles and new actors appear in the delivery process these functional areas must be revisited [Bray&06]. Moreover, end-users in user-centric platforms play new roles and thus their management must be considered too.

Therefore, we thoroughly think that the traditional areas must be extended in user-centric platforms to Partners Relationship Management and Suppliers Relationship Management. Furthermore, since user-centric platforms must provide a higher degree of automation and end-user actions must be translated to changes in the infrastructure we consider that an OSS/BSS Integration Layer is needed to accomplish this new functionality.

Figure 33 shows a high-level view of the OSS/BSS functionality in a user-centric service creation and delivery platform. The Service Creation Environment, the Resource Delivery Environment, the Execution Environment and the underlying Telecommunications and IT infrastructure and resources are not part of the OSS/BSS. However, they are the focus and the target of the Management and Operations Environment, and thus we introduce them here to provide a complete vision of a user-centric service creation and delivery platform.

Next sections provide details on each module of the Management and Operations Environment and its components. To highlight the components we focus on we have painted them with brown colour in the following figures.

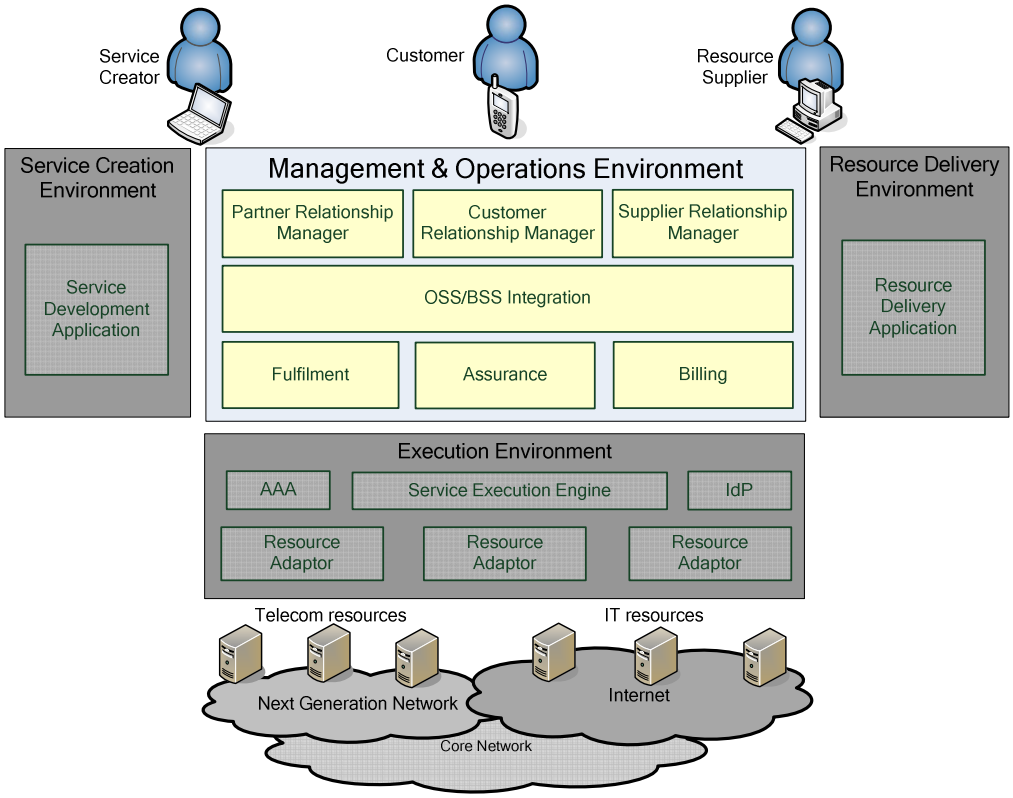

Figure 33 - High-level view of the OSS functionality.

5.2.2 Partner Relationship Manager

This functional area deals with **Partner Relationship Management** (PRM). In the context of this dissertation the overall goal of PRM is the management of communications between the platform and the service creators. Therefore, PRM addresses solutions for the business processes described within the service creator lifecycle providing the functionality needed to support it.

The Partner Relationship Manager enables the platform to customize and make more efficient administrative tasks by making tools and real-time information available to all the creators. Its components provide functionality for:

- engagement of new partners such as initiating and completing business agreements;
- delivery of the information and tools needed to start creating new services such as username/password and access to a Service Development Application;
- features for interacting with creators including problems reported on their services;
- settlement and payments management for the work carried out and;
- other features designed to facilitate the relationship between an enterprise and its partners.

Although Partner Inventory might be included within the Partner Relationship Manager we prefer to keep it in the OSS/BSS Integration Layer together with the Customer Inventory. The reason for this decision is that in user-centric platforms end-users can perform the roles of both service creator (partner) and service consumer (customer). Having both repositories together makes the management and operations processes easier.

Since PRM software currently addresses all the requirements to support the service creator lifecycle management we will not provide further details on these processes.

5.2.3 Supplier Relationship Manager

This functional area deals with **Supplier Relationship Management** (SRM). The general goal of SRM is managing an enterprise's interactions with the organizations that supply the goods and services it uses. In this dissertation we focus our efforts on resource suppliers, that is, the organizations that provide the platform with new resources that can be used by service creators to develop new services.

SRM provides a common framework based on the platform business processes, policies and information models to enable effective communication with its suppliers who may use quite different business practices and terminology. As a result, SRM increases the efficiency of processes associated with managing the platform ecosystem of resource suppliers.

The Supplier Relationship Manager provides tools and information to engage new resource providers onto the platform managing the initiation and completion of business agreements based on platform policies. It provides suppliers with the information needed to access platform features such as username/password, or a Resource Delivery Application to start delivering resources. The Supplier Relationship Manager also allows communicating with the resource suppliers, thus managing their interactions with the platform e.g. in case of problems reporting. Finally, SRM provides processes to carry out settlement and payments to the suppliers.

It is worth introducing at this point the work of Alemán et al [Aleman&07], which describes a Business Mashup Framework (BMF) that addresses business relationships and economic transactions between a platform and its resource suppliers in an open marketplace scenario. The BMF includes the business-related elements required by providers to share their resources such as components for business policies description, and components for the management of Service Level Agreements (SLA), Business Level Agreements (BLA) and Revenue Sharing Agreements (RSA). These components support the definition of value chains and the management of the revenue flows associated to a service purchase. Thus, BMF fulfil the requirements set on the resource supplier lifecycle processes and might be used as an implementation of the Supplier Relationship Manager.

Due to the fact that there are different SRM products that fulfil the requirements to support the service creator lifecycle management we will not provide further details on these processes.

5.2.4 Customer Relationship Manager

This functional area deals with **Customer Relationship Management** (CRM). This term applies to processes implemented by a company to handle its relationship with its customers, thus supporting market and consumer lifecycle business processes. CRM

functionality includes interfacing customer and storing their details, combining policies, processes, and strategies to unify its customer interaction, and providing a mechanism for tracking customer information.

Figure 34 shows a simplified view of the different components of the Customer Relationship Manager:

Operational CRM. It supports front-end business processes that address customers. This functional area provides functionality for customer engagement, self-service, customer-side ordering or problem reporting.

Analytical CRM. It analyzes customer data in order to infer some knowledge useful for the platform e.g. analyzes customers' behaviour and carries out market segmentation.

Campaign management. It defines target groups formed from the client base according to selected criteria, sends campaign-related material, and tracks, stores and analyzes campaign statistics. Recommendation tools are included within this category.

Privacy Manager. It allows customers to govern and decide on the use and release of their personal identifiable information. When gathering data as part of a CRM solution, a company must consider the desire for customer privacy and data security, as well as the legislative and cultural norms. For example, indicating that their data will not be shared with third parties without their prior consent or that no illegal access by third parties has been performed.

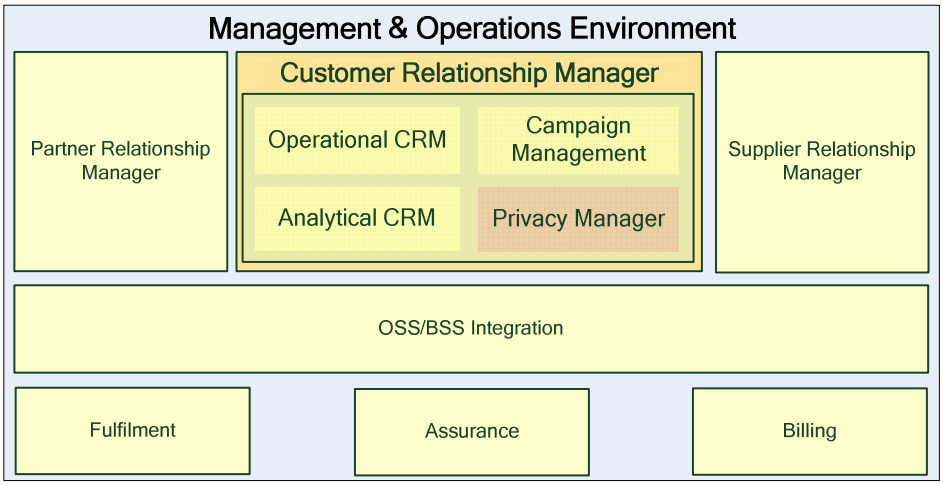

Figure 34 - Customer Relationship Manager functionality details.

Although sometimes Customer Inventory is considered as part of the CRM, we rather keep it in the OSS/BSS integration functional area. The main reason for this decision is that Customer Inventory is a central process to some other functional areas such as Identity Management or even the Execution Environment. On top of that, Customer Inventory is not a monolithic information silo, but rather an interface to a set of distributed sources of information that must be aligned. These sources might be scattered in different platform entities or even out of the platform boundaries provided by some resources. Nevertheless, we keep the Privacy Manager as part of the CRM since it interfaces the customers and is aimed at managing their information.

CRM software and products currently addresses most of the requirements to support market and customer lifecycle management and thus we will not provide further details on these processes. However, user-centric privacy management has not been properly addressed in spite of the fact that identity management solutions provide some form of

built-in privacy features. Therefore, the Privacy Manager is one of the focuses of this dissertation and further details will be provided in following chapters.

5.2.5 OSS/BSS Integration

The OSS/BSS Integration area contains two different types of groupings (Figure 35). First, we have the definition of the information that drives the OSS such as business processes and policies, along with the definitions of the information that needs to be shared across the different processes and applications. Second we have the technology that is required to support the integration and that is common across fulfilment, assurance and billing areas.

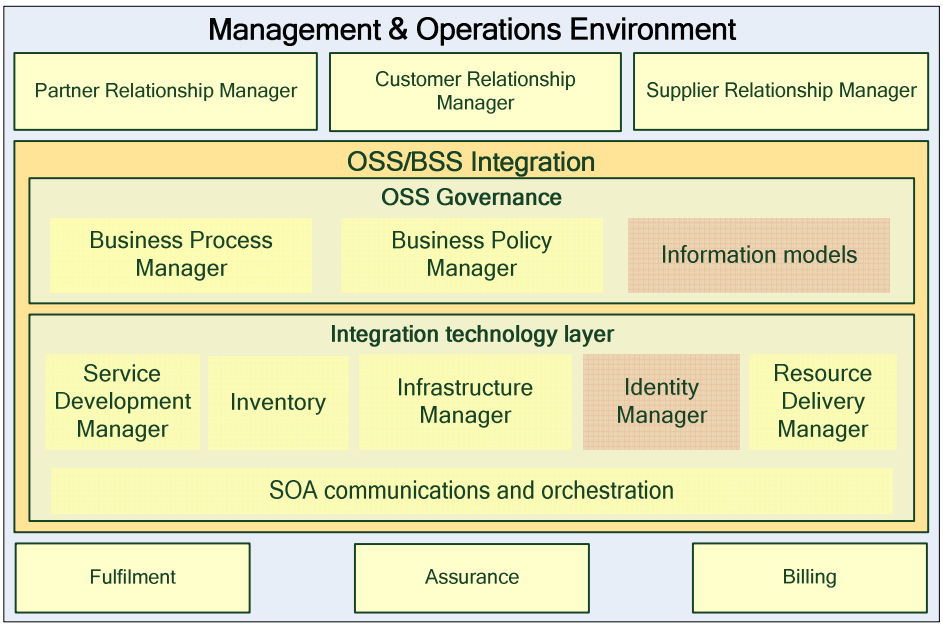

Figure 35 - OSS/BSS integration functionality details.

5.2.5.1 OSS Governance

This functional area includes the components that govern the OSS as a whole. It includes a **Business Process Manager** that allows capturing the definition of the business processes and modifying them. This component provides several benefits such as maintaining separation between business processes and applications; understanding the relationship between OSS/BSS processes and other business processes, and; loading the processes into process management engines for automation and monitoring.

The **Business Policy Manager** supports the definition of the general business policies and the specific policies defined for the OSS. Business policies are needed to carry out the platform strategy and planning at its different levels: market and customer, service, resource, supplier and partner. This module supports in understanding and modelling how high-level policies are implemented through lower level policies, and monitoring them for compliance.

Finally, we need consistent **information models** for data that is common across processes or applications. Common syntax and semantics are crucial for communication inside and outside the enterprise borders. There are well-known standards and specifications such as TMF Shared Data/Information Model (SID) that can be used as a basis for defining the platform information models.

It is worth noting at this point that we are dealing with a platform that aims at working as an open marketplace of resources and services. Since resources are delivered by loads of suppliers out of the platform boundaries a consistent information model is a must to properly introduce and manage these *external* resources. In turn, resources are dynamically composed by partners to create new *services* that must be described according to the same information model to guarantee coherence and their operation and management across the lifecycle.

The definition of one **information model to completely describe resources and services in all their facets is one of the contributions of this dissertation**. We thoroughly describe it in following chapters.

5.2.5.2 Integration technology layer

The integration technology layer provides the technology for common functionality and enables the integration of the various OSS/BSS components.

The **Infrastructure Manager** provides part of the functionality defined by the TMF within the operations support and readiness processes group: general set of functionality that supports the fulfilment, assurance and billing areas. This component includes functions such as management, monitoring and reporting on infrastructure needed to support services, resources, customers, suppliers and partners. Although TMF includes inventory as part of this group due to its relevance we split it into its own area.

Since the Infrastructure Manager focuses on infrastructure we have added two new components to deal with resources delivery and services development, namely, the **Resource Delivery Manager** and the **Service Development Manager**.

The Resource Delivery Manager deals with the allocation, installation, configuration and activation of new resource types. This component receives the outcomes of the Resource Delivery Application and sets up the resource dependencies within the Operations and Management Environment, so that the new resource type is ready to be used in service compositions and can be properly managed by the fulfilment, assurance and billing areas.

The Service Development Manager interfaces the Service Creation Environment, specifically the Service Development Application. When the creation process has finished, it receives the outcomes and prepares them to be passed on to the Service Deployment Manager within the fulfilment area, so that a new service can be available. For that, this module registers the new service type in the Service Inventory.

Resource Delivery Manager and Service Development Manager extensively use the information models defined in the OSS Governance area. This ensures a smooth delivery of resources and services by external players. Therefore, they provide a key functionality for the success of the platform as a marketplace, since they are the bridge that allows external players' products to become part of the platform.

Inventory area includes resource, service, customer, partner and supplier inventory as well as information regarding the way they are related. Once a new resource has been delivered all the needed information must be stored in the resource inventory so that OSS processes are able to operate the new resource. Quite in the same line, when a new service is developed its description must be stored in the service inventory for further operation. And as for platform users, customer inventory manages identities of the platform consumers while partner and supplier inventory stores details needed, for example, for future settlement and payments.

While theoretically Identity Management is not different from any other form of management, we pull out the management of the identity mechanisms because of the importance, and often, requirements for closer auditing, law enforcement and privacy protection. Note that the **Identity Manager** does not deal with the identity mechanisms, but rather the management of those mechanisms. For example, an Identity Provider (IdP) that federates the customer's identity in the platform with the customer's identities in different resource providers supporting single sign-on operations and identity sharing is an identity mechanism and is thus not part of the identity management from the point of view of OSS. Configuring the IdP to implement business policies and customer privacy preferences, and monitoring it for any breaches in the identity mechanisms is part of the functionality the Identity Manager provides.

We think that proper identity management is one of the cornerstones for the success of user-centric environments since identity mechanisms provide unique features such as user-context information, personalization, usability improvements and higher security levels. However, in spite of the fact that all the federated identity frameworks include built-in privacy features all they lack comprehensive frameworks for **user-centric privacy management**. **This dissertation contributes to cover this gap with innovative solutions that are described in the following chapters.**

Finally, **SOA communications and orchestration** provide support for the actual communications mechanisms. This could be provided through a middleware, a service bus or other mechanisms. Besides, this area must provide support also for the process and policy engines that need to handle the orchestration of the processes across OSS components.

5.2.6 Fulfilment

The functionality most people initially think of when considering fulfilment is that needed to support the service subscription and resource provisioning. However, fulfilment may also include the functionality needed to support the design, implementation and deployment of new service types. In our architecture (Figure 36) we split these areas since they work at different business times and different actors drive their functionality: service creators design and implement their services using the Service Development Application, while the Management and Operations Environment deploys the new services. Note that the Service Development Manager interfaces both to adapt the outcomes of one to the requirements of the other.

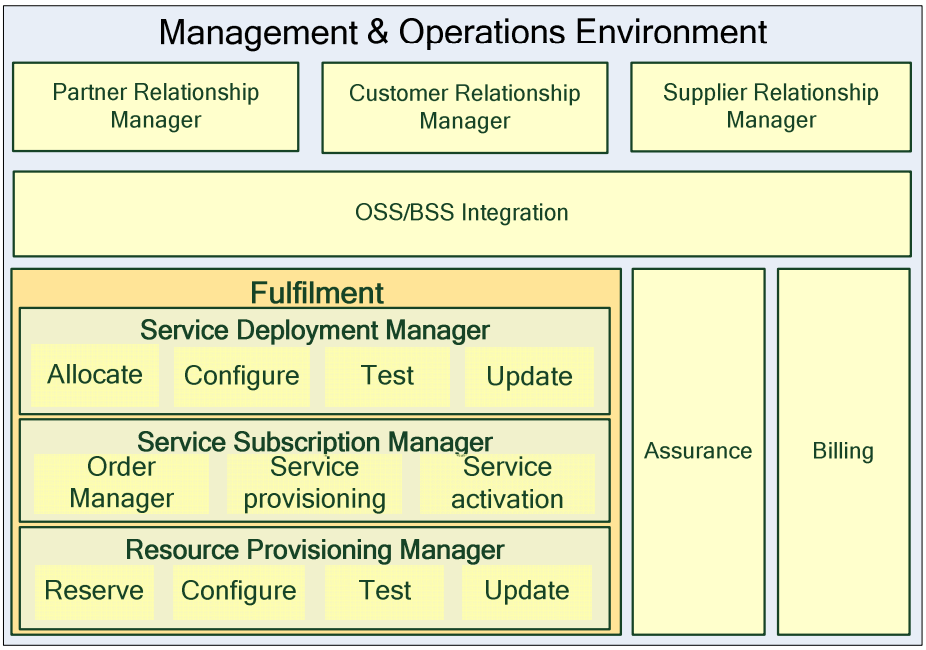

Figure 36 - Fulfilment functionality details.

5.2.6.1 Resource Provisioning Manager

When we look at the fulfilment provided by the Resource Provisioning Manager we need to consider the functionality required to support the resources independently of any specific service instance. However, specific service compositions and instances will drive the invocation of this component.

The **Resource Provisioning Manager** deals with the resource operation to meet specific service requirements or to alleviate specific resource capacity shortfalls, availability concerns or failure conditions. The functionality it provides to the Operations and Management Environment includes:

- Allocating the appropriate specific resources to support service orders or requests from other processes;
- Reserving specific resources for a given period of time until the service order is confirmed;
- Configuring specific resources, as appropriate;
- Testing the specific resources to ensure the resource is working correctly;
- Recovery of resources;
- Updating of the Resource Inventory to reflect that the specific resource has been allocated to specific services, modified or recovered;

In user-centric platforms, Resource Provisioning Manager provides an interface for the aforementioned functionality and forwards the invocations received to the specific resource management interface, which must be implemented by the resource supplier. It should be noted that the resource management interfaces and their implementation are out of the scope of this dissertation. They are currently standardized, for example, by DMTF WS-Management [DMTF-WSM] and OASIS Web Services Distributed Management (WSDM) [OASIS-WSDM] initiatives.

5.2.6.2 Service Subscription Manager

The Service Subscription Manager is in charge of carrying out customers' subscription to existing services. It is composed of order management, service provisioning and service activation. In addition, the Service Inventory is heavily involved in the service subscription.

While interfacing with customers is part of the Customer Relationship Manager, the **Order Manager** provides the technical details of order management. Order management begins with an evaluation of the customer order to ensure technical feasibility. Part of the feasibility check is to provide order validation for completeness and consistency. Then the order is decomposed into the constituent services (just one in the simplest case), provisioning and activating them using the other functions.

Service Provisioning has the task of verifying the availability, suitability and reservation of resources prior to conduct a service subscription. If specific service level commitments are required of the service, the provisioning needs to be sure that the resources used can provide the necessary service levels. For other services, the provisioning may be relatively trivial and might be even performed as part of the service activation function.

Service Activation coordinates and executes the steps that need to be taken to enable or disable a service for a particular customer. The focus is on configuring the resources and infrastructure to enable customers the access to the service. Service activation needs to ensure atomicity of its actions i.e. in the end either the service is fully activated or the activation fails and all the resources are returned to their pre-activation state. It should be noted that part of activating a service needs to be making the necessary changes in the assurance and billing systems to ensure that the service can be monitored, supported and billed.

Service subscription is a well-known discipline of OSS and there are plenty of commercial solutions to fulfil the requirements set. Besides, user-centric platforms do not pose specific requirements regarding this functional area. For some commercial solutions we refer the readers to [TMF-Prosspero], where solutions in the area of Service Activation and Order Management are being certified.

5.2.6.3 Service Deployment Manager

This component is in charge of the clean and efficient handoff of a new service type from the Service Development Application to the Management and Operations Environment. For that it is supported by the Service Development Manager. This activity becomes more critical as the service lifespan shortens.

The Service Deployment Manager functionality includes:

- Allocating all needed resources for the service deployment. For that it communicates with the underlying Resource Provisioning Manager to carry out the provisioning of the resources needed.
- Configuring the infrastructure and other components of the Management and Operations Environment to support the new service.
- Testing the specific service to ensure it is working correctly. This testing may involve friendly trials, establishing performance baselines for the service, and generally validating that all operational and billing systems can handle it.

- Updating the information contained in the Service Inventory as to the configuration of specific services and their status.

Other functionality is also possible to support service evolution and recovery. If the new service is an enhancement to or replacement for an existing service, the Service Deployment Manager must make any necessary changes to customers of the old service.

5.2.7 Assurance

The components of this functional area are responsible for monitoring resources and services for faults or performance degradation, report the detected problems and fix them when possible. Sometimes the platform is not able to fix the problem and then it must be reported to the resource provider or service creator.

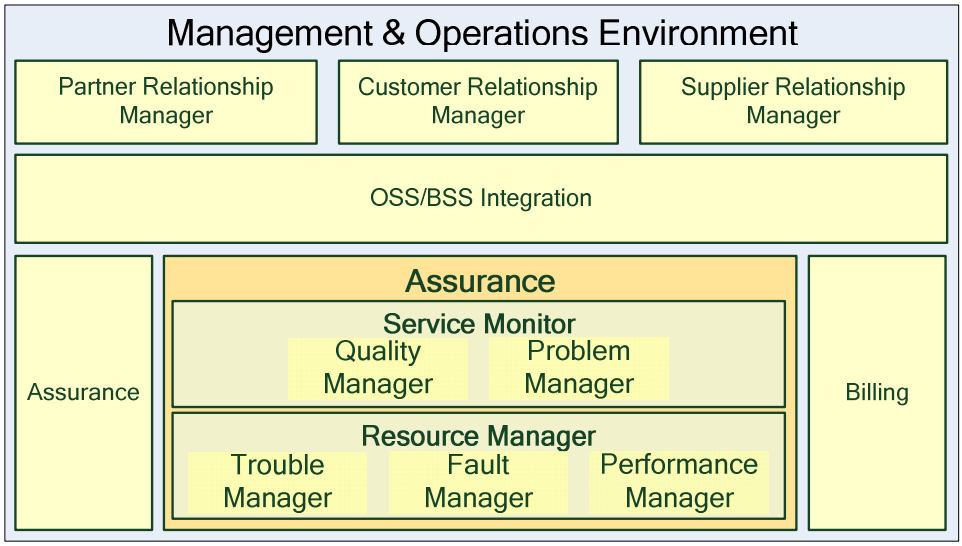

Figure 37 - Assurance functionality details.

5.2.7.1 Resource Manager

In user-centric platforms resource management is mainly focused on the vigilance of the underlying resources that make up the services and the resolution of the detected problems. Therefore, this functional area focuses on detecting faults and ensuring that resources are performing as expected. For that three main components are used: Fault Manager, Performance Manager and Trouble Manager.

The **Fault Manager** role is to know whether or not the various resources are working. It supports the collection and correlation of alarms and other relevant events to provide an accurate view of the health of the resource ecosystem. However, the lack of faults does not necessarily mean that the resource is running properly. Though it may be functioning, the resource may not be performing; the load on it may be such that it is just being asked to do more than it can.

The **Performance Manager** is the component that collects and analyzes performance data to ensure that it is within specified parameters. The data can be collected, for example, from performance counters in the Service Execution Engine. It may also be collected from instrumentation added to the Resource Adaptors in the form of probes. These probes could be passive (monitoring activities and taking measurements) or active (simulating a demand for service and measuring the pertinent response times). Whenever the data crosses the predefined thresholds, an event is generated to the Fault

Manager. In addition to the real-time nature of performance management, the data might be also used to identify trends and create forecasts.

Finally, the **Trouble Manager** supports the resolution of any detected faults and problems. For that it communicates with underlying resources and tries to solve the problem on its own. If this is not possible, then it communicates with the Supplier Relationship Manager to report the problem so that the resource provider can fix it.

As in the resource provisioning case, most of the functionality that these components provide must be implemented by the resource supplier. Again, the interfaces for that and their implementation are out of the scope of this dissertation. For further information on standard procedures we refer the readers again to [DMTF-WSM] and [OASIS-WSDM].

5.2.7.2 Service Monitor

This module monitors the end-to-end services being delivered to customers, whether individually per customer or aggregated across customer groups. It includes two components, namely, the Quality Manager and the Problem Manager.

The **Quality Manager** monitors that the services delivered match the customer expectations. For that, SLAs might be defined and monitored.

In user-centric platforms, due to the amount of services being created and removed and their short lifetime, it is not feasible to define and monitor SLAs for each single service session. While this may be practical, or even necessary, for some services, it may be prohibitively expensive and thus not desirable for other types of services. On the other hand, for most services the requirement is to have an aggregate view across the customer base, with the ability to focus on particular customers when required. This view is provided by the Customer Relationship Manager, providing customers with channels to report their problems.

Finally, the **Problem Manager** analyzes the detected problems. Some of them may be caused because of a failure in an underlying resource, and in this case the Problem Manager is able to fix it. However, since end-users create their own services, sometimes the platform might be unable to solve the detected problems and all it can do is report them on to the service creators. For that, the Problem Manager uses the Partner Relationship Manager.

5.2.8 Billing

The components of this functional area are responsible for collecting significant events useful for the production of accurate bills in time, processing and collecting payments from customers, and carrying out settlements and payments to suppliers according to agreed business terms.

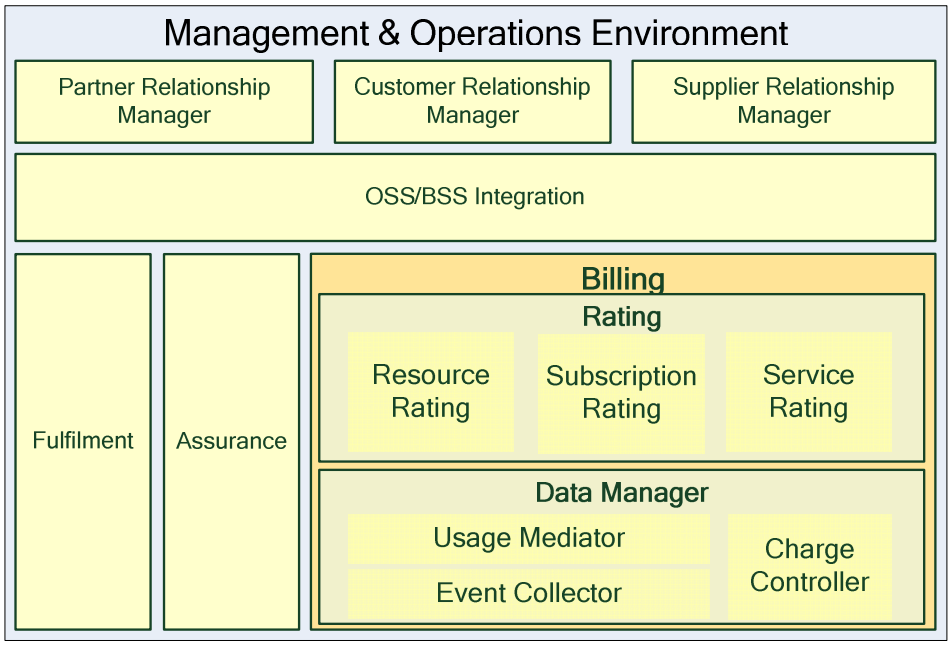

Figure 38 - Billing functionality details.

5.2.8.1 Resource Data Manager

Three main components provide the functionality needed for the billing area at the resource level. First, the **Event Collector** gathers raw usage data from the infrastructure. Then, the **Usage Mediator** validates, normalizes, converts and correlates this information into usage data for each service type, service subscription and resource type. This categorized usage data will be used to calculate customers' bills and suppliers and partners payments.

While usage mediation is sufficient for post-paid billing, pre-paid billing schemes require charge control mechanisms that can authorize session initiation based on account balance, terminating the session if necessary when a balance is exhausted. The **Charge Controller** must work closely with the components that enable this functionality in the Execution Environment such as the Authentication, Authorization and Accounting (AAA) module.

5.2.8.2 Rating

We have included three components in the rating area, each one focused on a specific stakeholder: **Resource Rating, Subscription Rating** and **Service Rating.**

Resource Rating translates the usage information generated by the Usage Mediator into settlements for individual resource suppliers. This includes rating the usage of each resource and aggregating it into a periodic invoice. This module does not deal with payments to resource providers, which are carried out by the Supplier Relationship Manager.

Subscription Rating translates the usage information into charges for individual customers. This includes identifying and applying tariffs and charging algorithms to specific parameters encapsulated in usage records. The charges are aggregated into a periodic bill. This module does not deal with bill invoice or payments collection, which are carried out by the Customer Relationship Manager.

Finally, Service Rating translates the service usage information into settlements for individual service creators. This includes rating the usage of each service and aggregating it into a periodic invoice. Service rating does not tackle payments to service creators, which are carried out by the Partner Relationship Manager.

5.3 Chapter summary and original contributions

This chapter has analysed the different business lifecycles that may occur in the context of a user-centric service creation and delivery platform. Based on this analysis and due to the lack of proposals in the reviewed literature the author has proposed a set of business processes needed for a proper management and operation of the aforementioned platforms. The traditional management and operation systems have been revisited from this original point of view.

As a result, the author has proposed the following original contribution:

- A reference end-to-end architecture for the management and operation of user-centric service creation and delivery platforms. The architecture has been described following a top-down approach, beginning with a high-level overview and providing deeper details on each component.

Part of this original contribution, namely the description of the service lifecycle and the resource lifecycle management processes, were contributed [OMA-arc08b] to the Open Mobile Alliance Service Provider Environment Architecture group to be included within the OSPE specifications.

Next chapter will describe the information model that supports the management and operations area. The information model implementation and its relationship with the different modules will be explained too. Finally, the relationship with well-known standards for the management of Telecommunications systems is explained.

6 INFORMATION MODEL FOR THE MANAGEMENT AND OPERATION OF USER-CENTRIC SERVICE CREATION AND DELIVERY PLATFORMS

Services are provider-client interactions that provide values. One of the key features that differentiate services from traditional software components is self-description, which separates the service specification from the service implementation thus supporting the loose coupling of SOA. In a user-centric environment services and resources can be considered as services too, because they operate following provider-client interaction and are self-descriptive entities.

A service (resource) specification is usually grouped based on specific concerns. For example Web services technology uses the Web Services Description Language (WSDL) [W3C-WSDL] to describe interface signatures and endpoint bindings, uses various Quality of Service (QoS) specifications to describe non-functional properties, and uses orchestration languages such as the Business Process Execution Language (BPEL) [OASIS-BPEL] to describe the logic of a composition.

This chapter describes an innovative proposal for an information model useful for the description of the services and resources living within a user-centric service creation and delivery platform. This model is flexible enough to support the automation of the lifecycle management processes and to cope with the variety of technologies that the different stakeholders might use.

The model has been validated, among others, in the OPUCE project [OPUCE] where it is currently in use. Furthermore, its value has been acknowledged by the Open Mobile Alliance where it has been submitted for inclusion in the ongoing OMA Service Provider Environment specification

6.1 Information model description

Within the context of user-centric service creation and delivery platforms we can find two top-level concepts that can be modelled as services. The first one, namely a Resource, is provided by suppliers and do not have direct interaction with users. Instead, a Resource is represented by the platform as a building block that creators may use to compose Services, which is the second top-level concept. Therefore, in our information model, one Service is compound of one or more Resources, while one Resource can take part from none to several Service compositions.

Both Services and Resources must be completely described so that the platform is able to properly manage and operate them. Although every single Service and Resource will have its own characteristics, they will also share some commonalities and thus we propose to describe them following the same root Specification. The Specification is then extended to ResourceSpecification and ServiceSpecification to describe the specific characteristics of Resources or Services. In order to keep the relationship we have defined between Services and Resources, we state that a ResourceSpecification is associated to none or many ServiceSpecifications while a ServiceSpecification refers to one or many ResourceSpecifications.

All these concepts and their relationships are shown in the following figure. We have added the prefix *UserCentric* to the entities in order to easily distinguish them from other entities later on this chapter.

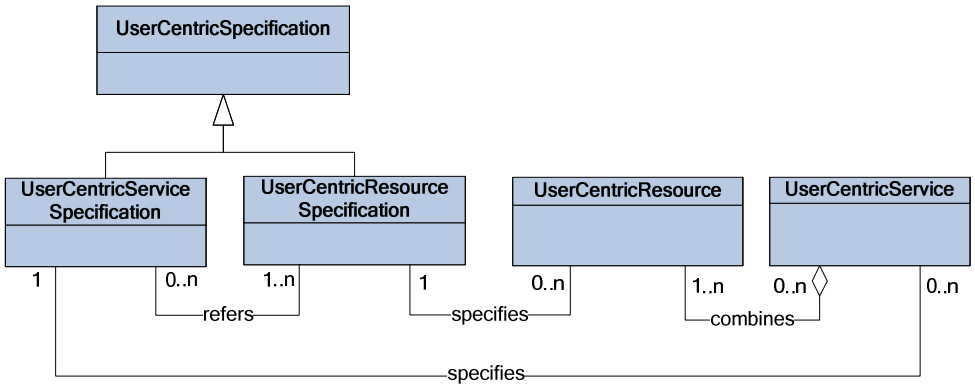

Figure 39 - Resources, Services and their Specification in the information model.

In order to further elaborate on the Specification concept we take some ideas from the SeCSE project [SECSE]. This project made a big effort in creating a specification mechanism which allows providing sufficient information about all aspects of a service description, while maintaining compatibility with standard approaches and being flexible enough to be able to respond to changes that may occur in the near future.

The approach is based on the notion of facets [Sawyer&05]. A Facet is a partial description obtained as a projection of the Service or Resource over one or more Properties. These partial descriptions can be grouped together as needed in order to completely describe a Resource or Service i.e. Facets are aggregated to create ResourceSpecifications or ServiceSpecifications.

Both Services and Resources share the same root Specification. Having common Facets for both groups facilitates reuse of management and operation tasks. However, due to the different description aspects needed for each group, some Facets providing descriptions for Services will not be needed in the Resource description, and vice versa.

Figure 40 adds these new concepts and relationships to the information model partially shown in Figure 39.

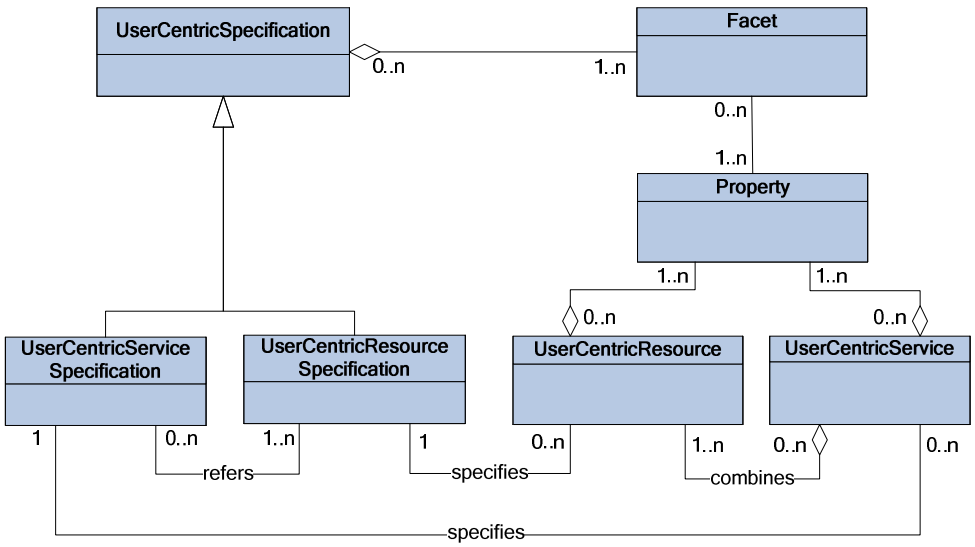

Figure 40 - Facets, Properties and Specifications in the information model.

Now that we know that our Service and Resource Properties will be expressed by means of Facets we can further elaborate on this concept. Since Facets should address purposeful tasks for the platform we have extended the general Facet concept to address

those properties that are required in our platform. These extensions are not based in any theoretical analysis but based on empirical results: We have found these Facets useful or required some time during the development, and thus we have added them to the Facet set. This fact already highlights one of the major values of the proposed information model i.e. easily extensible and flexible enough to cope with new requirements.

Among the set of Facets we pay attention to we can mention:

- *LogicFacet*, which describes the logic that allows a Service execution. Since Resources will be deployed and run out of the platform boundaries there is no need for LogicFacet for Resources.
- *FunctionalInterfaceFacet*, which describes the functionality that either a Service or a Resource offer for consumption.
- *ManagementInterfaceFacet,* which describes the management interface a Service or Resource offer.
- *SemanticFacet*, which provides a semantic description of Services and Resources.
- *PrivacyFacet,* which describes the privacy information that either a Service or a Resource exchange and how this information is internally managed.
- *DeploymentFacet*, which describes the information needed for a proper deployment of a Service. Note that a ResourceSpecification will not contain a DeploymentFacet since Resource deployment is out of the scope of the platform and concerns just the Resource provider.

It is worth noting at this point that the set of Facets that can be used to describe a Service or Resource is infinite, because different user-centric platform implementations will provide different features and requirements, and thus different Facets may be needed. It is not the aim of this dissertation to describe all of them, but just those that are useful to explain our contributions. For an extended list the reader can refer to [OPUCE-D3.1].

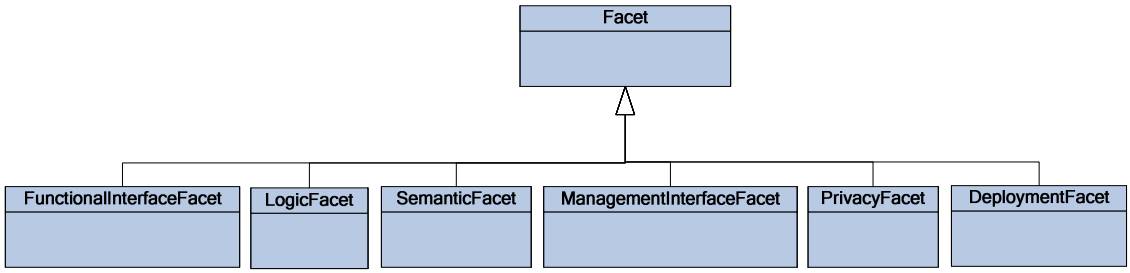

Figure 41 - Facet specialization in the information model.

Facet and Facet extensions are part of the information model, but in order to apply this model to the real world we need a means to specify and describe Facets. For that, we borrow also the FacetSpecification concept from [Sawyer&05], which defines a FacetSpecification as a structured description of the Properties described by the Facet in a given FacetSpecificationLanguage. The FacetSpecificationLanguage is the textual medium for communicating the Service or Resource information the Facet is describing. In most cases a language is expected to be either natural language or XML-based. The former allows for easier human understanding, while the latter makes it easier that software programs can interpret it.

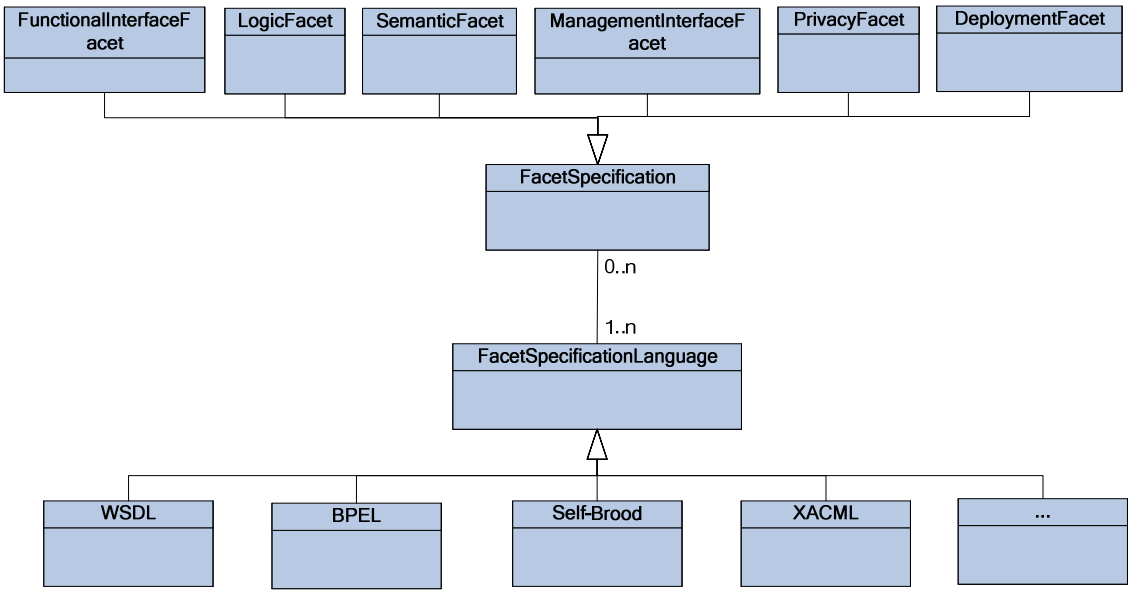

Figure 42 - Facet and FacetSpecification in the information model.

Next table shows a few examples of mandatory, optional, and not applicable (n/a) Facets for both a Resource and a Service in a user-centric service creation and delivery platform. By not applicable it is understood that it is out of the scope of the user-centric platform to provide this Facet since it is not needed e.g. the platform is not providing the logic of a Resource as it is enough to know its interface. An example of possible FacetSpecificationLanguage is given for each Facet too. Note that this do not exclude other languages to be used as the model supports it. However we provide the examples for the sake of clarification.

Table 5 – Facets usage in the description of user-centric services and resources.

Facet	*Resource*	*Service*	*Language*
Service Logic	n/a	**Mandatory**	BPEL
Functional Interface	**Mandatory**	**Mandatory**	WSDL
Semantic Description	**Mandatory**	**Mandatory**	OWL
Management Interface	Optional	Optional	WSDL
Privacy	Optional	Optional	XACML
Deployment	n/a	Optional	SPML

Two Facets are mandatory for a Resource, namely the functional interface and semantic description. The former is intended to describe the interface the Resource will offer for composition. The latter allows the Resource to be looked up in a repository or catalogue. As for Services one more facet is mandatory i.e. service logic. This Facet will describe the logic the Service executes. In a user-centric platform this Facet is generated during the creation process after the creator has composed the new Service.

The other Facets are all optional, depending on the capabilities of the user-centric platform and the particular Resource or Service. For example, a deployment Facet can be supported by the platform, but may not be needed for some Services. Quite in the same line the management interface is useful when Resources must be managed by the platform. Sometimes though the Resource owner will not allow an external entity to

manage its resources or simply might be nothing to manage, hence the ManagementInterfaceFacet will not be needed.

To conclude the description of the information model we highlight again its flexibility and extensibility. In order to create a new ResourceSpecification or ServiceSpecification, the main tasks to do are:

- Select and define the Facets that are needed to solve the problems we face, and;
- Find or create the languages that will be used to express the new facet. Some facets could not be described using a standard or already defined language. In this case, new languages may be necessary for these facets.

Finally, we put all the concepts together in the next figure, where the whole information model is represented.

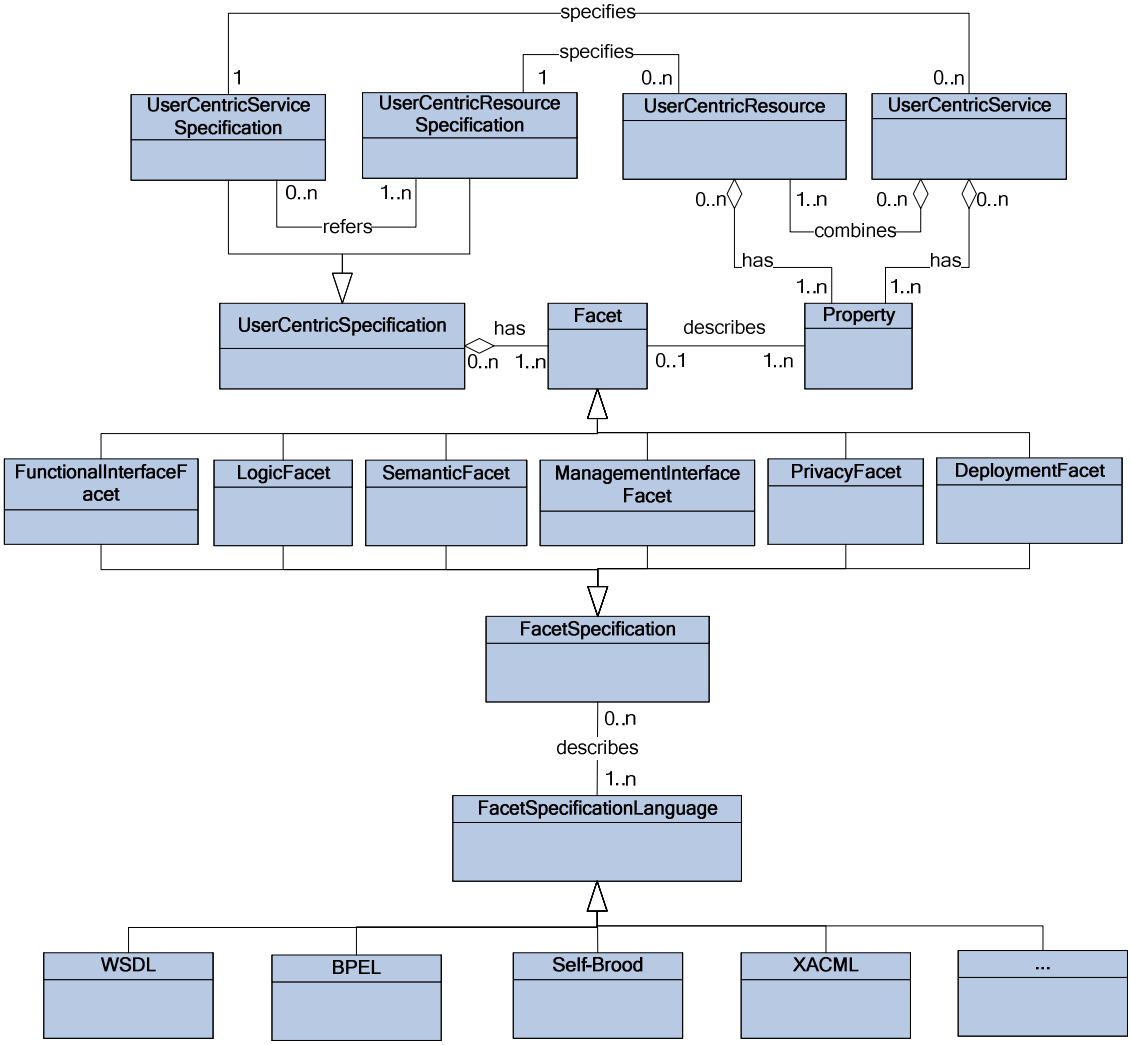

Figure 43 - Information model for service and resource specification.

6.2 Information model implementation

Once the information model has been defined, this section provides further details on how it can be implemented. For that, we begin with two top-level concepts: the UserCentricSpecification and the FacetSpecification.

The UserCentricSpecification must contain the following information:

- ID (mandatory). An internal identifier to uniquely identity this Service or Resource.
- Name (mandatory). A human-readable name, which is given to a Resource by its supplier at the time of delivery and is given to a Service by its creator at the time of creation.
- Version (mandatory). To distinguish between versions in case of Service or Resource evolution.
- Set of Facets. This set includes the mandatory facets as described in **Table 5**, and the optional facets that complete the description.

Each Facet will describe just one type of properties (FacetType) for the Service or Resource, but it can have several descriptions for the same FacetType. For example, the service logic Facet could be described by means of an orchestration of resources, or it might be decided that a choreography for these resources could be a better approach. One or another will be used depending, for instance, on specific performance and scalability requirements. To have into account these requirements, each FacetDescriptor contains the description of the language used to implement a Facet (ImplementationLanguage) and a link to its implementation (ImplementationLink).

Figure 44 shows the UserCentricSpecification structure and its internal elements. This data model has been implemented as an XMLSchema.

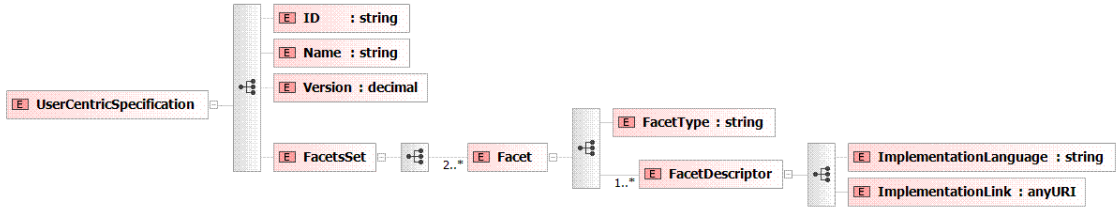

Figure 44 - Specification structure for user-centric services and resources.

The target of the ImplementationLink is an instance of the FacetSpecification implemented using a particular description language. The FacetSpecification, besides providing information about the FacetType and ImplementationLanguage used, includes the ImplementationData i.e. the code in the ImplementationLanguage that describes the Resource or Service properties. The reason for describing the FacetType and ImplementationLanguage in both UserCentricSpecification and FacetSpecification is because these information structures might be stored in different places.

The proposed FacetSpecification structure is shown in the following figure and has been implemented as an XMLSchema too.

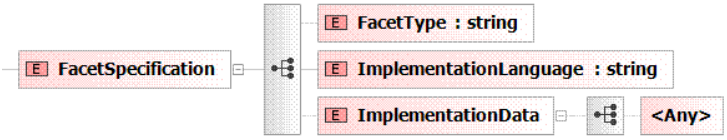

Figure 45 – Specification structure for facets.

Next figure shows the relationships among the elements of a UserCentricSpecification (left) and a FacetSpecification (right).

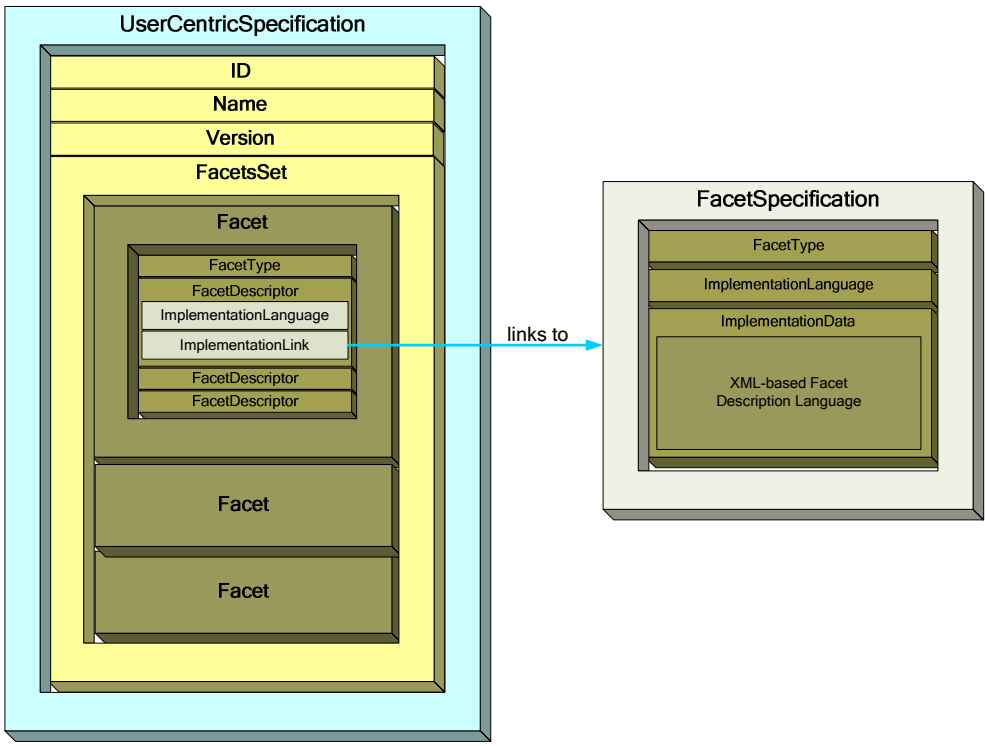

Figure 46 – Faceted service specification structure.

6.3 Relationship with the platform architecture

We use the specification structure to completely describe services and resources, and to support the platform in driving them through the different steps of their lifecycle. Although we do not detail here how the different modules manage the different facets this section provides an overview on how the resource and service descriptions are generated and introduced into the platform. Next chapter will thoroughly describe all the processes and modules involved in the management of a facet, namely the privacy facet.

6.3.1 Resource description

The resource supplier uses the Resource Delivery Application to supply the platform with new resources. This application allows suppliers to describe their resources, providing at least a semantic description and the functional interface. This information is internally used by the Resource Delivery Application to generate the resource specification and facets.

Then, the Resource Delivery Application sends the resource description to the Resource Delivery Manager, which first deploys the new resource to an available Resource Adaptor and then stores the resource description and status into the Resource Inventory. The new resource is then available for composition (Figure 47).

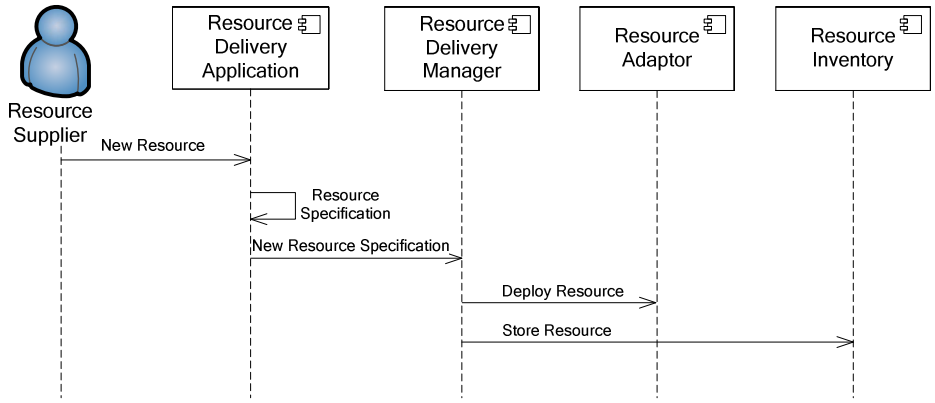

Figure 47 – Sequence diagram for the resource delivery process.

6.3.2 Service description

The service creator uses the Service Development Application to compose a new service from the set of available resources. This application carries out all needed processes to automatically generate the service description and facets from the user composition. If further information is needed, such as semantic information, the Service Development Application will ask the creator for it. Once the service specification has been generated, the Service Development Application sends it to the Service Development Manager, which in turn stores it into the Service Inventory and signs the Deployment Manager that a new service has been created. The new service is now ready for subscription (Figure 48).

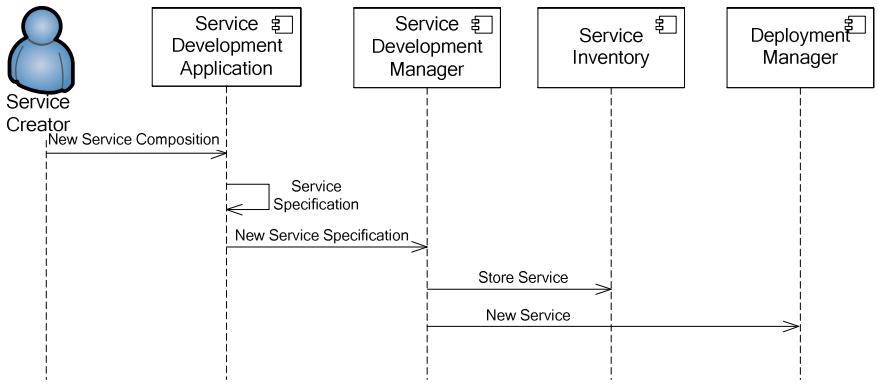

Figure 48 - Sequence diagram for service delivery process.

6.4 Relationship with TMF specifications

The TeleManagement Forum's Shared Information/Data Model (SID) [TMF-GB922] is building a common language and information framework that will allow common representation and a standardized meaning for terms used in the management domain. Due to its relevance in the management and Telecommunications domains and since our information model also targets these worlds this section aligns the described information model with the one described in the SID Service Addendum [TMF-GB922-4SO].

TMF SID defines the top-level terms Product, Service and Resource. Products refer to what is offered to the market, while Service refers to how the Product is implemented: Although Services are the artifacts delivered to consumers they are represented to them as Products. Actually, Products in the service provider environment are realized as

CustomerFacingServices. CustomerFacingServices might aggregate several lower level Services known as ResourceFacingServices, which do not interface the Customer and are related to Resources by means of LogicalResources and PhysicalResources. All these entities and their relationships are shown in Figure 49.

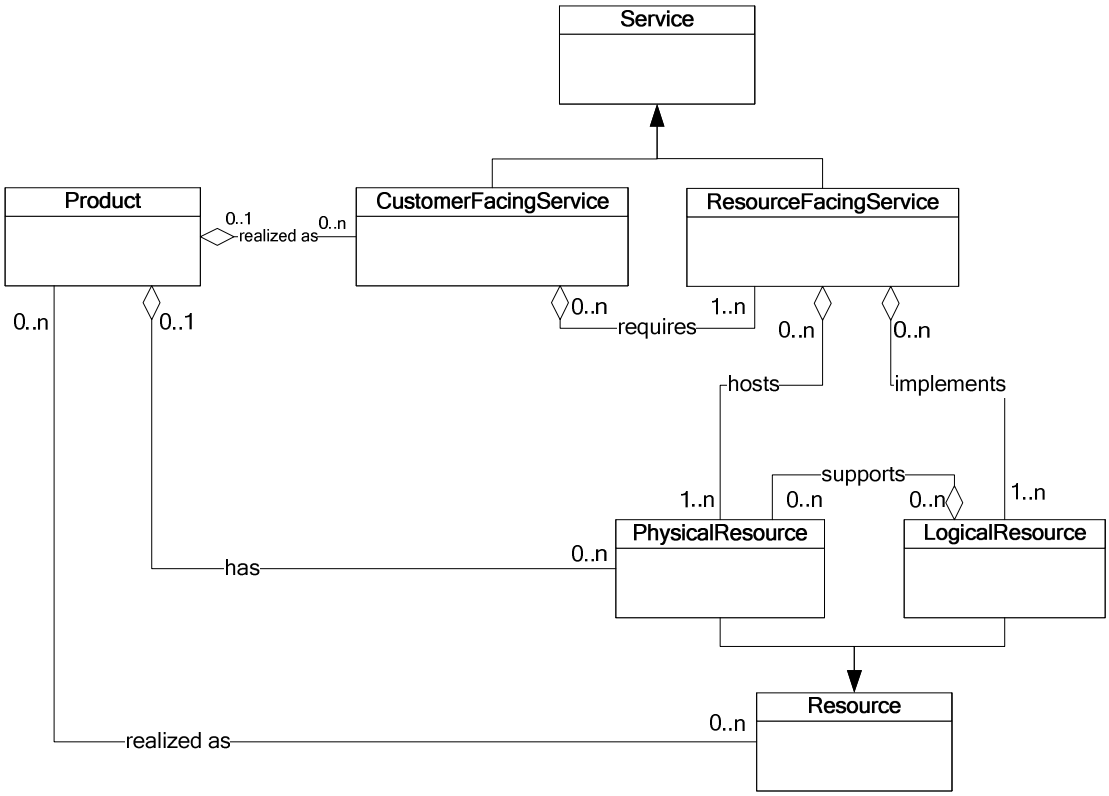

Figure 49 – Product, Resource and Service in TMF SID.

We can map the entities in our information model to the TMF SID ones providing we make some assumptions. First, in our model Products are always modelled as Services following a one to one relationship i.e. one service is directly offered to customers as one product. Therefore, we declare that user-centric services are a specialization of CustomerFacingServices as for the SID terminology.

User-centric services are composed of several lower level software entities (we have called them resources in user-centric platforms) that are not directly exposed to consumers and that are defined and used within the platform but implemented and hosted by a resource provider out of the platform boundaries. Therefore, resources in user-centric platforms can be modelled as TMF SID ResourceFacingService, LogicalResource and PhysicalResource entities. This idea perfectly fits with our definition of resource in user-centric platforms, since a resource is mainly composed of an adaptor to the platform (the ResourceFacingService), an implementation (the LogicalResource) and a host (PhysicalResource) that will really deliver the product to customers. From now on, we will pay attention to the CustomerFacingService and ResourceFacingService, which are the entities we have modelled within the user-centric service creation and delivery platform.

Next figure shows how our information model can be defined in TMF SID terms.

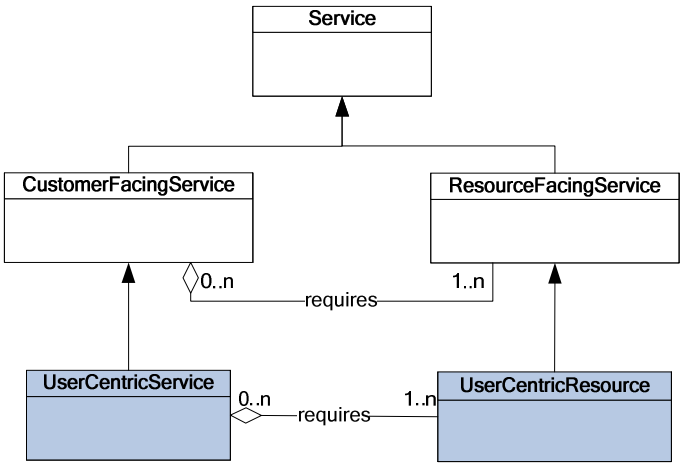

Figure 50 - User-centric services and resources defined in TMF SID terms.

The SID framework also defines a ServiceSpecification abstract concept. It represents a generic means for implementing a particular type of Service. A ServiceSpecification defines the common portion of a set of Services, while Service defines a specific instance that is based on a particular ServiceSpecification. The same applies to CustomerFacingService and ResourceFacingService entities (Figure 51).

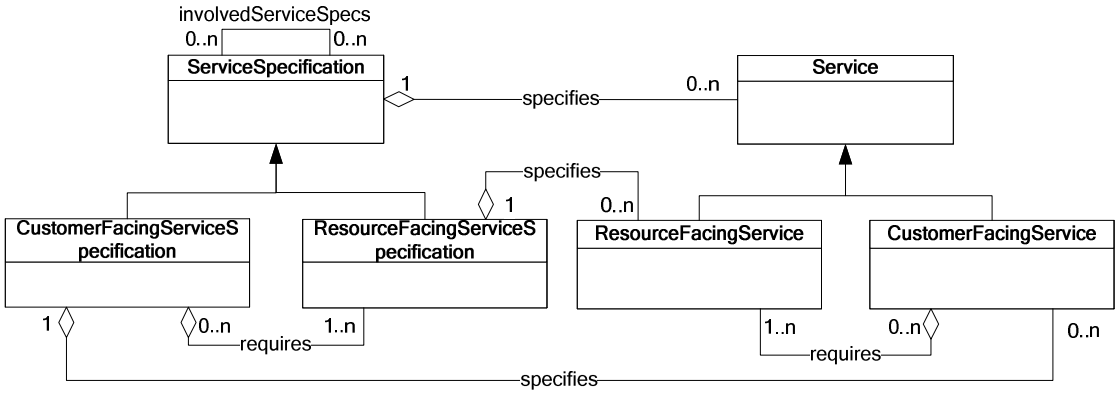

Figure 51 - Service specification in TMF SID.

Following our mapping, we can extend CustomerFacingServiceSpecification to define our UserCentricServiceSpecification. In turn, we also extend ResourceFacingServiceSpecification to define our UserCentricResourceSpecification. This extensions and how they fit into the user-centric service creation and delivery information model are shown in Figure 52.

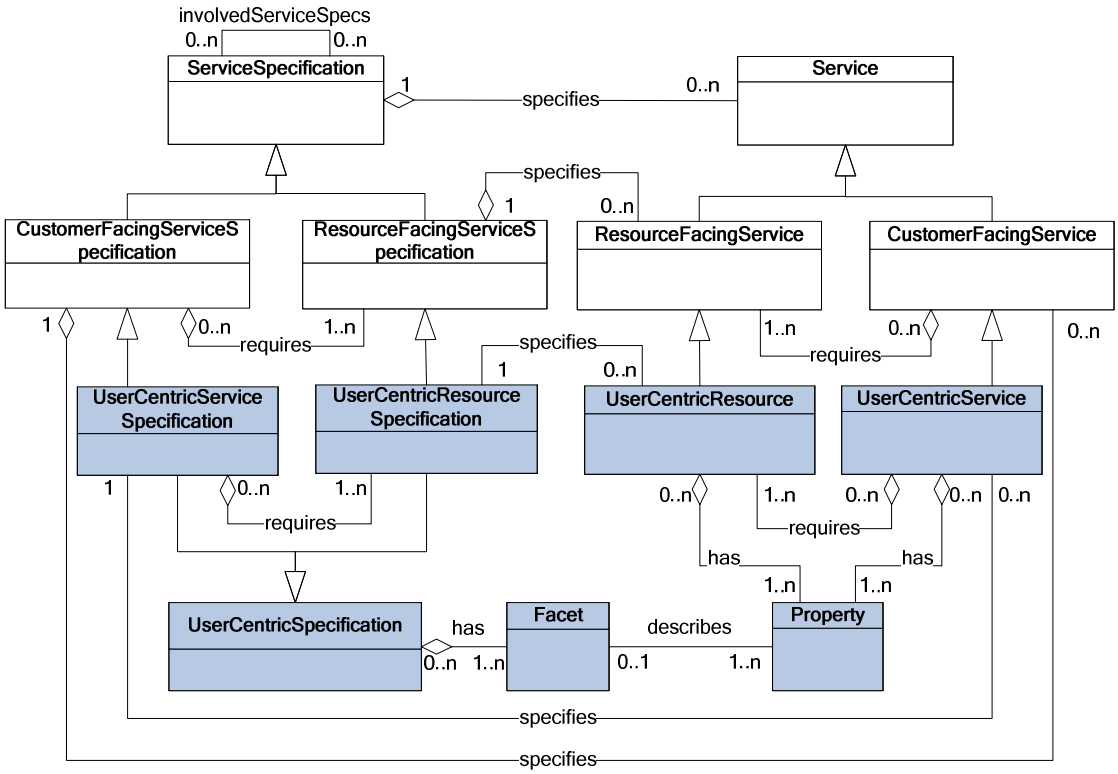

Figure 52 –Service and resource specifications in terms of TMF SID.

6.5 Relationship with OMA specifications

The Open Mobile Alliance focuses on specifying enablers for the service layer in order to create an environment in which communications services may be developed and deployed. For the sake of this work two OMA on-going works are relevant, namely the OMA Service Environment (OSE) and the OMA Service Provider Environment (OSPE).

The OSE sets that every OMA enabler must offer two interfaces, namely the functional interface (I_0) and the management interface (I_1). Enablers can communicate with underlying resources using the resource facing interface (I_2), out of scope of OMA specifications. The OSE does not define nor point to any specific enablers' implementation.

The OSE definition of enabler perfectly fits with the concept of resource we use in this work. We do not mind the resource implementation but just how to use and manage it. Moreover, OSE does not define specific functional interfaces but it states that every enabler will declare its own functionality. Therefore, we can take advantage of OMA enablers and use them as resources for our user-centric service creation and delivery platform.

In order to introduce OMA enablers into the platform they must be provided with a complete resource description, as explained in previous sections. Since we use a faceted approach to describe resources we can map OMA enablers' description to the resource description we use. OMA enablers will need, at least, a functional interface facet and a management interface facet. In order to be included into the platform a semantic description facet must be added, too. Therefore, we can model an OMA enabler as a

user-centric resource which is described, at least, by a functional interface facet, a management interface facet and a semantic description facet.

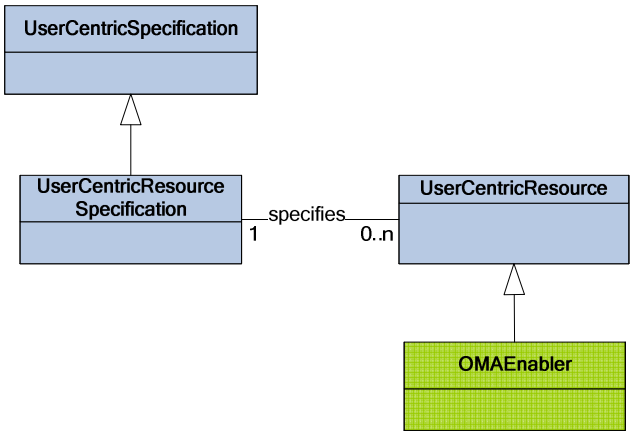

Figure 53 - OMA Enabler modelled as a user-centric resource.

The resource adaptor will be the architecture component in charge of translating messages from the platform to the OMA enabler. The translation can be as naive as routing the message to the destination. However, the adaptor might also need to provide advanced functionality if required by the enabler owner, such as including security tokens in the invocations. Therefore, further facets might be needed to completely describe the enabler.

As for the management interface, it can be directly used by the platform fulfilment, assurance and billing components to manage the enabler. In this case, the resource adaptor must be designed so that it translates the platform management messages to I_1 messages. However, the platform can also take advantage of the OSPE work, which is specifying a new enabler that focuses on lifecycle management, service level tracing and service level management.

Within the OSPE architecture, a Service Model and Catalogue (SMAC) module has been defined. It manages the service model, the deployment instances and the catalogue of data. All this data together supports OSPE in order to execute lifecycle management and level tracing operations in other enablers. OSPE group has considered that the faceted service description we have presented in this chapter perfectly fits the needs of the OSPE SMAC and service description. Therefore, a description of the conceptual model for service specification plus a service specification example have been contributed to the OSPE [OMA-arc08a].

6.6 Chapter summary and original contributions

This chapter has proposed the following original contribution:

- An information model for service and resource description in user-centric service creation and delivery platforms.

First, the conceptual model has been introduced and then a design and implementation based on XMLSchema has been depicted. The relationships with the proposed architecture have been explained too. Finally, the relationships of the conceptual model with related standards have been specified.

This original contribution was elaborated by the author of this dissertation in the context of the OPUCE project [OPUCE]. The information model was successfully developed and validated within the aforementioned project, where it currently supports the

description of all user-generated services [OPUCE-D3.1]. The model was extended with the definition of several facets such as provisioning, simulation, scheduling, etc.

The information model was also used in a Master Thesis conducted in the Departamento de Ingeniería de Sistemas Telemáticos belonging to the Universidad Politécnica de Madrid [Gañan08]. It was also extended in a follow-up project [Martinez09] with the definition of a privacy facet that allows describing privacy requirements for resources and services.

It is worth mentioning that the information model and a service specification example were also contributed to the Open Mobile Alliance Service Provider Environment Architecture group to be included within the OSPE Technical Specification [OMA-arc08a].

7 PRIVACY MANAGEMENT IN USER-CENTRIC SERVICE CREATION AND DELIVERY PLATFORMS

User-centric service creation and delivery platforms deliver the promise of allowing end-users creating, sharing and subscribing the services that better fit their needs. As it was shown in chapter 4, one of the values consumers perceive from a service yields on the level of personalization it provides. And, in the end, personalization requires knowledge of users' identity attributes i.e. services cannot be personalized if the users' characteristics are unknown. When we refer to users' identities we do not mean just static attributes such as favourite colour, given name or mother tongue. Quite on the contrary, those attributes that can provide enhanced value for consumers are dynamic in nature such as location or presence status.

User-centric service creation and delivery platforms pose a risk for consumers' privacy though. Due to the nature of user-centric services some consumer's identity attributes must be shared with the resources the services are made of. Reciprocally, some specialized resources may provide services with identity-based information or functionality such as consumers' location or personal payment services. But resources are provided by third party suppliers, which are out of the platform boundaries, and European and national legislation regarding privacy protection states that users must be informed and provide consent on the use of their attributes when shared among different companies. This is of the utmost importance when it comes to certain sensitive attributes such as location.

Therefore there is a need in user-centric platforms to provide mechanisms that support sharing identity information while allowing users to control and govern its use and release i.e. identity and privacy management. As it was explained in chapter 5, identity and privacy management can be considered as specialized areas for the management and operation of Telecommunications platforms and thus they are generally included within the Operations and Business Support Systems. However, the management of the identity information in user-centric platforms and how to approach user-centric privacy management has not been properly addressed.

This chapter provides a description of some of the author's contribution in this field. These original contributions have been validated within national and international projects, and also in Master Thesis within the DIT-UPM.

7.1 User-centric identity-enabled services

The major value of the use of identity-based information in any service delivery platform probably comes from the enablement of next generation added-value services that specific identity attributes such as location or presence status provide [Roussos&03]. On top of that, proper use of identity information provides better usability and improves the user-experience. It is also at the core of the relationship of the platform provider with its customers, both creators and consumers, and other companies such as the resource providers. Moreover, it increases efficiency, enhancing security and open new revenue opportunities. Thus, the use of consumers' identity information provides benefits for all the roles in the business model.

The following benefits derived from the use of identity information can be highlighted:

- Automated access to the service portfolio supported by single sign-on and dynamic service discovery and invocation, which enhances the usability of the platform and the consumers' user-experience.
- Service adaptability and context awareness, which allows services to react according to the circumstances under which they operate. These circumstances are usually based on consumers' identity attributes such as location, presence status or consumer's device.
- Service personalization, which allows service creators to customize pre-existing services and components based on personal attributes and user profiles.

User-centric service creation platforms can benefit even more than traditional service delivery platforms from the use of identity attributes. Since services are created by users that share them with other users, creators must be provided with means to prepare the services for automatic personalization. For example, tags representing identity information provide a way to include consumer's identity attributes in services before knowing who the consumer is. The identity tag will be automatically replaced with the real value it represents at runtime. In this way the platform place the consumer in the centre of the universe of services.

7.1.1 An identity-enabled service example

In order to better explain the contributions described in this chapter we use an example of a simple identity-enabled service that can be created with a user-centric service creation and delivery platform: *MapMe*. This service allows users to receive a map of their surroundings by sending a premium SMS. The service logic is quite straightforward: First, the service will obtain the user's geolocation; then a map centred in that position is retrieved; and finally, the map is sent back to the consumer by MMS. Taking this description into account, the following resources must be orchestrated by a creator: Geolocator i.e. a geolocation service, Mapper i.e. a map server, MMSSender i.e. Multimedia Messaging Service (Figure 54).

Figure 54 - Example of identity-based service composition.

This service requires identity information about the consumer to properly work. Some of this information can be gathered from the platform (incoming message number) but some other is provided by special resources, which we refer to as identity-enabled resources. For example the Geolocator resource provides the consumer's location.

Since identity-enabled resources provide very sensitive personal information only services working on behalf of the consumer should be allowed to retrieve it. Besides, not all services invoked by the consumer must be allowed access to identity information but just those the consumer trusts. As a result, services must be authenticated before accessing an identity-enabled resource, and then the authorization to retrieve sensitive information must be checked. To avoid degradation in the user experience, the platform should automatically authenticate services against the identity-enabled resources.

Finally, our example service uses MMSSender to deliver maps to consumers. MMSSender requires the destination number to work, which is a consumer's identity attribute. If this resource is provided by a third party provider legislation must be

considered since personal identifiable information will be sent out of the platform domain.

7.1.2 General requirements

Taking into account the European Union Data Protection Directive [EU2006-24], we can derive the specific requirements for each role in a user-centric service creation and delivery platform:

1. The platform must not release and the resource providers/service creators must not collect attributes that are irrelevant for the resource/service they provide. A special case is that when a resource is not interested in the consumers' attributes but on gaining access to the resource. In this case the platform should derive the authorization from the consumer's attributes without releasing any of them. In any other case the resource provider must explicitly specify the attributes that is processing e.g. MMSSender must specify that it is processing the consumers' mobile phone number.
2. The platform must explicitly state the purposes of the personal data it processes. Resource providers and service creators must also explicitly state the purposes of the data they process, so that consumers are always informed about the use and release of their personal information.
3. The platform must ask for consumer consent for the set of attributes it is processing. Each service must also ask consumers for consent for the set of attributes it is processing. When asking for consumer consent, the statement that describes the purpose and the relevance of the attributes must be available. Furthermore, users must also be informed about which final entities may use their attributes (as it is stated in the Article 10 of [EU1995-46]) i.e. the resources that will consume that information.
4. Consumers must be allowed to query the set of identity attributes the platform or its resource providers have got about them, and to correct them when they are not accurate. They must also be able to grant or deny access to them, and to know which providers have used them.
5. The platform should provide a liability disclaimer to prevent misuse and abuses by service creators, resource providers and service consumers. Resource providers and service creators should also provide liability disclaimers for the use of their resources and services.

As we have shown, the platform and the resource provider are the roles directly affected by the privacy and data protection directives as they must declare the identity attributes they use and reason for using them. They should also include liability disclaimers to prevent misuse and avoid abuses. These requirements are quite straightforward and they could be fulfilled beforehand. Next section describes the author's proposal to fulfil the others.

7.1.3 Proposal

The approach we propose to fulfil the requirements described in the previous section is:

1. **Provide an identity management infrastructure**. This infrastructure must support the use of identity-based services by consumers, the composition of identity-enabled resources by service creators, and the sharing of identity information between services and resources.

2. **Provide a privacy management infrastructure** that allows describing the set of identity attributes that services and resources use and/or release, and the reason for using them. The Management and Operation Environment must provide the means for resource providers to include this information when delivering identity-enabled resources. The description for services must be seamlessly and automatically generated by the platform using the available information.

   Additionally, the privacy management infrastructure must provide a user-centric privacy control i.e. consumers must be allowed to decide their privacy preferences, to manage their personal information, and to control who and when has accessed these data. The preferences must be automatically checked before the consumer subscribes a service to ensure that the service does not violate them. Besides, privacy preferences will be enforced at runtime, so that no personal information is released without consumer's consent.

7.2 Identity management infrastructure

An underlying identity management infrastructure is needed to support identity-enabled resources and their composition into services. In our context resource providers belong to different administrative domains and thus we have chosen a federated solution as a basis for our proposal: It supports that each company maintains its own customers repository with accounts and associated identity attributes, and identifies each user properly when required.

In particular, we follow the Liberty Alliance approach to federated identity management. The Liberty approach associates providers into trusted domains called circles of trust allowing the definition of trust relationships among them. Inside a circle of trust, users can federate (link) isolated accounts that they own across different providers. Some entities could be especially prepared to manage these federations, as well as providing some other ancillary services. They are called identity providers (IdP) and play a central role within the Liberty architecture. (For more information on federated identity management and the Liberty approach the reader can refer to Chapter 3 section 5).

We envision that in the context of user-centric service creation and delivery platforms the platform provider will play the role of IdP of the circle of trust, authenticating users and asserting their identity to resource providers as needed. Besides, the platform will be the entity that queries or invokes the identity-enabled resources on behalf of the services deployed on it. The platform provider can also deploy other entities such as a Discovery Service, which allows the dynamic discovery of identity information and the resources that store it.

Reciprocally, resource providers can affiliate to the circle of trust so that their customers' accounts can be federated with the one they have at the platform. The resource provider affiliation is part of the capability delivery process included within the resource supplier lifecycle already described in chapter 5, section 1.1. A framework supporting the dynamic incorporation of third parties into a circle of trust and the mechanisms underlying have been described by the author in [Yelmo&09a]. Taking advantage of this framework, new resource providers can be incorporated automatically, dynamically negotiating and accepting service level agreements to control their activities. The collaboration is not only limited to third party providers, but it may also be extended through collaboration agreements between platforms [Yelmo&09a].

The trust relationship between resource providers and the platform enables features such as single sign on, which avoids that the user and the service she is invoking must be authenticated every time an identity-enabled resource is requested. Resource providers might receive also identity information as part of the resource invocation e.g. the request to Geolocator requires a user's identifier and the request to MMSSender requires the consumers' mobile phone number. Additionally, resource providers can release identity information regarding the consumer e.g. Geolocator sends back the location of the consumer, which is needed as for the service logic.

Apart from the information retrieved from external resources, the platform must also store some identity information. For example, in the MapMe service, once the consumer sends the SMS requesting the map the platform catches the invocation and retrieves the consumers' phone number, which is used to deliver the map using the MMSSender. However, this information is also needed to identify the consumer within the platform and, for example, to apply her privacy preferences as needed or to account for the billing information. Therefore, the platform will have a Customer Inventory, which stores and provides consumers' identity attributes.

Summarizing, the use of a federated identity management infrastructure ensures the management and selectively disclose of user-related identity information within the platform and with its resource providers, while preserving and enforcing privacy, data protection and security needs. Figure 55 provides an overview of the federated identity management infrastructure that supports the use and sharing of identity-enabled resources.

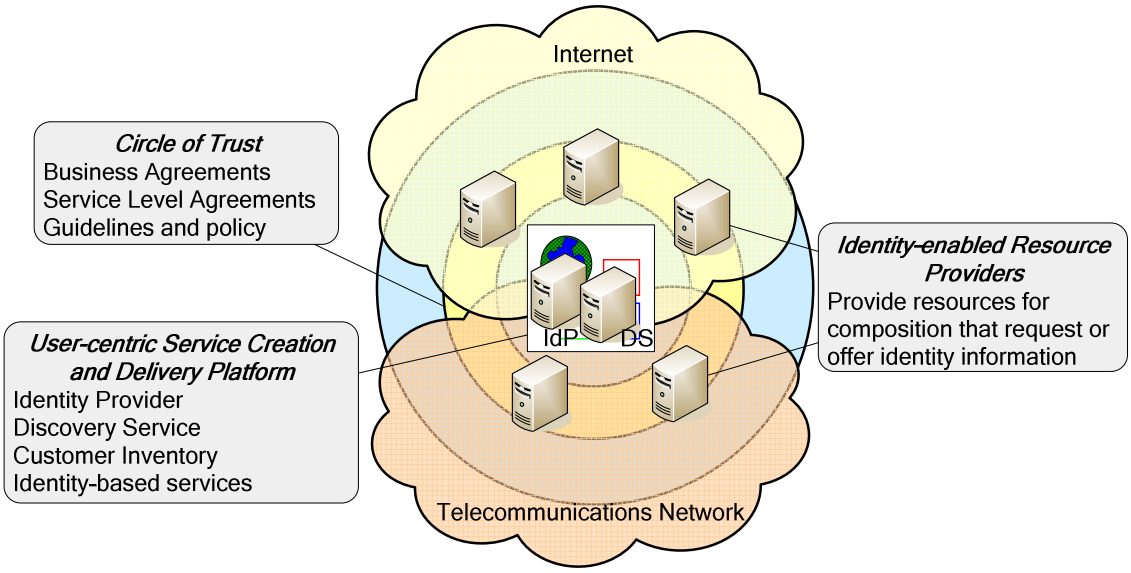

Figure 55 – High-level view of the identity management infrastructure.

Resource adaptors play an important role in this infrastructure, as they translate invocations from the service and the orchestration engine to the identity-enabled resources avoiding the overhead and complexity of Liberty protocols: Services do not need to understand Liberty protocols. The sequence works for our example as follows (Figure 56):

1. The consumer sends a premium SMS requesting the MapMe service.
2. The request gets the platform and is forwarded to the Service Execution Engine, which extracts the telephone number that sent the SMS. The Service Execution

Engine uses the IdP to get the consumer's identity in the platform, and pass the request on to the MapMe service.

3. The service, following the logic dictated by the creator, invokes the Geolocator using the consumer identifier.
4. The invocation gets the resource adaptor, which queries the Discovery Service for the consumer's alias in the Geolocator provider, as well as an End Point Reference (EPR, usually an URL) and credentials that will allow the access to the resource.
5. Using the EPR and the credentials, the adaptor invokes the real resource.
6. If the credentials are valid, the Geolocator sends back the consumer's location to the adaptor, which in turn forwards it to the MapMe service.

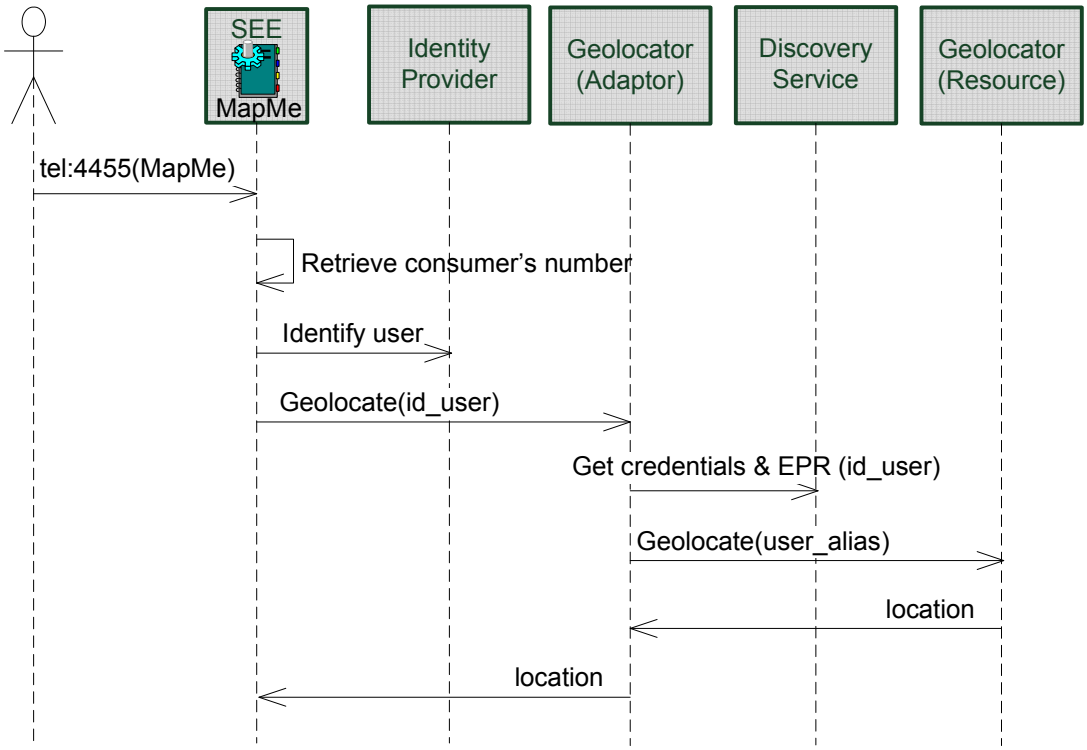

Figure 56 –Resource adaptor proxying an identity-enabled resource.

The details of the identity management infrastructure are out of the scope of this dissertation. They are given here just to complete the description and to provide an overall vision of the original contributions that the author proposes. For further details on a proposal of identity management infrastructure for a user-centric service creation and delivery platform the reader can refer to [Trapero09].

7.3 Privacy management infrastructure

The privacy management infrastructure must consider at least two different privacy dimensions to properly guarantee the protection of consumers' personal information. Firstly, privacy must be analyzed from the platform point of view. Secondly, privacy must be analyzed from the consumer point of view. These two approaches must be aligned to ensure a complete privacy management in user-centric service creation and delivery platforms. As a result, we can describe three types of policies to manage the use of identity information:

- ***P0 – resources and services statements***. They express the resource or service relationship with the consumers' identity information. For example, I need the consumer's credit card number to charge the service delivery or, I need to authenticate the consumer you work on behalf of in order to release the location. This information can be enriched with detailed information, for example, regarding the retention policy to apply i.e. I will retain your credit card number for 3 weeks, or I will delete it after your session expires.
- ***P1 – consumer's preferences***. They are dictated by users themselves and express what they want to be done or not done with their identity information. For example, I do not want to provide my credit card number to any service or I do not want to use services that request my location.
- ***P2 – identity governance policy***. They actually govern what is done with the identity information at the point where it is stored i.e. the resource provider in our case. Identity governance policies must mirror consumers' preferences so that they enforce what users have decided.

Other policy types can be identified such as the service acceptance conditions (e.g. Do not accept credit card number unless...) or the governance conditions upon information release (e.g. If you receive the credit card number, you must delete it after 3 days) [Madsen&06]. We do not consider these policies in our work (Figure 57).

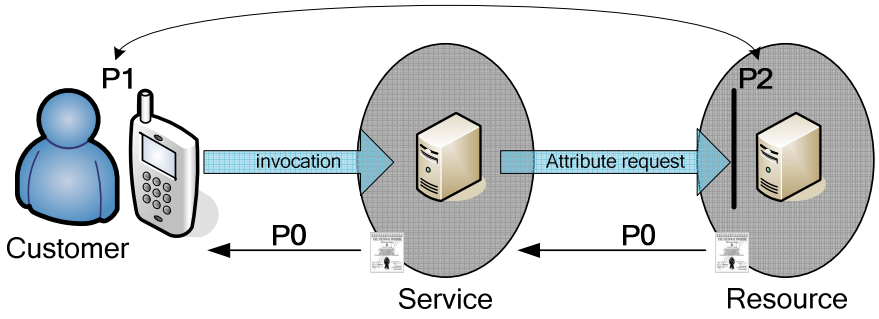

Figure 57 – Different dimensions of privacy policies in user-centric platforms.

On the one hand identity-enabled resources and services provide a description regarding their use of identity information (P0). On the other hand consumers must be allowed to describe their preferences (P1), which are checked against the service descriptions (P0) and translated into policies that govern the use and release of identity-enabled resources (P2).

7.3.1 Privacy management from a platform viewpoint

A user-centric based service platform requires major flexibility and dynamism in managing privacy and data protection compared to current service management systems. In order to automate the processes between the creation and the execution of the services we have taken advantage of the information model defined in chapter 6. The information model has been extended to include a new facet, namely privacy facet (Figure 58). This facet contains the privacy statement for the identity-enabled resource or service and includes the set of identity attributes it is processing and the purpose. Other information can be added such as the intended recipient and the retention policy that will be applied.

In our conceptual model each facet is described in a separate XML-based specification. This allows us to choose any XML-based language to express the privacy policy as far as it complies with our requirements. The Platform for Privacy Preferences (P3P) [W3C-P3P] is a protocol developed by the W3C that defines an XML-based language through which services can describe their privacy policies in a machine readable format. Categories of information include different types of data being collected, the purpose(s) for collection, and which organizations will have access to the collected data. It covers enough of our requirements regarding privacy policies.

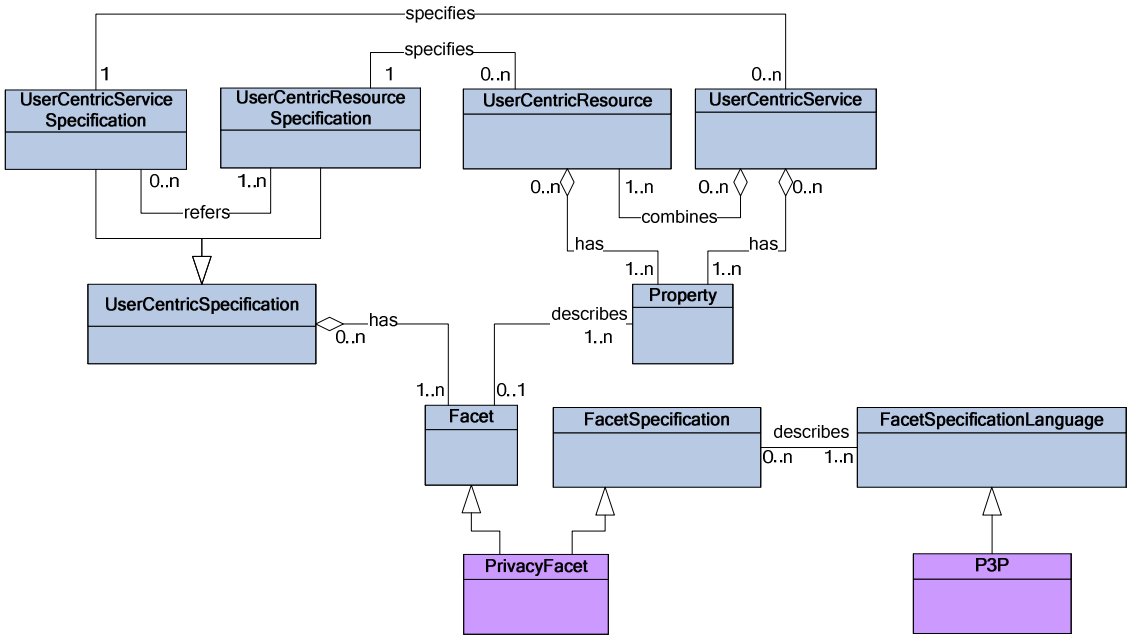

Figure 58 - Privacy policy in the service and resource specification.

Resource suppliers use the Resource Delivery Application to supply the platform with new identity-enabled resources. This application allows suppliers to describe their resources including the functional interface and the privacy statement. At this point it can be checked if both descriptions are aligned i.e. if the identity attributes have the same name and type in both descriptors. The information is internally used by the Resource Delivery Application to generate the resource specification and facets, which are stored in the Resource Inventory and used to deploy the new resource.

As for identity-based services, the service creation process begins when the creator uses the Service Development Application to compose a new service from the set of available resources. Once the service is finished the application must automatically generate the privacy statement for it. The process as follows:

1. The privacy facets for the identity-enabled resources are retrieved from the Resource Inventory.
2. The service parameters and internal variables are evaluated and compared with the set of identity attributes requested or provided by the identity-enabled resources (as stated in the resources' privacy facet). For that, the BPEL code generated during the composition is analysed. As a result, the set of identity attributes that the service exchange is worked out as well as the resources that provide or consume them.
3. A new privacy statement that contains the set of identity attributes used by the service and its purpose is automatically generated. Should some additional

information be needed (e.g. the reason for the use of an attribute) the system can prompt the creator for it. The privacy statement is used to create the service privacy facet.

Next figure graphically shows the information used to generate the privacy statement for the MapMe service. Once the service specification has been generated (now including the privacy facet) it is passed on to the Service Development Manager, which stores it into the Service Inventory and signs the Deployment Manager that a new service has been created. The new service is now ready for subscription.

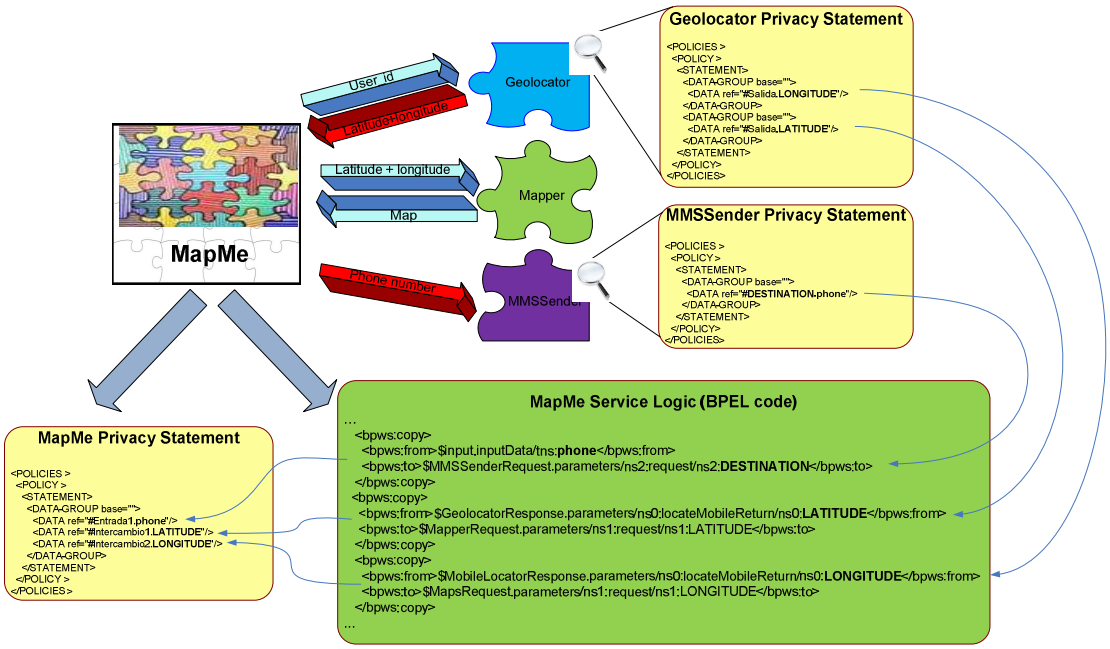

Figure 59 - Information used to create a service privacy statement.

Service subscription is carried out by the Service Subscription Manager within the Fulfilment area. Among the modules involved we pay special attention to the Order Manager, which evaluates the customer order to ensure technical feasibility. One of the steps that are checked here is whether the service can be subscribed as for the consumer's privacy preferences. For that, the Order Manager retrieves the service privacy facet and compares it against the consumer's privacy preferences. The result is that the service can be subscribed, or that the service cannot be subscribed due to the consumer's preferences, or that the consumer must be prompt for explicit consent. At this point the platform must also ask the consumers for their acceptance of the service liability disclaimer.

A user-centric platform is expected to provide enhanced user-experience due to the fact that users are not skilled developers. One simple trick that helps to improve user perception is to show different colours to categorize services regarding the evaluation of consumers' privacy preferences, instead of waiting for the consumer to create a new order and then evaluate (and probably reject) it.

Next screenshot shows the solution adopted in a validation prototype. Services available for subscription are shown using different colours depending on whether there is no restriction for service subscription regarding privacy preferences (green), or the consumers has stated that he must explicitly authorize a subscription to a service that requires some personal attribute (yellow), or the service subscription cannot be carried

out due to mandatory restrictions in the use of personal information (red). When there is some reason to stop the service subscription a short explanation is given (Figure 60).

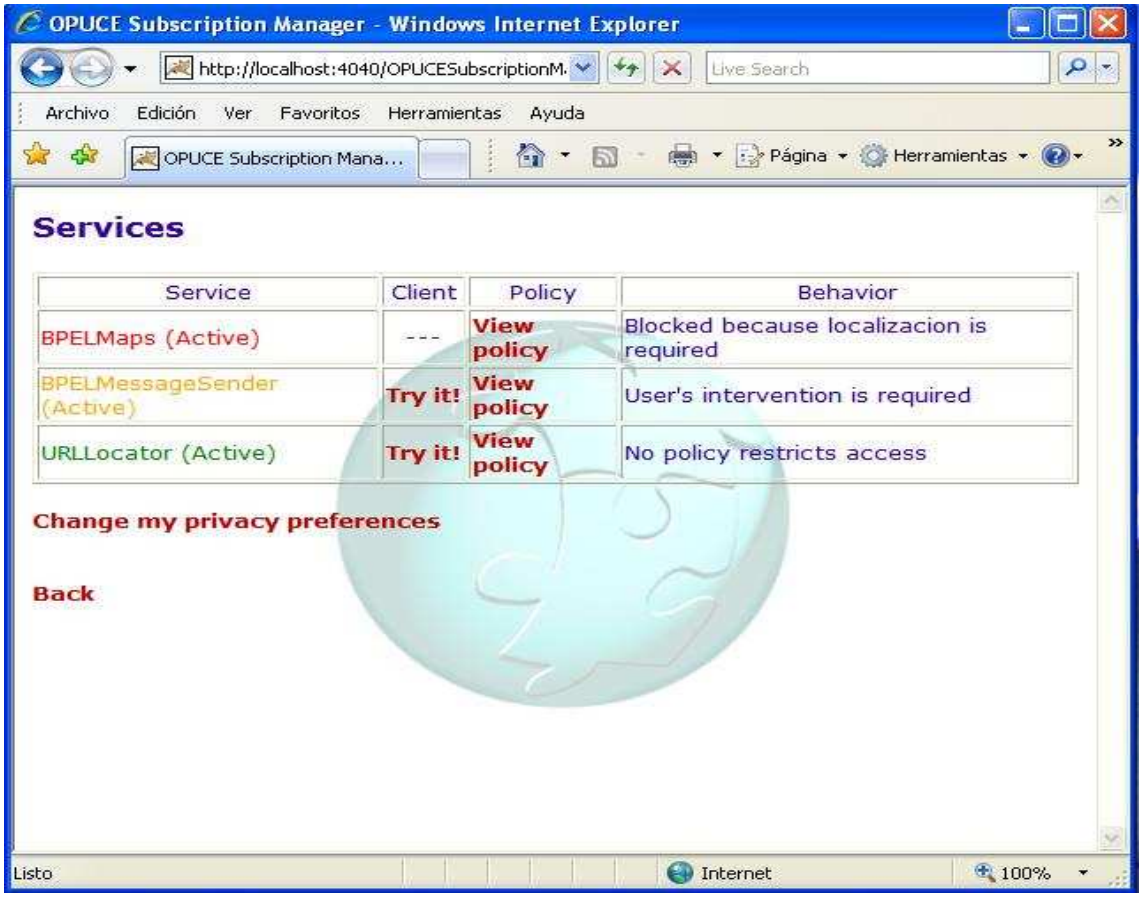

Figure 60 - Privacy preferences evaluation at subscription time.

At runtime, the service execution environment will enforce consumers' privacy preferences, checking whether invocations among services and resources are allowed. Next section will provide details on the steps and components involved.

7.3.2 Privacy management from a consumer viewpoint

The major stakeholder for the privacy management in user-centric service creation and delivery platforms is the consumer. Consumers must be allowed to manage the whole lifecycle of their identity information. This poses a set of requirements to the privacy infrastructure:

- Consumers must be able to retrieve the list of their shared identity-based information and its location (which resource provides it).
- Consumers must be able to access the resources providing identity information about them, and modify or cancel the values of their personal data.
- Consumers have the right to know which services/resources have used their personal information.
- Consumer must be able to govern the access to their personal information.

Figure 61 shows a high-level view of the architectural elements involved and their relationships. The platform module that interfaces the consumer is the ***Privacy Manager***, within the CRM. This module is supported by the underlying identity

management infrastructure, which is deployed both within the platform boundaries (Discovery Service, Identity Provider and Identity-enabled Services) and out of them (Identity-enabled Resources). We assume here that Liberty-based relationships have been setup among these entities, which supports the basic operations of registering identity resources in the CoT (A), discovering identity resources (B) and querying identity resources (C).

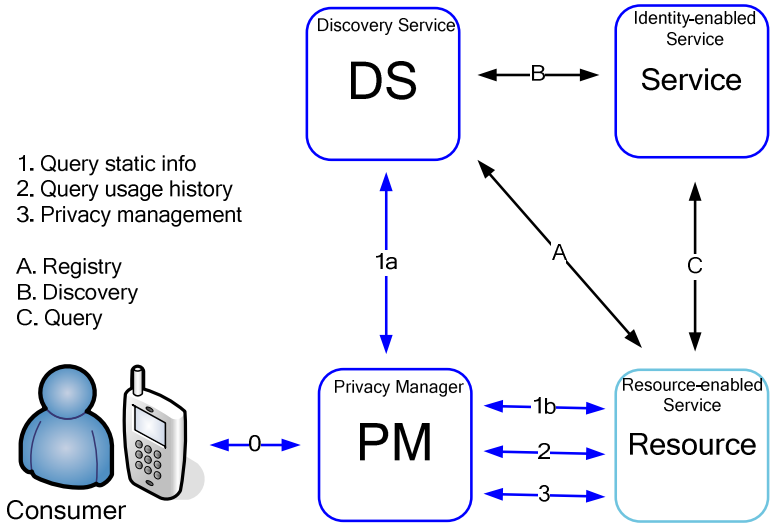

Figure 61 - High-level view of the user-centric privacy management.

To better explain how the architecture works we support our description with three scenarios. The first one allows consumers to retrieve a static view of their identity information i.e. where the identity information is stored and what its value is, and to modify it. The second one allows consumers to query the history of use of their identity information. The last one shows the processes involved when a user manages privileges for the access to his identity information.

7.3.2.1 Scenario 1: Static view retrieval

Consumers use the Privacy Manager to retrieve a static view of all their identity-enabled resources. It queries the CoT to know what identity resources are available for that particular user, where these resources are distributed and, if needed, their specific values. The Privacy Manager also allows users to manage this information.

This scenario is compound of three major steps:

1. Consumer authenticates against the CoT using the Privacy Manager.
2. Consumer gets an overall picture of his/her identity resources distribution.
3. Consumer manages the values of his/her identity resources.

The details of the elements involved are shown in the following picture:

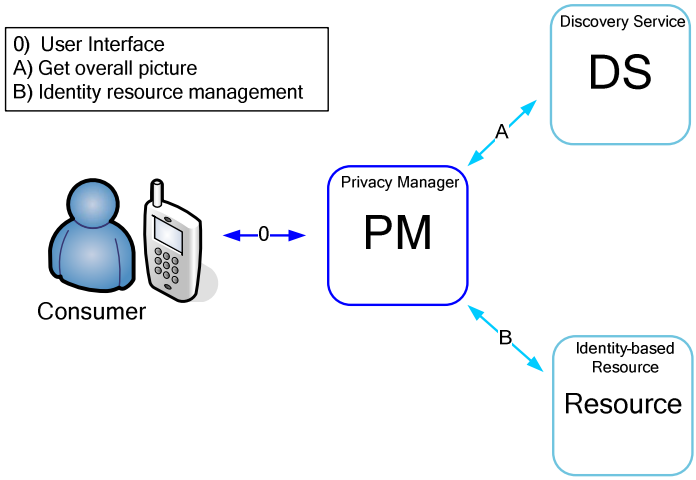

Figure 62 - Details of the components involved in the static view retrieval.

A generic requirement for all the scenarios is that the Privacy Manager must be authenticated, on behalf of the consumer, against the CoT in order to gain access to the CoT entities. Since the user has logged in into the platform, and the platform contains the IdP of the CoT then the user is also authenticated against the CoT. The authentication can be achieved by any of the Liberty specified mechanisms such as Single Sign On as described in Liberty ID-FF specifications or Authentication Service as described in Liberty ID-WSF specifications. At the end of this process the Privacy Manager obtains an End Point Reference (EPR) and credentials to access the Discovery Service (DS bootstrap).

Once the authentication is done, the consumer can get an overall picture of the distribution of the identity resources. Fulfilling this requirement is quite straightforward since it is supported by Liberty ID-WSF protocols [LibertyDisco]. Next sequence diagram shows the entities involved in this process.

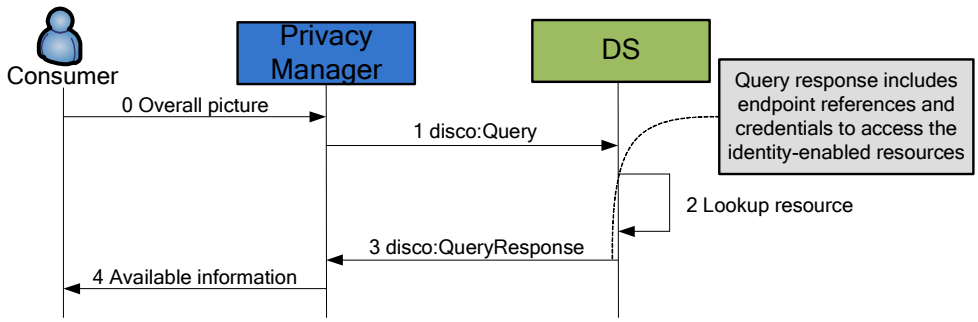

Figure 63 - Sequence diagram for the retrieval of identity resources.

Finally, once the consumer is presented the overall set of identity resources, he can choose one to manage. The management operations include retrieving the value details of one identity resource. Further operations might be available such as updating or cancelling the information.

Data Service Template (DST) is the Liberty protocol that allows an entity in the CoT to access identity resources in order to query/update/cancel personal data on behalf of a user. Thus, DST is enough to fulfil this requirement.

To successfully implement this solution, the Privacy Manager must perform as a Liberty Web Service identity Consumer (WSC) to query or update a Liberty Web Service

identity Provider (WSP). The Privacy Manager got the EPR and credentials needed to access the WSP when the overall information about identity resources was retrieved (Figure 63 step 3).

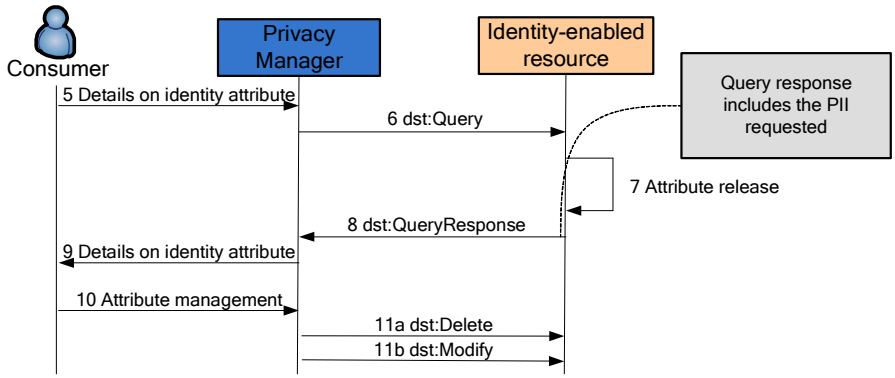

Figure 64 - Sequence diagram for the management of identity resources.

7.3.2.2 Scenario 2: Usage history retrieval

Once the Privacy Manager has retrieved a static view of the identity resources of a consumer in a CoT (Scenario 1), the user is able to know the usage history of one of his/her identity resource and for that he/she selects it. The Privacy Manager shows the history of use of that resource with details about the resource type and value, timestamp of access and the service that accessed the resource. Further information can be presented if available such as privacy promises made by the requestor or conditions imposed on the release of the information.

The Privacy Manager can retrieve the history of use by different means:

- Using Subscription/Notification mechanism [LibertySubs]. Liberty provides standard mechanisms for WSCs to subscribe to different events on identity-enabled resources. Usually these events are related to personal information updates, but other events are not precluded. Therefore, the Privacy Manager should subscribe to notifications in any resource provider who custodies customer's identity resources. Thus, when that provider releases some of these resources it will send a notification to the Privacy Manager. This mechanism is always client-initiated (push mode), and the server is not allowed to request notification information from the client.
- Using Liberty ID-WSF Accounting Service [LibertyAccount]. The resource provider that releases the information must perform as an accounting client and the Privacy Manager as an accounting server. A new event type should be defined by extending the <*event*> complex type as defined in [LibertyAccount]. This new event type must include the information related to the use of the identity resource. This mechanism can be seen as a specialization of the notification mechanism but focused on accounting events. Again, it is always client-initiated (push mode), and the server is not allowed to request accounting information from the client.
- Extending the DST protocol [LibertyDST]. We assume that every resource provider accounts the release of identity resources as in the accounting service. However, we would like the Privacy Manager to be able to request accounting information (pull mode). We consider that the accounting information can be considered as an extension of the customer's identity information: Logs add

relevant information about the identity information consumption. Therefore, we propose to use the DST protocol to access them and for that we extend DST with a new operation: *trace*. This operation will allow the Privacy Manager performing as a Liberty WSC to request a resource provider the usage information about some customer identity resource.

The main benefit of the DST extension approach is that it can be initiated by the Privacy Manager (pull mode). This means that the information will be retrieved whenever the Privacy Manager wants to, and will be limited to what it asks for. Thus, we do not foresee any scalability or performance problems. On the other hand this approach is not Liberty compliance. This means that some new developments will be needed, and that standard products will not support this feature. However, if successful, there is place for standardization of the new (extension) protocol.

The main advantage of the subscriptions/notifications approach is that it is Liberty compliance, and thus no further (out-of-specification) developments are needed. On the other hand, subscription/notification features are not mandatory in Liberty ID-WSF and thus many products might not have implemented it. Nevertheless, implementing a standard feature is always less disruptive than developing and integrating a non-standard one. And as for scalability and performance issues this approach needs one notification to be sent per identity resource and per customer every time a resource provider is accessed. This could cause some performance problems.

The accounting service presents the same advantages than the subscription/notification model regarding Liberty compliance, but it also improves the performance problems because it allows reducing the amount of messages generated by setting thresholds. For example, notifications can be sent in a per access rule i.e. a resource provider sends one single account with information about all the resources accessed, thus reducing the amount of messages. On the Privacy Manager side we do not foresee scalability or performance problems, as it will just receive messages related to the customer it works on behalf of. To conclude, from a functional point of view we would prefer the DST Extension mechanism as it is the only one able to provide a pull mode.

The high level architecture for this scenario is shown in the next figure.

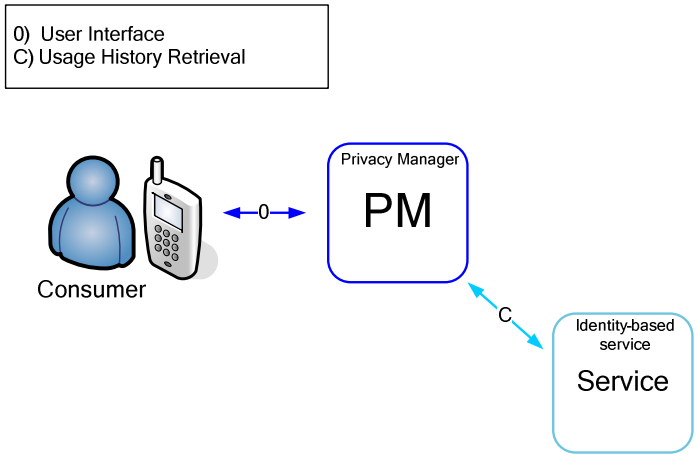

Figure 65 - High level architecture for usage history retrieval.

7.3.2.3 Scenario 3: Privacy management

Liberty specifications acknowledge the need for privacy policy support. For example, the use of policies within the usage directive part of a DST message has been specified. The specifications also describe that both the DS and the WSP must enforce users' privacy preferences when releasing their identity resources. Moreover, an approach for the use of P3P privacy policies has been described [LibertyPrivacy]. However, Liberty specifications do not describe how users can manage their privacy preferences nor set any policy language as mandatory.

This section elaborates on mechanisms to allow users to manage privacy policies describing their privacy preferences. The basic idea behind this requirement is that a user, using the Privacy Manager, must be allowed to decide what can be done with their identity resources.

In our scenario the Privacy Manager has retrieved a static view of the identity resources of a consumer in the CoT (Scenario 1). Now the user wants to set some privacy preferences on his/her identity resources and for that he/she selects one of them. The Privacy Manager shows the current privacy preferences governing that resource and allows the user to modify them.

This scenario is compound of four major steps:

1. Consumer selects one identity resource to see its privacy preferences.
2. The Privacy Manager retrieves and presents the privacy preferences associated to the identity resource.
3. Consumer modifies the privacy preferences and the Privacy Manager updates them in the custodian of the identity resource (the resource provider).
4. The custodian enforces the privacy preferences when some service tries to access the identity resource.

The architecture for this scenario is shown in the next figure.

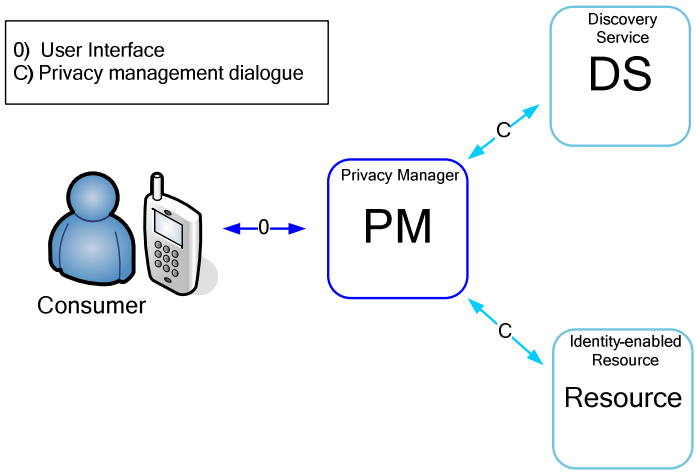

Figure 66 - High-level architecture for user-centric privacy management.

7.3.2.3.1 Privacy preferences

We assume that the user wants to set preferences to control the use of her identity resources in a resource provider. The variables that participate in this preference are: the

service requesting the resource (requester), the resource itself, the operation to perform, the permission granted and the user the identity resource refers to. The requester can be any service that tries to access the resource. The permission can be set to grant, deny or askMe (when the user prefers to decide on a per invocation basis). The resource values are constraint to those defined within those the resource provider offers. The operation values might be the ones defined in DST protocol i.e. query, create, delete, modify and subscribe. Since services will just query resources for information we consider just this operation.

Since the combinations of rules increases exponentially (#requesters x #resources) we should allow for simpler options such as allow anyone to discover this specific resource or allow just this service to discover any resource. Therefore options such as all or just one should be supported.

It might be also possible that users want to set more advanced rules for the release of their information. For example, do not release this identity resource unless it is for one-time use or, whenever someone wants to retrieve this identity resource ask me for permission or, if this identity resource is released then the requestor should delete it in 1 week.

On the one hand checking these rules depends on the information the requestor provides i.e. requestor promises. On the other hand, after checking principal preferences some conditions might be set on the released information i.e. custodian orders. Liberty IGF [LibertyIGF] describes languages (CARML and AAPML) to express both requestor promises and custodian orders, and the mechanisms and protocols needed to interact. However, as far as the authors know there is no available implementation to manage these languages, which makes hardly difficult to consider such aspects in the timeframe of this dissertation.

Once a user's privacy preferences have been set they must be associated to the custodian of the identity attributes it refers to, or more specifically, to the attributes themselves. Assuming an underlying identity management network based on Liberty architecture and protocols, we propose two models to implement this association:

- A new identity profile can be defined in the resource: privacy profile. This approach has the advantage that the privacy profile will be defined once and can be used in every Liberty WSP regardless of the identity attributes it stores. Besides, the privacy profile and repository will be independent of the WSP, thus allowing for easier upgrade of and integration with current deployments. On the other hand, privacy policies are not WSP agnostic i.e. they might refer to identity attributes specific of that profile.
- The privacy policies can be added to the target attribute and profile that contains it as an extension. This approach allows associating the attribute and the privacy policy that governs its use and release. Besides, it does not introduce any new feature to Liberty specifications but leverages on the existing ones. The extension must be defined once and then it can be added to any identity profile. On the other hand the profile must be upgraded introducing non-standard elements.

7.3.2.3.2 Consumers express their privacy preferences

Consumers can express their privacy preferences by different means. For example, they can choose one out of several pre-defined privacy policies and associate it to an

identity-enabled resource provider. Each privacy policy is described in natural language so that users can understand it. This natural language description is mapped to a specific policy described in a privacy policy expression language. Usually, policies are hierarchical so that it is easier for users to compare among them and choose the one that better suits their needs. This approach has been followed in Internet Explorer and in [LibertyPrivacy]. The approach benefits from the simplicity and usability of the model because users do not have to deal with the policy details.

Consumers could be also allowed to define each detail of the privacy policy. Although this approach provides great flexibility in the description of users' preferences it poses some risks for the usability: just advanced users understand (and probably want to know) the meaning of the policy. This should be offered as an advanced option e.g. Internet Explorer provides an advanced button to set users' custom privacy preferences out of the 5 pre-defined levels.

We will go for an intermediate model, quite in the line of Internet Explorer. First, we provide default policies to govern the use of all the privacy information. These policies are associated to consumers' identity resources already known. Then, using the Privacy Manager interface users can change the policy applied to an identity resource selecting one out of a set of pre-defined policies expressed for their commodity in natural language (Figure 67, up). Finally, we go deeper and allow users to define specific options for the use and release of each data of their profile (Figure 67, down).

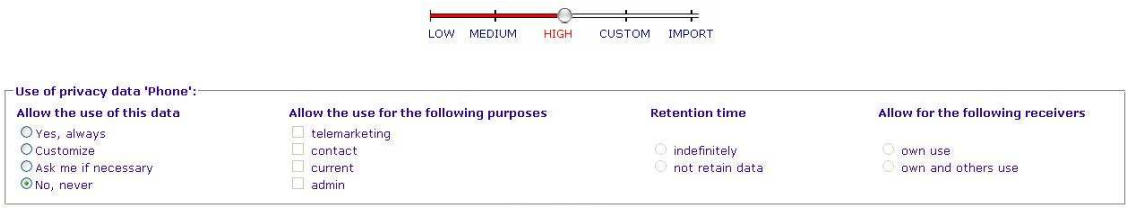

Figure 67 - Screenshot for default (up) and custom (down) privacy preferences.

7.3.2.3.3 Privacy preferences management

We have described how users decide the privacy preferences they want for the resources that store identity information about them and the processes to translate this information into a privacy policy. Now we describe how the Privacy Manager sends this information to the resource provider, and how it can query that information afterwards.

As we have described, privacy policies are associated to identity attributes using an extension of the identity profile. Liberty DST protocol provides the mechanisms to create or update identity attributes defined within an identity profile. Therefore we leverage on DST protocol to allow the Privacy Manager to set privacy policies associated to an identity attribute.

For this mechanism to work, the Privacy Manager must play the role of a Liberty WSC and include the privacy policy as part of the Create or Modify element that is sent to the provider. This mechanism does not introduce any change in current DST protocol, as the policy will be carried as any other information in the body part of the message. On arrival of the policy, the resource will retrieve the policy and store it.

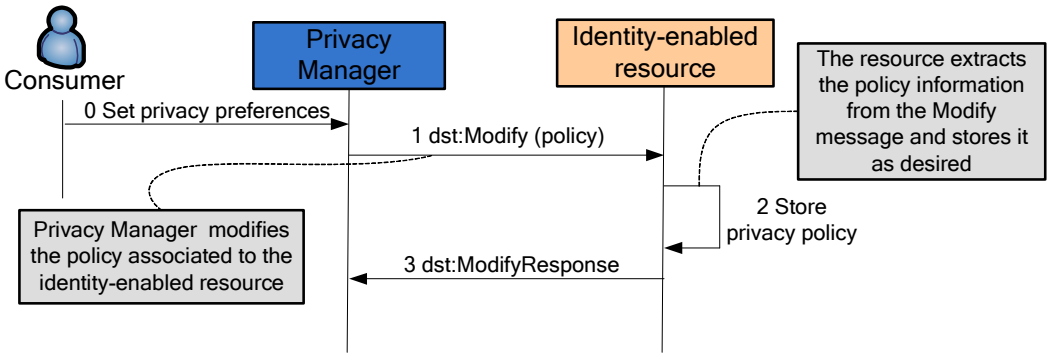

Figure 68 - Privacy Manager setting privacy policies.

Once a policy is associated to a resource, the Privacy Manager is able to retrieve it using the same mechanism that was used to set them: Using DST protocol. In this case, however, the Privacy Manager will use the Query operation. Once the policy has been retrieved it will be translated to privacy preferences so that the consumer can understand it.

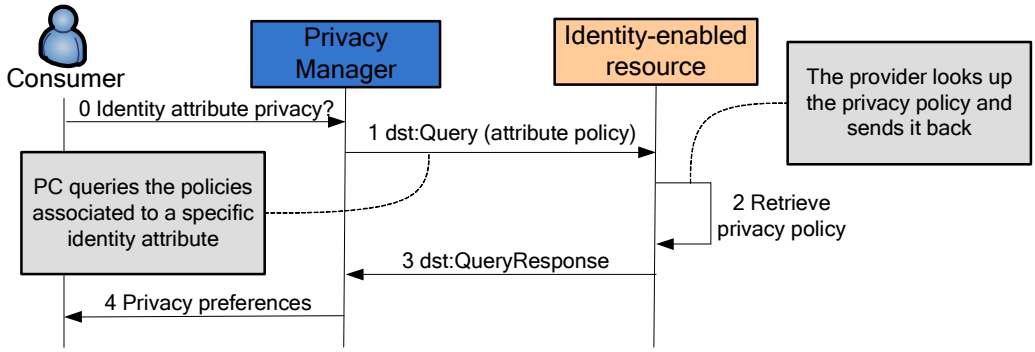

Figure 69 - Privacy Manager quering privacy policies.

7.3.2.3.4 Privacy policy enforcement at an identity-enabled resource

Privacy policies must be enforced whenever a request to an identity-enabled resource is received. In our scenario, two entity types are responsible for policy enforcement, namely the Discovery Service and the identity-enabled resource. We analyze the case of enforcement in an identity-enabled resource, but the conclusions are the same for the case of a Discovery Service.

We introduce three new entities in the Liberty architecture to fulfil our requirements: Policy Enforcement Point (PEP), Policy Decision Point (PDP) and Policy Repository [Yavatkar&00]. The PEP catches the invocation to the identity resource and asks the PDP for authorization. PDP uses the PR to retrieve the policies to apply and decide to grant, deny or take further actions. The decision is communicated to the PEP who allows or denies the request, or takes further actions.

The PEP main task is to retrieve information about the requesting entity, the requested resource and the consumers it refers to. As we have reduced the operations available to just one then it can be set to the appropriate value. PEP creates a request to the PDP with the information retrieved. The PDP receives the request and retrieves the applicable policies from the repository. PDP compares the request and the policies and sends the decision back to the PEP.

When the PEP receives the decision it can release the requested resource, deny the operation or pause the operation until further actions (ask the identity attribute owner)

are taken. The last step can be implemented using a Liberty Interaction Service [LibertyIS].

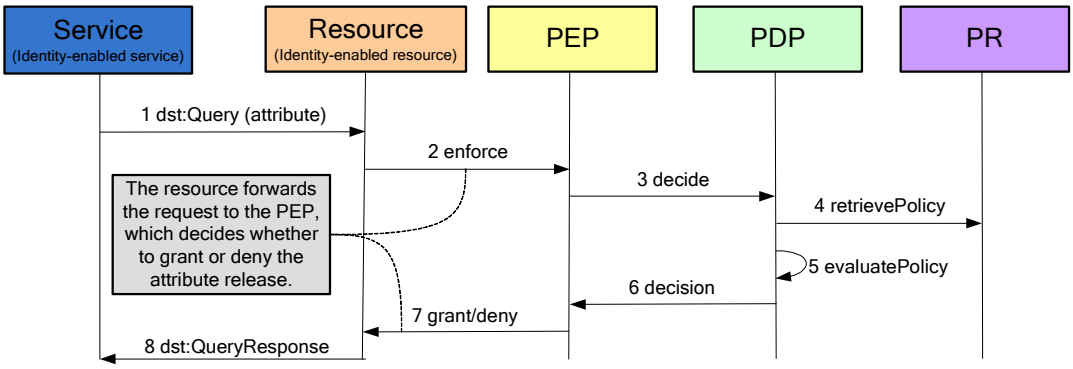

Figure 70 - Sequence diagram for privacy enforcement.

7.4 Chapter summary and original contributions

This chapter has described the author's contributions in the field of privacy management in user-centric service creation and delivery platforms. First, the motivation for the use of identity-enabled resources and services in user-centric platforms has been explained and its general requirements have been described. Then, the underlying identity management infrastructure that supports it has been depicted. Finally, the privacy management infrastructure, its components and the processes and mechanisms involved have been thoroughly described.

Summarizing, this chapter has described the following original contribution:

- A privacy management infrastructure in user-centric service creation and delivery platforms.

This original contribution was elaborated and validated by the author of this dissertation in the context of two different projects, namely OPUCE [OPUCE] and SEGUR@ [SEGUR@]. The former focused on the definition of privacy facets as the means to describe services and resources privacy information. The latter provided the context for the analysis and development of the Liberty-based user-centric privacy management infrastructure. Additionally, the use of privacy facets and privacy preferences in user-centric platforms has been validated in a Master Thesis conducted in the Departamento de Ingeniería de Sistemas Telemáticos belonging to the Universidad Politécnica de Madrid [Martinez09]. To conclude, it is also worth mentioning that some original contributions in the field of user-centric privacy management have been filed as a PCT patent application [P28702WO1] in the European Patent Office, in collaboration with Ericsson España S.A.

Next chapter will describe these and other activities that have supported the validation of the conceptual framework, the reference architecture and the original contributions that have been explained throughout this dissertation. In addition, the most relevant results derived from these contributions will be detailed.

8 VALIDATION AND RESULTS

Next sections aim to provide the reader with an overview of the different actions that the author has carried out in order to validate the ideas and original contributions that have been described throughout the previous chapters. The validation efforts include prototypes that have been developed during Master Thesis that the author has tutored or has collaborated with. Validation has been possible also within national and international research projects the author has been involved in.

In addition, the original contributions have been used to provide further research and scientific results by means of publications in relevant journals and conferences as well as some book chapters. Some of the results of this dissertation have been also awarded after submission to different conferences and prizes. The contributions have also provided industrial results by means of a PCT patent application and contributions submitted to first class telecom-oriented standard development organizations.

8.1 Validation in Master Thesis

The author has worked as research staff in the Departamento de Ingeniería de Sistemas Telemáticos of the Universidad Politécnica de Madrid since the early stages of his PhD. During this time he has had the opportunity to collaborate and tutor different Master Thesis of Telecommunications Engineering students that were finishing their grade. In particular, three of them have been relevant for the sake of the validation of some of the ideas and contributions described in this dissertation:

- ***An open-source implementation of an identity management platform following Liberty ID-WSF specifications [Blanco08].*** This Master Thesis was used to validate the ideas supporting the use of an identity management infrastructure in a collaborative environment. The outcomes and lessons learned were applied to improve the conceptual model for the identity management infrastructure supporting the privacy control.
- ***Development of an open platform for user-centric service composition and deployment [Gañan08].*** This Master Thesis implemented a prototype of user-centric service creation and delivery platform validating the conceptual framework of this dissertation and the reference architecture. Additionally, it implemented the software entities managing the information model that supports the faceted description of services and resources, which allowed its validation and provided some inputs that were useful to improve the information model.
- ***Development of an application prototype for the protection of personal information in user-centric converged services platforms [Martinez09].*** This Master Thesis has been used to validate the original contributions regarding the description and composition of services' privacy statements in user-centric platforms. This work complemented the platform developed in [Gañan08] with privacy features allowing users to seamlessly create identity-enabled services. The modules developed supported the platform in dynamically generating the service privacy description from the resources descriptors. Additionally, this prototype allows users to define their privacy preferences which are checked at subscription time to allow or deny the service subscription. Privacy preferences are also enforced at execution time, thus truly governing the use and release of identity attributes by services and resources in user-centric platforms.

8.2 Validation in OPUCE project

OPUCE stands for Open Platform for User-centric service Creation and Execution. OPUCE [OPUCE] was a research project within the European Union Sixth Framework Programme for Research and Technological Development. It bridged advances in networking, communication and information technology services towards a unique service environment where personalized services are dynamically created and provisioned by the end-users themselves. The general objective of OPUCE was to leverage the creation of a user-centric service ecosystem giving users the chance to create their own personalized services as is currently done on the Internet.

The author had the privilege of working in OPUCE project from its early stages. This has brought the opportunity of validating some of the ideas and contributions of this dissertation within the project context. In particular, the author participated in the definition and description of the actors and roles of a user-centric platform as well as the use cases that drove the platform development [OPUCE-D2.1]. On top of that, he also contributed to the project with the definition of the information model that supports the service and resource specification following the faceted approach [OPUCE-D3.1]. This specification has been thoroughly used in OPUCE.

Finally, the author has led the verification and validation task of the project [OPUCE-D5.3]. The task aimed at verifying that the OPUCE platform met the requirements that were set at the beginning of the project and at validating that a working product was developed. Special attention was given to the user-experience validation, conducted by means of extensive interviews with end-users where they were allowed trying the platform. The results of this validation have provided valuable information to improve the conceptual framework of this dissertation, especially when it comes to the business model proposal and the values that consumers perceive from a user-centric service creation and delivery platform.

8.3 Validation in SEGUR@ project

Segur@ project [SEGUR@] is a research project within the Spanish National Plan for Research and Development addressing some of the topics covered by this dissertation such as ICT, security and trust, privacy, etc. It aims at creating a security and trust framework to support the use of ICT in the e-Society, which includes and identity and privacy management infrastructure.

The author has been involved in the project from the very beginning contributing to the activities included within AP5 mainly T5010 – Identity and privacy management architecture, T5020 – Integration of authentication infrastructure, T5050 – Interoperability between identity management systems. This has provided the background for the contributions regarding privacy and identity infrastructure and an environment to validate them. For example, the mechanisms that support user-centric privacy control in user-centric platforms have been validated within SEGUR@ T5010.

To summarize the validation efforts, next figure graphically shows the relationships between the validation activities carried out (left) and the different scopes of the dissertation involved (right).

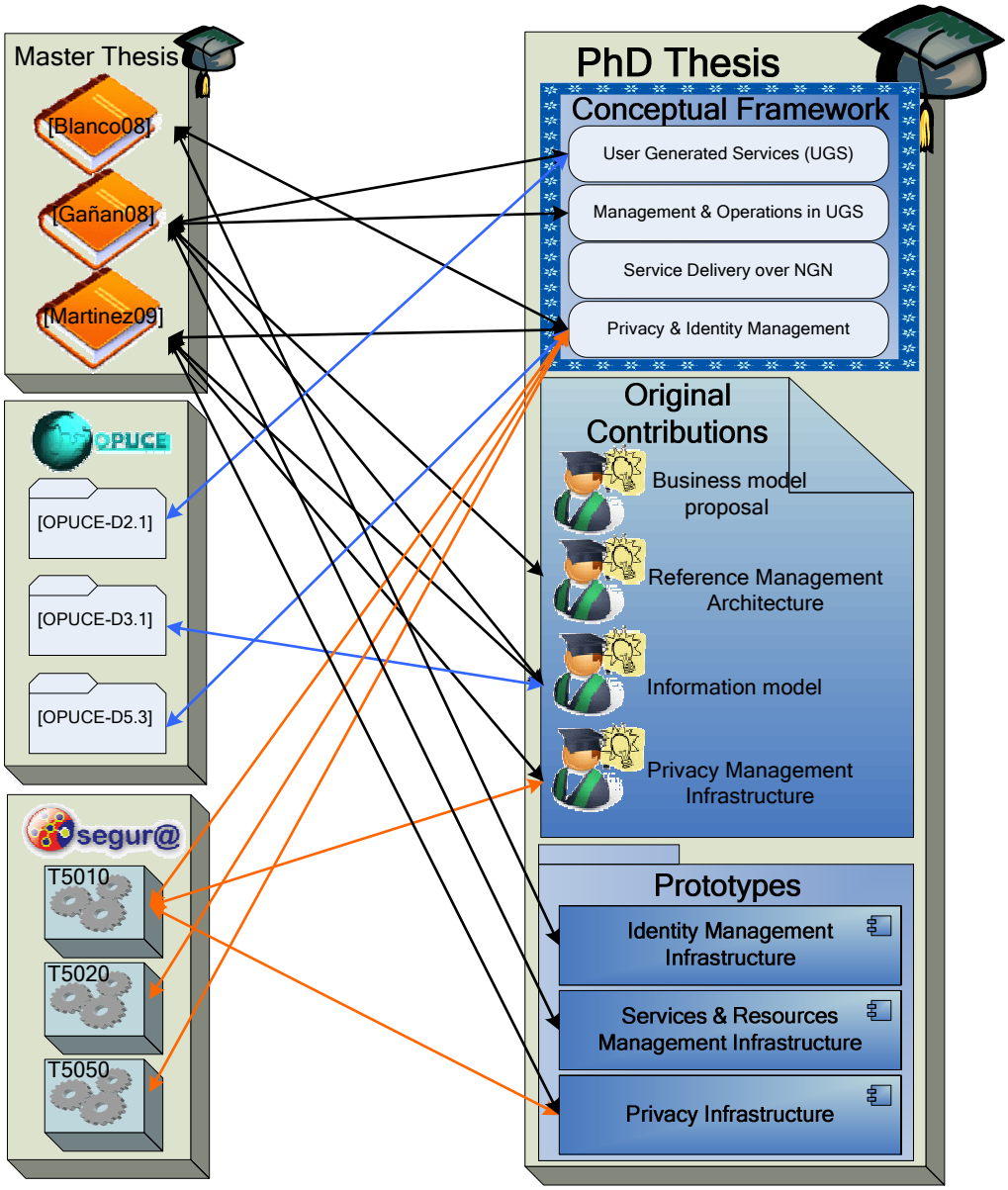

Figure 71 - Dissertation scopes and validation activities.

8.4 Results dissemination

The results of this dissertation have been described and submitted for publication to relevant journals and congresses. Besides, the author has contributed to a book chapter in the context of the dissertation. The following list provides further details:

- *Personalize Service Creation and Provision for the Mobile Web [Sheng&09]*. The author of this dissertation was invited to collaborate on this book chapter with contributions regarding the description of the Telecommunications network convergence process, how to open mobile networks to collaboration and external development, and how to integrate a service platform with the network infrastructure. Additionally, contributions regarding the identity and privacy management infrastructure were provided to the chapter.
- *A User-centric Mobile Service Creation Approach Converging Telco and IT Services [Yu&09]*. This paper has been accepted for publication in the 8th International Conference on Mobile Business (ICMB 2009), to be held in Dalia

(China) in June 2009. The paper describes the fundamentals and major concepts behind the user-generated service paradigm.

- *Personal Information Protection in User-centric Service Platforms [Yelmo&09b]*. This paper was presented in the V Congreso Iberoamericano de Telemática (CITA 2009). The paper analysis the problems that user-centric service creation and execution platforms face regarding privacy protection, and describes the solution that the authors have developed, most of them as a result of this dissertation.
- *Identity Management and Web Services as Service Ecosystem Drivers in Converged Networks [Yelmo&09a]*. This paper was submitted to an open call of the IEEE Communications Magazine, which is an indexed research journal in the Telecommunications domain as for the Information Science Institute Web of Knowledge (ISI WoK). The paper describes the mechanisms that allow a resource provider to join an identity management infrastructure such as the one proposed in this dissertation for a user-centric service creation and delivery platform.
- *Next Generation Mashups: How to create my own services in a convergent world [Trapero&08]*. This paper was accepted in the Telecom I+D Congress 2008. It describes the conceptual framework behind user-centric service creation and delivery.
- *Privacy and data protection in a user-centric business model for Telecommunications services [Yelmo&08b]*. This paper was accepted for publication in IFIP series after the author of this dissertation presented it in the Third International Summer School organized by IFIP WG 9.2, 9.6/11.7, 11.6 in cooperation with FIDIS Network of Excellence and Human IT. The paper described a business model proposal for user-centric service creation and delivery platforms and how identity and privacy management should be managed to fulfil the business model requirements. During the Summer School several comments were received aimed at improving the quality of the contributions, which were incorporated to the dissertation.
- *A user-centric service creation approach for next generation networks [Yelmo&08a]*. This paper was accepted for publication in the ITU-T/IEEE Kaleidoscope Conference held at ITU-T Headquarters in Geneva. The author presented the paper at the conference, where it received very good acceptance due to its contributions to the convergence of Next Generation Networks and Internet worlds. The paper described the approach followed to integrate a user-centric service creation and delivery platform with a Next Generation Network, and the benefits that the business model can provide to the Telecommunications service delivery.
- *A platform for the dynamic creation and automatic deployment of user-centric Telecommunciations services [Yelmo&07b]*. This paper was accepted in the Telecom I+D Congress 2007. It describes an early prototype of user-centric service creation and delivery platform developed within DIT-UPM.
- *User-driven service lifecycle management: Adopting Internet paradigms in telecom services [Yelmo&07a]*. This paper was accepted for publication in the International Conference on Service Oriented Computing in 2007, which is among the most relevant research congresses in the ICT domain as for the

Australian Computing and Research Education (CORE) index. The paper described the information model for the faceted specification and a first approach to the service and resource lifecycles in user-centric platforms.

8.5 Awards

The quality and originality of the author's contributions has been acknowledged in several research and professional fora where they were presented. The most relevant examples are:

- **First prize**, ex-aequo with other proposal, that recognizes it as the best proposal submitted to the 8th Edition of the ***New Applications for Internet Award*** [NAI] promoted by the Telefónica Chair for Next Generation Internet. Citing the Committee, "*The proposal was awarded first prize because it is a Web 2.0 platform that allows users to create new services in a simple manner, integrating and orchestrating existing services in both the Internet and Telecommunications worlds*". The goal of this prize is to promote the development of new services and applications for Internet.
- **First prize** to the **Best Scientific and Technical Paper** submitted to the **Telecom I+D** Spanish Congress held in Valencia in October 2007.
- **Second prize** to the **Best Scientific and Technical Paper** submitted to the **Telecom I+D** Spanish Congress held in Bilbao in October 2008.
- Selected by the Programme Committee Management as one of the nine **finalist candidates** for the three best paper awards of the **Kaleidoscope conference** organized by the **ITU-T and IEEE**. The choice of the 9 candidates started with the selection of 32 papers and 21 posters, which were selected from the 141 original papers submitted to the congress that followed a rigorous double-blind, peer-revision process (about 30% acceptance ratio).

8.6 IPRs

The quality and originality of some of the contributions of this dissertation have been also acknowledged by some of the companies the author has collaborated with. This is the case of Ericsson España, who has filed a PCT patent application [P28702WO1] in the European Patent Office (EPO) including some of the author's contributions regarding user-centric privacy management.

8.7 Contributions to standards

Some of the original contributions of this dissertation have been submitted to standardization bodies in the Telecommunications domain. This is the case of the information model and a service specification example, which were contributed to the Open Mobile Alliance Service Provider Environment (OSPE) Architecture Group to be included within the OSPE Technical Specification [OMA-arc08a] in the framework of the OPUCE project.

Additionally, and out of the OPUCE framework, the description of the service lifecycle and the resource lifecycle management processes were also contributed [OMA-arc08b] to the OMA OSPE Architecture Group to be included within the OSPE specifications.

8.8 Chapter summary and conclusions

This chapter has described all the initiatives that the author has carried out in order to validate the original contributions he has proposed as part of this dissertation. Among them, three Master Thesis have developed prototypes that have validated some of the contributions. Besides, some contributions have been validated within national and international research projects, such as the OPUCE and SEGUR@ projects.

In addition, the results of this dissertation have been accepted for publication in seven national and international journals and conferences, some of which are indexed as relevant research and scientific dissemination channels. On top of that, three of these publications have been awarded with prizes, thus acknowledging their quality and originality.

And as for industrial exploitation, two contributions have been done to the Open Mobile Alliance standardization committee. Furthermore, one PCT patent application describing a prototype implementing one of the contributions of this dissertation has been filed in the European Patent Office in collaboration with Ericsson España.

9 CONCLUSIONS

Supported by Next Generation Network realizations and by Service Oriented Architectures the new IP-based ICT world is blurring the border between the traditionally separated Internet and Telecommunications domains. To keep the pace with new entrants, telecom operators are introducing fresh paradigms that engage new actors in the previously-closed service creation and delivery industry. By involving users in the service conception process telcos aim to have customers environments revealed and come up with new unique ideas that fulfil users' latent needs and user-experience expectations. Additionally, this new paradigms may contribute to safe development and marketing expenses, thus helping to increase the value per bit carried.

Although the benefits that user-centric service creation and delivery platforms bring to the Telecommunications domain are enormous, there are many challenges that operators must solve first. To begin with, the business models that can be applied are not clear. Additionally, the fact that users are allowed to create their own services and drive their lifecycles pose great challenges to current operations and support systems. On top of that, user-centric services are expected to intensively make use of end-users personal information, which may arise many concerns regarding privacy and personal information protection.

This dissertation has aimed to cover the detected gaps by proposing a set of original contributions that may help to solve the detected problems. Next section provides a brief enumeration of the objectives that were set at the beginning of the research period. Then, the original contributions elaborated, which have been proposed to fulfil the objectives, are detailed. Finally, since this is a new and broad field of research, many interesting topics have not been addressed yet. The chapter concludes proposing a set of areas for further investigation.

9.1 Original objectives

The objectives stated at the beginning of this dissertation were:

1. To assess existing business models for service provision in the Telecommunications domain and their feasibility for user-centric service delivery platforms over next generation networks. Should not the previous business models be feasible, new business models will be proposed and described.
2. To analyze the challenges and potential problems that new user-centric service delivery platforms and their business models pose regarding operations support systems and service management over next generation networks. Should some entities and functions be affected, then new solutions or improvements will be proposed and described.
3. To analyze the risks that user-centric platforms pose for end-users privacy and anonymity, and the protection of their digital identities. Innovative proposals will be done that contribute to solve the detected problems.
4. To design an architecture and a set of tools that incorporate the results from the previous analysis and that contribute to solve the problems detected in the management and operation of user-centric services over next generation networks.
5. To validate the results of this thesis with a working prototype.

6. To contribute the results of this dissertation to national and international research projects as well as open source communities aligned with the context and objectives of this work.
7. To disseminate the results of this thesis in relevant national and international conferences and workshops, as well as in international journals and magazines.

9.2 Original contributions

As a result of the research activities carried out, the author has elaborated the following original contributions:

- **A business model for user-centric service creation and delivery platforms**. Since the analysed business model did not fulfil the requirements for these platforms the author has proposed an innovative business model.
- **A high-level reference architecture for user-centric service creation and delivery platforms over next generation networks**. The reference architecture has taken into account the peculiarities of user-centric platforms over traditional telecom-oriented service delivery platforms.
- **A reference end-to-end architecture for the management and operation of user-centric service creation and delivery platforms**. The architecture has been described following a top-down approach, beginning with a high-level overview and providing deeper details on each component. A prototype has been developed to demonstrate the feasibility and correctness of the proposal.
- **An information model for service and resource description in user-centric service creation and delivery platforms**. The information model is available as XML Schema, and has been successfully validated in two Master Thesis and further used in a European research project. Moreover, the information model has been contributed to the Open Mobile Alliance Architecture Group for its inclusion within the OMA Service Provider Environment specification.
- **A privacy management infrastructure for user-centric service creation and delivery platforms**. Firstly, the risks that user-centric platforms pose for end-users privacy and anonymity and the protection of their digital identities have been assessed. Additionally, a Master Thesis has validated the contributions by implementing a working prototype. On top of that, this infrastructure has been partially filed as a new PCT patent application.

The research work described in this document has been carried out within the context of the IST European Integrated Project OPUCE (*Open Platform for User-centric service Creation and Execution*), 6th Framework Programme (Contract No. 34101), and the SEGUR@ project, within the CENIT program, with reference CENIT-2007/2004.

It is also worth mentioning that partial results of this dissertation have been disseminated in more than ten publications submitted to relevant national and international conferences and workshops, as well as in international journals and magazines, where they have been awarded several times. On top of that, a PCT patent application describing an apparatus to help users to control their privacy has been filed.

These original contributions and results aim to advance the situation of European citizens and economy. First, fostering openness by means of contributing the results to standardization bodies. Then, promoting the well-being of European citizens by means of the social applications that can be developed using user-centric platforms. Finally,

the privacy contributions described in the dissertation help to protect the autonomy of individuals and retain control over their personal information, which is a must for the development of the Future Internet as for the European Research Agendas and Priorities.

9.3 Future research

Management of emerging ICT service platforms is a hot area with many interesting subjects to research. Major standardization bodies such as the TeleManagement Forum or the Open Mobile Alliance are currently addressing some topics. In particular, secured and reliable collaboration among different administrative domains in modern service marketplaces requires further investigation and provides interesting research opportunities.

There is also room for improvement on the mashups portability among different user-centric platforms. During the First ITU-T Kaleidoscope Conference held in the ITU headquarters in Geneva, where the author give a presentation on user-centric platforms and their relationships with next generation networks, one of the agreed drawbacks in current platforms was the lack of *de-facto* or *de-jure* standards that may help to export user-generated services from one platform to another. Standards will help to reduce entrance barrier for new actors and thus will promote competition.

It is worth mentioning that one of the major drawbacks of current ICT platforms, including user-centric ones, comes from the scalability and performance issues that service orchestration in Telecommunications face. SOA was not initially thought for real-time systems and thus it poses some constraints when high throughput and low latency is required. This fact has been experienced during the validation activities for the OPUCE platform, which the author has coordinated. Alternatives are scarce and immature, and work on this area brings motivating research opportunities.

Usability and user-experience improvements are also research areas for user-centric platforms. Since these platforms target non-technically skilled end-users they must follow a user-centred design. Usability is especially important when it comes to privacy control. This dissertation has proposed some original ideas that may help to improve the current situation. Nevertheless, the concepts have not been validated with real end-users and thus a validation activity is desirable to verify the basic assumptions.

Finally, privacy is increasingly becoming a hot topic and an objective for different Strategic Research Agendas. This dissertation has provided some contributions that advance the state of the art of this domain. However, it has not considered the social dimension that current Web platforms include. Therefore, future research points towards privacy in the context of social networks.

Bibliography

[3GPP]	Third Generation Partnership Project Website, http://www.3gpp.org/ (Feb 2009)
[3GPP2]	Third Generation Partnership Project 2 Website, http://www.3gpp2.org/ (Feb 2009)
[3GPP-ims]	3GPP TS 23.228, *IP Multimedia Subsystem (IMS)*, version 8.0.0, Mar 2007.
[ACF]	Autonomic Communications Forum Website, http://www.autonomic-communication-forum.org/ (Jul. 2008)
[Afuah&01]	Afuah, A. and Tucci, C., *Internet Business Models and Strategies*, Mc Graw Hill, 2001.
[Ahn&07]	Ahn, G. and Ko, M., *User-centric Privacy Management for Federated Identity Management*, Proceedings of International Conference on Collaborative Computing (CollaborateCom), Nov 2007, pp 187-195.
[Aleman&07]	Alemán, S., Chamorro, J., Torres, E.J. and de la Iglesia, F., *Business Mashup Framework*, 7th Edition of the New Applications for Internet Award, http://internetng.dit.upm.es/wp-content/uploads/File/6_business_mashups_framework.pdf (Feb 2009)
[AMAZON]	Amazon Website, http://www.amazon.com (Feb 2009)
[Anderson06]	Anderson, C., *The Long Tail: Why the Future of Business is Selling Less of More,* Hyperion, 2006.
[AOLDN]	AOL Developer Network Website, http://dev.aol.com/ (Jan 2009)
[APPEL]	Langheinrich, M. (Ed), *A P3P Preference Exchange Language 1.0 (APPEL1.0),* W3C Working Draft 15 Apr 2002, http://www.w3.org/TR/P3P-preferences
[ATIS]	Alliance for Telecommunication Industry Solutions Website, http://www.atis.org/ (Feb 2009)
[Baker&01]	Baker, G. and Megler, V., *The Semi-Walled Garden: Japan's i-mode Phenomenon*, IBM pSeries Solutions Development, Oct 2001.
[Basole&08]	Basole, R.C. and Rouse, W.B., *Complexity of service value networks: Conceptualization and empirical investigation*, IBM System Journal, vol 47, no 1, pp 53-70, Jan 2008.
[BETAVINE]	Vodafone Betavine Website, http://www.betavine.net/ (Jan 2009)
[Blanco08]	Blanco, A., Implementación en código fuente abierto de una plataforma para la gestión de identidades según el estándar Liberty ID-WSF 2.0, Master Thesis, ETSI Telecomunicación – Universidad Politécnica de Madrid, May 2008.
[Boom&04]	Boom, S. and Ferry, D., *JAIN SLEE 1.0 Specification, Final Release*, Sun Microsystems Inc. and Open Cloud Limited, Mar 2004.
[Bray&06]	Bray, C., Spink, P., Nicholas, M. and Zai, H., *Transforming Operational Support Systems: The Reasons for OSS Transformation and the Approach for Successful Implementations*, IBM Corporation, 2006.
[Caetano&07]	Caetano, J. *et al*, *Introducing the user to the service creation world: concepts for user centric creation, personalization and notification,* Proceedings of the International Workshop on User centricity – state of the art, Budapest (Hungary), 2007.
[Calhoun&03]	Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and Arkko, J., *Diameter Base Protocol*, IETF RFC 3588, Sep 2003.
[Camarillo&06]	Camarillo, G. and García-Martín, M.A., *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*, Second Edition, John Wiley & Sons Ltd., 2006.
[Camp04]	Camp, J.L., *Digital Identity*, IEEE Technology and Society Magazine, vol 23, issue 3, pp 34-41, Fall 2004.
[Chappell02]	Chappell, D. and Jewell, T., *Java Web Services*, O'Really & Associates Inc., 2002.
[Chappell06]	Chappell, D., *Introducing Windows CardSpace,* Apr 2006, available online at http://msdn2.microsoft.com/en-us/library/aa480189.aspx
[Chesbrough05]	Chesbrough, W.H., *Open Innnovation: The New Imperative for Creating and Profiting from Technology*, Harvard Business School Press, 2005.
[CONCORDIA]	Concordia Project Website, http://projectconcordia.org/ (Feb 2009)
[Cuevas&06]	Cuevas, A. *et al*, *The IMS Service Platform – A Solution for Next-Generation Networks Operators to Be More than Bit Pipes,* IEEE Communications

	Magazine, vol 44, no 8, pp 75-81, Aug 2006.
[Dickerson04]	Dickerson, K.R., *Standards as an Enabler for Next Generation Networks*, BT Technology Journal, vol 22, no 2, pp 39-47, Apr 2004.
[DMTF-CIM]	Distributed Management Task Force, *CIM Compliance Specification,* version 1.1, Dec 2003.
[DMTF-WSM]	Distributed Management Task Force, *Web Services for Management (WS-Management) Specification*, version 1.0.0, Dec 2008.
[Erl05]	Erl, T., *Service-Oriented Architecture (SOA): Concepts, Technology, and Design*, Prentice Hall PTR, 2005.
[ETSI]	European Telecommunications Standards Institute Website, http://www.etsi.org/ (Feb 2009)
[ETSI-OSA]	ETSI Standard ES 203 915-1, *Open Service Access (OSA); Application Programming Interface (API); Part 1: Overview (Parlay 5)*, version 1.2.1, Jan 2007.
[ETSI-ParlayX]	ETSI Standard ES 202 391-1, *Open Service Access (OSA); Parlay X Web Services; Part 1: Common (Parlay X 2)*, version 1.2.1, Dec 2006.
[EU1995-46]	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, pp. 31-50, Oct 1995
[EU2002-58]	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L 201, pp 37-47, Jul 2002.
[EU2006-24]	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending Directive 2002/58/EC, Official Journal L 105, pp. 54-63, Mar 2006.
[Evans&06]	Evans, D.S., Hagiu, A. and Schmalensee, R., *Invisible Engines: How Software Plaforms Drive Innovation and Transform Industries*, The MIT Press, 2006.
[FIA]	European Future Internet Portal, http://www.future-internet.eu/ (May 2009)
[FIDIS]	Future of Identity in the Information Society Website, http://www.fidis.net/ (Feb 2009)
[Fielding&99]	Fielding, R. *et al*, *Hypertext Transfer Protocol: HTTP/1.1*, IETF RFC 2616, Jun 1999.
[FORRESTER]	Forrester Social Technology Profile Tool Website, http://www.forrester.com/Groundswell/profile_tool.html (Jan 2009)
[FP7]	Seventh Framework Programme Website, http://cordis.europa.eu/fp7/ (May 2009)
[Gañan08]	Gañán, A., *Creación de un entorno para la composición y el despliegue de servicios en una plataforma abierta y centrada en el usuario*, Master Thesis, ETSI Telecomunicación – Universidad Politécnica de Madrid, Jun 2008.
[Garraham&93]	Garraham, J.J. *et al*, *Intelligent Network Overview*, IEEE Communications Magazine, vol 31, no 3, pp 30-36, Mar 1993.
[GOOGLE]	Google Mashup Editor Website, http://editor.googlemashup.com/ (Jan 2009)
[Greene&08]	Greene, W. and Hayes, T., *Service Delivery Frameworks: The Service Provider's Mashup*, Pipeline Publishing LLC, vol. 4, issue 8, Jan 2008.
[Griffin&07]	Griffin, D. and Pesch, D., *A Survey on Web Services in Telecommunications*, IEEE Communications Magazine, vol 45, no 7, pp 28-35, Jul 2007.
[GSMA]	GSM Association Website, http://www.gsmworld.com/ (Jan 2009)
[GSMA-Access]	GSMA 3rd Party Access Website, https://gsma.securespsite.com/access/entry (Jan 2009)
[Hippel06]	von Hippel, E., *Democratizing Innovation*, The MIT Press, 2006. Available for download under Creative Common License at http://web.mit.edu/evhippel/www/books.htm
[Hippel94]	von Hippel, E., *The Sources of Innovation*, Oxford University Press, 1994. Available for download under Creative Common License at http://web.mit.edu/evhippel/www/books.htm
[Hirsch&06]	Hirsch, F. *et al*, *Mobile Web Services: Architecture and Implementation*, John Wiley & Sons Inc., 2006.

[Hommel06]	Hommel, W., *Policy-based Integration of User and Provider-Sided Identity Management*, Proceedings of the International Conference on Emerging Trends in Information and Communication Security (ETRICS 2006), LNCS vol 3995, pp 160-174, Springer, 2006
[HP-ngoss08]	Hewlett-Packard White Paper, *Rethinking Operations Support Systems in the New Telecom Era: A Builder's Guide*, May 2008.
[HP-sdp07]	Hewlett-Packard White Paper, *HP Service Delivery Platform*, Oct 2007.
[Hunt06]	Hunt, P. (Ed), *Client Attribute Requirements Markup Language (CARML) Specification*, Working draft 03, Nov 2006.
[ICT08]	European Commission, *The Future of the Internet*, Conference Session Report on The Future of the Internet, ICT Event 2008 (Lyon, France), Nov 2008.
[IEEE-NGSON]	IEEE Next Generation Service Overlay Network Working Group Website, http://grouper.ieee.org/groups/ngson/ (Jul. 2008)
[IETF]	IETF Website, http://www.ietf.org/ (Feb 2008)
[IPSF]	IPsphere Forum Website, http://www.ipsphereforum.org/ (Feb 2009)
[IPSF-TS]	IPSphere Forum, *IPSphere Framework Technical Specification (Release 1)*, Jun. 2007.
[ITIL]	ITIL Website, http://www.itil-officialsite.com/ (Feb 2008)
[ITU-T]	The Telecommunication Standardization Sector of International Telecommunication Union Website, http://www.itu.int/ITU-T (Feb 2008)
[ITUT-FGIdM]	ITU-T Focus Group on Identity Management Website, http://www.itu.int/ITU-T/studygroups/com17/fgidm/ (Feb 2009)
[ITUT-ngn05]	ITU-T, *NGN Focus Group Proceedings*, Nov 2005.
[JAJAH]	Jajah Website, http://www.jajah.com (Feb 2009)
[Jaokar&06]	Jaokar, A. and Fish, T., *Mobile Web 2.0*, Futuretext, 2006.
[Jensen&08]	Jensen, C., Ruiz, C. and Wind, R., *User-Generated Content: The Case for Mobile Services*, IEEE Computer, vol 41, no 12, pp 116-118, Dec 2008.
[Jorstad&05]	Jørstad, I., Dustdar, S. and van Do, T., *An Analysis of Current Mobile Services and Enabling Technologies*, International Journal of Ad Hoc and Ubiquitous Computing, vol 1, nos 1/2, pp 92-102, 2005.
[Knightson&05]	Knightson, K., Morita, N. and Towle, T., *NGN Architecture: Generic Principles, Functional Architecture, and Implementation*, IEEE Communications Magazine, vol 43, no 10, pp 49-56, Oct 2005.
[Koivukoski&05]	Koivukoski, U. and Räisänen, V. (Ed.), *Managing mobile services: Technologies and business practices*, John Wiley & Sons Inc., 2005.
[Lee&05]	Lee, C.S. and Knight, D., *Realization of the Next Generation Network*, IEEE Communications Magazine, vol. 43, no. 10, pp. 34-41, Oct 2005.
[LIBERTY]	Liberty Alliance Website, www.projectliberty.org/ (Feb 2009)
[LibertyAccount]	Le Van Gong, H. (Ed), *Liberty ID-WSF Accounting Service*, Version 1.0 Revision 5, Liberty Alliance Project, Oct 2007, http://www.projectliberty.org/specs
[LibertyDisco]	Hodges, J. and Cahill, C. (Eds.), *Liberty ID-WSF Discovery Service Specification*, Version 2.0, Liberty Alliance Project, Jul. 2006, http://www.projectliberty.org/specs
[LibertyDST]	Kellomäki, S. and Kainulainen, J, (Eds.), *Liberty ID-WSF Data Services Template*, Version 2.1, Liberty Alliance Project, Jul 2006, http://www.projectliberty.org/specs
[LibertyIGF]	Madsen, P. (Ed.), *Liberty IGF Privacy Constraints Specification,* Draft version 1.0-04, Liberty Alliance Project, Jan 2008, http://www.projectliberty.org/specs
[LibertyIS]	Aarts, R. and Madsen, P. (Ed), *Liberty Id-WSF Interaction Service Specification*, Version 2.0-errata-v1.0, 2007, http://www.projectliberty.org/specs
[LibertyPrivacy]	Robert, A. et al, *Liberty Architecture Framework for Supporting Privacy Preference Expression Languages (PPELs)*, Version 1.0, Liberty Alliance Project, Nov 2003, http://www.projectliberty.org/specs
[LibertySubs]	Kellomäki, S. (Ed.), *Liberty ID-WSF Subscriptions and Notifications,* Version 1.0, Liberty Alliance Project, http://www.projectliberty.org/specs
[Lockhart&06]	Lockhart, H. *et al*, *Web Services Federation Language (WS-Federation)*, Version 1.1, Dec 2006, available online at www.ibm.com/developerworks/webservices/library/ws-fed/
[M.3010]	ITU-T Recommendation M.3010, *Principles for a Telecommunications*

	Management Network, Feb 2000.
[M.3050.0]	ITU-T Recommendation M.3050, *Enhanced Telecom Operations Map (eTOM) – Introduction*, Mar 2007.
[M.3050.1]	ITU-T Recommendation M.3050.1, *Enhanced Telecom Operations Map (eTOM) – The business process framework*, Mar 2007.
[M.3050.s1]	ITU-T Recommendation M.3050 Supplement 1, *Enhanced Telecom Operations Map (eTOM). Supplement 1 – Interim view of an interpreter's guide for the eTOM and ITIL practicioners,* Feb 2007.
[M.3200]	ITU-T Recommendation M.3200, *TMN management services and telecommunications managed areas: overview*, Apr 1997.
[M.3400]	ITU-T Recommendation M.3400, *TMN management functions*, Feb 2000.
[MacKenzie&06]	MacKenzie, C.M. *et al* (Ed.)*, Reference model for Service Oriented Architecture*, OASIS Committee Specification 1, Aug 2006.
[Madsen&06]	Madsen, P., Cassasa, M. and Wilton, R., *A Privacy Policy Framework – A position paper for the W3C Workshop of Privacy Policy Negotiation*, Oct 2006, http://www.w3.org/2006/07/privacy-ws/papers/28-madsen-framework/
[MAEMO]	Maemo Website, http://maemo.org (Jan 2009)
[Martinez09]	Martínez, C., *Desarrollo de un prototipo de aplicación para protección de información personal en plataformas de servicios convergentes centrados en el usuario*, Master Thesis, ETSI Telecomunicación – Universidad Politécnica de Madrid, Feb 2009.
[Mendyk07]	Mendyk, D. (Ed.), *Telco Web 2.0 Mashups: A New Blueprint for Service Creation*, Light Reading's Services Software Insider, Vol. 3, No. 2, May 2007.
[Mishra06]	Mishra, P., *AAPML: Attribute Authority Policy Markup Language*, Working draft 08, Nov 2006.
[MORIANA]	The Moriana Group, *SDP 2.0: Service Delivery Platforms in the Web 2.0 Era,* Sep 2008, available online at http://www.morianagroup.com/
[MOSH]	Mosh Website, http://mosh.nokia.com (Jan 2009)
[MS-CSF]	Microsoft Corporation Whitepaper, *Microsoft Connected Services Framework – Enabling Service Delivery Using the Microsoft Connected Services Framework*, Jan 2005.
[MS-CSS]	Microsoft Connected Services Sandbox Website, http://www.networkmashups.com/ (Jul 2008)
[MS-IDM]	Microsoft Corporation Whitepaper, *Microsoft's Vision for an Identity Metasystem*, May 2005.
[NAI]	New Applications for Internet 2008 Award Homepage, http://internetng.dit.upm.es/eventos?em_action=register_form&event_id=18 (Feb 2009)
[Nakhjiri&05]	Nakhjiri, M. and Nakhjiri, M., *AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility*, John Wiley & Sons Ltd., 2005.
[NESSI]	NESSI http://www.nessi-europe.com (Feb 2009)
[OASIS]	OASIS Website, http://www.oasis-open.org (Feb 2009)
[OASIS-BPEL]	Alves, A. *et al* (Ed.), *Web Services Business Process Execution Language Version 2.0*, OASIS WSBPEL TC, Jan 2007, available online at http://docs.oasis-open.org/wsbpel/2.0/
[OASIS-SAML]	Cantor, S. *et al* (Ed.), *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS SS TC, Mar 2006, available online at http://docs.oasis-open.org/security/saml/v2.0/
[OASIS-SPML]	Cole, G. (Ed.), *OASIS Service Provisioning Markup Language (SPML) Version 2*, OASIS SP TC, Apr 2006, available online at http://docs.oasis-open.org/provision/spml/v2.0/
[OASIS-Telecom]	OASIS Telecommunications Services Member Section Website, http://www.oasis-telecom.org/ (Feb 2009)
[OASIS-WSDM]	Wilson, K. and Sedukhin, I. (Ed.), *Web Services Distributed Management: Management of Web Services (WSDM-MOWS) 1.1*, OASIS Web Services Distributed Management TC, Aug 2006, available online at http://docs.oasis-open.org/wsdm/
[OASIS-WSS]	Nadalin, A. *et al* (Ed.), *Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)*, OASIS WSS TC, Feb 2006, available online at http://docs.oasis-

	open.org/wss/v1.1/
[OASIS-WSTrust]	Nadalin, A. *et al* (Ed.), *WS-Trust 1.3*, OASIS WS-SX TC, Mar 2007, available online at http://docs.oasis-open.org/ws-sx/ws-trust/
[OECD-ugc07]	Organisation for Economic Co-operation and Development, Participative Web: User-Created Content, OECD DSTI/ICCP/IE(2006)7/FINAL, Apr 2007.
[OMA]	Open Mobile Alliance Website, http://www.openmobilealliance.org/ (Feb 2009)
[OMA-arc08a]	OMA Architecture Input Contribution: Conceptual Model for Service Specification in OSPE, OMA-ARC-OSPE-2008-0007-INP_Conceptual_Model_For_Service_Specification_In_OSPE, Aug 2008.
[OMA-arc08b]	OMA Architecture Input Contribution: Service and Component Life Cycle Management Process, OMA-ARC-OSPE-2008-0014-SLM-process, Oct 2008.
[OMA-OSE]	OMA Service Environment (OSE): Architecture Description, Open Mobile Alliance, OMA-AD-Service-Environment-V1_0_4-20070201-A, Version 1.0.4, Feb 2007
[OMA-OSPE]	OMA Service Provider Environment (OSPE): OMA Service Provider Environment Requirements, OMA-RD-OSPE-V1_0-20050614-C, Candidate Version 1.0, Open Mobile Alliance, Jun 2005.
[OMA-OWSER]	OMA Web Services Enabler (OWSER): Overview, Open Mobile Alliance, OMA-OWSER-Overview-V1_0-20040715-A, Version 1.0, Jul 2004.
[OPENID]	OpenID Website, http://openid.net/ (Feb 2009)
[OPENMF]	Open Movil Forum Website, http://open.movilforum.com/ (Jan 2009)
[OPUCE]	OPUCE Website, http://www.opuce.eu (Feb 2009)
[OPUCE-D2.1]	OPUCE Deliverable 2.1, *Use cases, definitions and requirements*, May 2008.
[OPUCE-D3.1]	OPUCE Deliverable 3.1, *Service, Service Lifecycle and Service Components Specification*, Feb 2009.
[OPUCE-D5.3]	OPUCE Deliverable 5.3, *System Validation (Lab Trials Results)*, Feb 2009.
[O'Reilly05]	O'Reilly, T., *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software,* Sep 2005, available online at http://www.oreilly.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html
[OSA]	Open Services Architecture/Parlay Website, http://www.parlay.org/ (Feb 2009)
[P28702WO1]	Del Álamo, J.M., San Miguel, B., Yelmo, J.C., Monjas, M.A., *Privacy Controller*, PCT Application, PCT/EP2009/054223, 8th April 2009.
[P3P]	Marchiori, M. (Ed), *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C Recommendation 16 Apr 2002
[PARLAY]	The Parlay Group Website, http://www.parlay.org/ (Feb 2009)
[PARTNER]	Orange Partner Website, http://www.orangepartner.com/ (Jan 2009)
[Peltz03]	Peltz, A., *Web Services Orchestration and Choreography,* Computer, vol 36, pp 46-52, Oct 2003
[Ping07]	Ping Identity Corporation White Paper, *Internet-Scale Identity Systems: An Overview and Comparison*, Feb 2007.
[PLANI+D]	Plan Nacional I+D+i Website, www.plannacionalidi.es/ (Feb 2009)
[Pollet&06]	Pollet, T., Maas, G., Marien, J. and Wambecq, A., *Telecom Services Delivery in a SOA*, Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), vol 2, pp 21-26., Vienna (Austria), 2006
[POPFLY]	Microsoft Popfly Website, http://www.popfly.ms/ (Feb 2009)
[PRIME]	Privacy and Identity Management for Europe Website, https://www.prime-project.eu/ (Feb 2009)
[QUEDWIKI]	IBM QUEWiki Website, http://services.alphaworks.ibm.com/qedwiki (Feb 2009)
[Rademakers&08]	Rademakers, T. and Dirksen, J, *Open Source ESBs in Action*, Manning Publications, 2008.
[Radhakrishnan07]	Radhakrishnan, R., *Identity & Security – A common Architecture & Framework for SOA and Network Convergence*, Futuretext, 2007.
[Reilly&05]	Reilly, J. and Creaner, M., *NGOSS Distilled: The Essential Guide to Next Generation Telecoms Management,* The Lean Corporation, 2005.
[RIBBIT]	Ribbit Website, http://www.ribbit.com/ (Jan 2009)
[Rigney&00]	Rigney, C., Willens, S., Rubens, A. and Simpson, W., *Remote Authentication Dial In User Service (RADIUS)*, IETF RFC 2865, Jun 2000.
[Rosemberg&02]	Rosemberg, J. *et al*, *SIP: Session Initiation Protocol*, IETF RFC 3261, Jun 2002.

[Rosenberg&04]	Rosenberg, J. and Remy, D., *Securing Web Services with WS-Security*, Sams Publishing, 2004.
[Roussos&03]	Roussos, G., Peterson, D. and Patel, U., *Mobile Identity Management: An Enacted View*, International Journal of Electronic Commerce, vol 8, no 1, pp 81-100, Fall 2003.
[Saeidian&08]	Saeidian, H. and Mulkey, S., *Performance Evaluation of Eventing Web Services in Real-Time Applications*, IEEE Communications Magazine, vol 46, no 3, pp. 106- 111, Mar 2008.
[Sawyer&05]	Sawyer, P., Hutchison, J., Walkerdine, J. and Sommerville, I., *Faceted Service Specification,* Proceedings of the Workshop on Service-Oriented Computing Requirements (SOCCER), Paris, Aug 2005.
[SDPA]	The SDP Alliance Website, http://www.thesdpalliance.com/ (Jul. 2008)
[SECSE]	Service Centric System Engineering (SeCSE) Website, http://www.secse-project.eu/ (Feb 2009)
[SEGUR@]	Segur@ Website, http://www.cenitsegura.com/ (Feb 2009)
[Sheng&09]	Sheng, Q.Z., Yu, J, Del Álamo, J.M. and Falcarin, P., *Personalized Service Creation and Provision for the Mobile Web*, In Weaving Services, Location, and People on the WWW, I. King and R. Baeza-Yates(Eds), Springer, June 2009 (In press)
[SKYPE]	Skype Website, http://www.skype.com/ (Feb 2009)
[TELCO2.0]	STL Partners Ltd., *Telco 2.0 Manifesto: How to make money in an IP-based world*, May 2007; available online at http://www.telco2.net/manifesto/
[TINAC]	TINA Consortium Website, www.tina-c.com/ (Feb 2009)
[TISPAN]	Telecommunication and Internet converged Services and Protocols for Advanced Networking Website, http://www.etsi.org/tispan/ (Feb 2009)
[TISPAN-oss05]	ETSI TR 188 004, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; OSS vision*, May 2005.
[TISPAN-oss06a]	ETSI TR 188 003, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); OSS Requirements; OSS definition of requirements and priorities for further network management specifications for NGN*, Mar 2006.
[TISPAN-oss06b]	ETSI TR 188 001, *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; Operations Support Systems Architecture*, Mar 2006.
[TMF]	TeleManagement Forum Website, http://tmforum.org/ (Feb 2009)
[TMF-CIM]	TeleManagement Forum, *CIM – SID Solution Suite*, Release 1.0, Jun 2005.
[TMF-GB921]	TeleManagement Forum, *GB921 – Enhanced Telecom Operations Map (eTOM) – The Business Process Framework for the Information and Communications Services Industry*, version 6.1, Nov 2005.
[TMF-GB922]	TeleManagement Forum, *GB922 – Shared Information/Data (SID) Business View: Concepts & Principles*, version 6.1, Nov 2005.
[TMF-GB922-4SO]	TeleManagement Forum, *GB922-4SO – Information Framework (SID): Service Overview Business Entity Definitions Release 8.0*, version 7.9, Jul 2008.
[TMF-GB924]	TeleManagement Forum, *GB924 – Service Framework Guidebook,* version 1.0, Sep 2003.
[TMF-GB930]	TeleManagement Forum, *GB930 – The NGOSS Approach to Business Solutions*, version 0.6, Nov 2005.
[TMF-Prosspero]	TeleManagement Forum Prosspero Initiative Website, http://www.tmforum.org/prosspero (Feb 2009)
[TMF-TR139a]	TeleManagement Forum, *TR139 – Service Delivery Framework Overview*, version 1.0, Jan 2008.
[TMF-TR139b]	TeleManagement Forum, *TR139 – Service Delivery Framework Overview*, working draft version 2.0, May 2008.
[Trapero&08]	Trapero, R., Suárez, D., Del Álamo, J.M., León, A., Martín, Y.S., Ordás, I., Martínez, A., Yelmo, J.C., *Next Generation Mashups: Cómo crear mis propios servicios en un mundo convergente*, Proceedings of the XVIII Jornadas Telecom I+D, Bilbao (Spain), Oct 2008. Available online at http://www.telecom-id.com/Actas/ProceedingsTelecomI+D-2008.htm

[Trapero09]	Trapero, R., *Contribución a las Arquitecturas para la Provisión de Servicios Basados en Identidad Sobre Redes de Siguiente Generación*, PhD Thesis, Universidad Politécnica de Madrid (Work in progress).
[W3C]	World Wide Web Consortium Website, http://w3.org/ (Feb 2009)
[W3C-P3P]	Platform for Privacy Preferences Project Website, http://www.w3.org/P3P/ (Feb 2009)
[W3C-SOAP]	Gudgin, M. *et al* (Ed.), *SOAP Version 1.2 Part 1: Messaging Framework*, W3C Recommendation 24 June 2003, Jun 2003; available online at http://www.w3.org/TR/soap12-part1/
[W3C-WS]	Booth, D. *et al* (Ed.), *Web Services Architecture*, W3C Working Group Note 11 February 2004, Feb 2004; available online at http://www.w3.org/TR/ws-arch/
[W3C-WSDL]	Chinnici, R. *et al.* (Ed.), *Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language*, W3C Recommendation 26 Jun 2007, Jun 2007, available online at http://www.w3.org/TR/wsdl20
[W3C-WSPolicy]	Vedamuthu, A. *et al* (Ed.), *Web Services Policy 1.5 – Framework*, W3C Recommendation 4 Sep 2007, Sep 2007, available online at http://www.w3.org/TR/ws-policy
[W3C-XML]	Bray, T. *et al* (Ed.), *Extensible Markup Language (XML) 1.0 (Second Edition)*, W3C Recommendation 6 October 2000, Oct 2000, available online at http://www.w3.org/TR/REC-xml
[WEB21C]	Web21C SDK Developer Center Website, http://sdk.bt.com (Discontinued)
[Windley05]	Windley, P., *Digital Identity*, O'Reilly Media Inc., 2005.
[XACML]	Moses, T. (Ed), *Extensible Access Control Markup Language (XACML) Version 2.0,* OASIS Standard, Feb 2005
[XPDL]	The Workflow Management Coalition, *WFMC-TC-1025: Process Definition Interface – XML Process Definition Language*, version 2.00, Oct 2005, available online at http://www.wfmc.org/standards/XPDL.htm
[Y.2001]	ITU-T Recommendation Y.2001, *General Overview of NGN*, Dec 2004.
[Y.2011]	ITU-T Recommendation Y.2011, *General Principles and General Reference Model for Next Generation Network*, Jun 2004.
[YAHOO!]	Yahoo! Pipes Website, http://pipes.yahoo.com (Feb 2009)
[Yates&97]	Yates, M. *et al*, *TINA Business Model and Reference Points*, TINA-C Deliverable, Version 4.0, May 1997.
[Yavatkar&00]	Yavatkar, R. et al., *A framework for policy-based admission control*, IETF RFC 2753, Jan 2000, http://www.ietf.org/rfc/rfc2753.txt
[Yelmo&07a]	Yelmo, J.C., Trapero, R., Del Álamo, J.M., Sienel, J., Drewniok, M., Ordás, I., McCallum, K., *User-driven service lifecycle management: Adopting Internet paradigms in telecom services*, Proceedings of the International Conference on Service Oriented Computing (ICSOC 2007), LNCS vol. 4749, pp. 342-352, Springer, 2007
[Yelmo&07b]	Yelmo, J.C., Trapero, R., Del Álamo, J.M., *Una plataforma para la creación y despliegue dinámico de servicios de telecomunicación centrados en el usuario*, Proceedings of the XVII Jornadas Telecom I+D, Valencia (Spain), Oct 2007.
[Yelmo&08a]	Yelmo, J.C., Del Álamo, J.M., Trapero, R., Falcarin, P., Yu, J., Carro, B., Baladrón, C., *A user-centric service creation approach for next generation networks*, Proceedings of the First ITU-T Kaleidoscope Academic Conference on Innovations in NGN, Geneva (Switzerland), May 2008.
[Yelmo&08b]	Yelmo, J.C., Del Álamo, J.M., Trapero, R., *Privacy and data protection in a user-centric business model for Telecommunications services*, IFIP vol 262, The Future of Identity in the Information Society, pp. 447-461, Springer, Jun 2008
[Yelmo&09a]	Yelmo, J.C., Trapero, R. and Del Álamo, J.M., *Identity Management and Web Services as Service Ecosystem Drivers in Converged Networks*, IEEE Communications Magazine, vol 47, no 3, pp 174-180, Mar 2009.
[Yelmo&09b]	Yelmo, J.C., Martínez, C., Del Álamo, J.M. and Monjas, M.A., *Protección de la información personal en plataformas de servicios convergentes centrados en el usuario*, Proceedings of the V Congreso Iberoamericano de Telemática (CITA 2009), Gijón (Spain), May 2009.
[Yu&09]	Yu, J., Falcarin, P., Del Álamo, J.M., Sienel, J., Sheng, Q.Z. and Mejia, J.F., *A User-centric Mobile Service Creation Approach: Converging Telco and IT*

	Services, Proceedings of the 8th International Congress on Mobile Business (ICMB09), Delia (China), Jun 2009 (Accepted for publication).
[Zuidweg06]	Zuidweg, J., *Implementing Value-Added Telecom Services*, Artech House Inc., 2006.