Trust Framework and Service Delivery in SPICE

Hariharan Rajasekaran[1], Pekka Laitinen[2], Gábor Márton[3], Robert Seidl[1], Peter Weik[4]

(hariharan.rajasekaran, robert.seidl, gabor.marton)@nsn.com
pekka.laitinen@nokia.com
peter.weik@fokus.fraunhofer.de

[1]Nokia Siemens Networks, Sankt Martin Str. 76, 81541, München, Germany
[2]Nokia Research Center, Helsinki, Finland
[3] Nokia Siemens Networks, Köztelek u. 6, 1092 Budapest, Hungary
[4]Fraunhofer FOKUS, Kaiserin-Augusta Allee 31, 10589 Berlin, Germany

Abstract — Today's network operators are envisioning a converged communication future where the Internet meets the telecommunication world. The EU IST SPICE (Service Platform for Innovative Communication Environment) project goes one step closer to this future by developing a service platform for creating mobile services based on the web services paradigm of the Internet, combined with the capabilities offered by the telco world such as unified billing and charging, presence information, identity management, etc. This paper describes the trust framework of SPICE which is responsible for identity management and access control in such a combined environment with an example scenarios showing how access to services is controlled in SPICE.

Keywords: Identity Management; Generic Bootstrapping Architecture (GBA); Trust Framework

1. Introduction

The growth in the range of services offered in the Internet has been staggering in the past few years. While the network operators were busy trying to build a telco interface to the Internet in the form of the IP-Multimedia Subsystem (IMS), the services on the Internet have surged ahead with innovative offerings to the users. One of the main hindrances for rapidly launching services in the telco world as compared to the Internet is the complexity of creating services. The services in the telco world are vertically integrated with the network operators' infrastructure which varies considerably among operators while the services on the Internet are developed based on open standards and interfaces.

To overcome this shortcoming and speed up the service creation process in the telco world, the EU IST SPICE project aims at creating a service creation and execution framework for mobile services [1]. The services in SPICE are created based on the Web services paradigm from the Internet, with features such as service composition and service brokering and they make use of the enhanced capabilities provided by the underlying telecommunications network such as unified billing and charging, identity management, presence and location information, etc. The SPICE architecture description [2] provides a detailed overview of the SPICE architecture while Figure **1** shows the relevant layers on client and service delivery platform side that are in the main focus of the SPICE project..

This paper describes the trust framework investigated in SPICE which deals with identity management and access control issues for this converged communication framework. The concept is explained with two example scenarios illustrating how a service is delivered to a user by the SPICE platform.

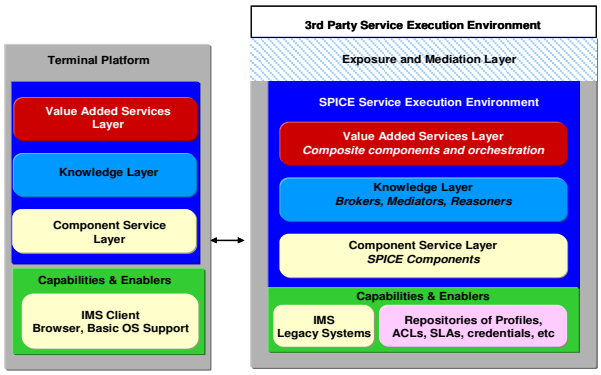

Figure 1 Overall SPICE Architecture

2. Identity Management and Access Control in SPICE

2.1 Identity Management and Authentication

One of the main design principles of the SPICE platform is that the users of the platform are necessarily IMS subscribers. This means that the users are provided with security credentials allowing the IMS operator to authenticate them. The identity management framework in SPICE offers different choices based on the method by which the user accesses a SPICE service. The SPICE initial access control architecture document [3] describes three options by which a user can access the SPICE platform:

– by using the SPICE platform like an IMS application server (AS) which implies that the IMS mechanisms for identity management and single sign-on are used
– by accessing it over HTTPS, making use of the 3GPP Generic Bootstrapping Architecture (GBA [4]) and a Network Application Function (NAF), which applies User Security Settings (USS) stored with the IMS operator or
– by a combination of GBA and Liberty Alliance [5], using the IMS credentials in the GBA authentication process. The SPICE service accessed by the user can then be seen as a Liberty Alliance Service Provider (SP). This option opens up the possibility of combining Internet-style identity federation mechanisms with credentials from the telco world and also for third-party Liberty-compliant services. SPICE implements such a combination based on the concepts proposed by 3GPP for such an interworking [6].

It is also possible for a user to use a non-IMS device to access the platform, but in this case the non-IMS device "borrows" the GBA credentials from another IMS-enabled device, of the same user, for the duration of the service access (recall that the authentication mechanisms of GBA [4] are primarily intended to be used with a smartcard which provides at least the secure storage of the shared secret). This is accomplished by the "GBA split terminal" mechanism. The workflow for this option is shown in Figure **2**.

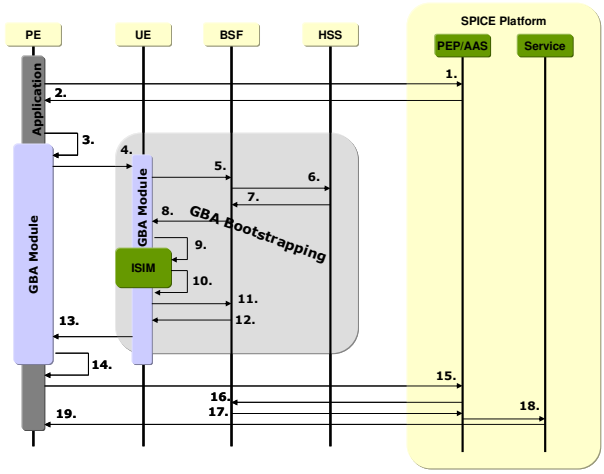

Figure 2 "GBA split terminal" mechanism of authentication

In the "GBA split terminal" scenario, the User Equipment (UE) is split in two parts where a separate Peripheral Equipment (PE), e.g. a personal computer has the application using the service, and the UE, e.g. a mobile phone, functions as the GBA key provider. The steps of the scenario, as depicted in Figure **2**, are briefly the following (for a more detailed description, see the SPICE initial access control architecture document [3]):

1. The application on the PE makes a request to the service.

2. The PEP/AAS (Authentication and Authorization Support) sends an authentication request to the application on the PE informing it that it wishes to use GBA for authentication.

3. Having discovered that GBA should be used for authentication, the application contacts the local GBA Module in the PE requesting the needed credentials (e.g. B-TID and Ks_NAF in this case).

4. The local GBA Module in PE contacts the GBA Module in the UE for the credentials. This could happen for example via Bluetooth, Infrared or cable connection.

The GBA Module in the UE discovers that the there is no existing valid GBA bootstrapping session with the BSF, hence steps 5-12 are executed; otherwise steps 5-12 are skipped. (for more details on the GBA bootstrapping process, please refer to the GBA specification [4]).

5. The GBA Module in the UE sends an HTTP GET request, containing the user's IMPI (IM Private ID, stored on a smartcard), to the BSF.

6-7. Based on the IMPI, the BSF retrieves an authentication vector (AV) and GBA User Security Settings (GUSS) from the operators Home Subscriber Server (HSS).

8. The BSF responds with HTTP Digest authentication challenge ("401 Unauthorized").

9-10. The GBA Module extracts the ISIM-specific challenge from the response, passes it to the ISIM application in the Universal Integrated Circuit Card (UICC i.e., smart card) which then calculates the response to the challenge.

11. The GBA Module derives a master key (Ks) from the calculated response for further use. The GBA Module also wraps the calculated response into an HTTP GET request with Digest authorization, and sends it to the BSF.

12. The BSF verifies the response (the user of the UE is now authenticated), generates a Bootstrapping Transaction Identifier (B-TID) identifying this bootstrapping session, as well as derives the master key (Ks), and stores both the B-TID and Ks for later use. There is now a shared secret Ks established between the GBA Module and the BSF; this secret is specific to the bootstrapping session and is of limited lifetime. The BSF returns the B-TID and the key lifetime to the GBA Module in the HTTP response message payload. The GBA Module stores the received B-TID together with the Ks. The GBA Module also derives a key Ks_NAF,

specific to the service, from Ks.

13-14. The GBA Module in the UE returns the B-TID and Ks_NAF (and their lifetime) to the GBA module in the PE, which then forwards them to the application.

15. The application uses the B-TID and Ks_NAF key to calculate a proper response to the authentication request sent by the PEP/AAS in step 2.

16. In order to verify the response, the PEP/AAS extracts the B-TID from it and contacts the BSF.

17. The BSF returns Ks_NAF and possibly further data extracted from the GUSS such as the user's persistent identifier at the service; for privacy protection purposes, this identifier is typically different from the primary identifier used at the HSS.

18. The authenticated and authorized request (with the user identity typically also inserted) is forwarded to the service.

19. The service returns the response to the application.

2.2 Access Control

The access control mechanism for service access in SPICE is based on policies [3]. It consists of Policy Enforcement Points (PEPs), policy decision points (PDPs), and Authentication, Authorization Support (AAS). All SPICE services are exposed to the outside world via a service exposure layer (SEL) which contains the PEP. Figure **3** shows the access control mechanism in SPICE. The PEP handler in the SEL sorts the incoming messages based on the request type and directs them to the appropriate PEP. The PEP with the help of the PDP and AAS enforces access policies and controls the access to services. The PEP in the service wrapper is responsible for service logic specific access control decisions while the PEP in the SEL is responsible for access control at the platform level.

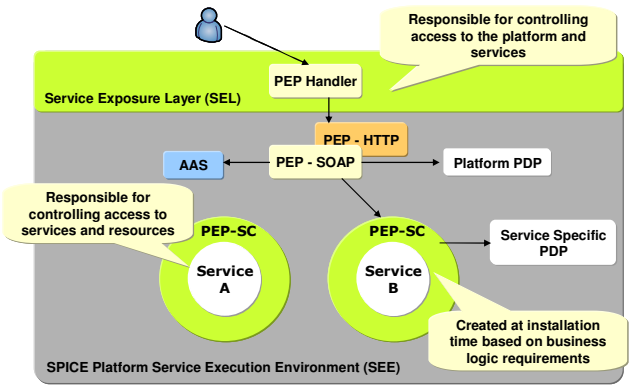

Figure 3 Access Control in SPICE

2.3 Trust Model and Inter-Platform Access

Regarding inter-platform communication, the SPICE trust model is relatively straightforward: communication between two SPICE platforms at two different operators is only possible if there is mutual trust established. Here we define trust as the validity of the following two assumptions:

- The communication between the parties is *secure*. Security of communication here means (1) authenticity of data origin, (2) data integrity, (3) confidentiality (optionally) and (4) anti-replay protection (optionally). Communication is secured by technology solutions a.k.a. security services corresponding to the above listed aspects (1-4).
- The other party is *friendly* i.e. it is not assumed to do malicious actions. Friendliness can be ensured by means of legal measures (written contract between the operators, similarly to roaming agreements); this is outside of our scope. There might also be technology solutions for ensuring friendliness, but again, these are outside of our scope currently.

Note that the above definition of trust is dedicated to our purposes in SPICE, and as such is quite limited in scope.

Security services are best implemented separate from the rest of platform elements. This saves service and component developers (even the developers of PEPs, PDPs, etc.) from the burden of implementing security features and makes the platform easier to maintain and configure. Borrowing the term from the 3GPP specification of IP network layer security [11], the elements implementing the security services are called Security Gateways (SEGs). Security Gateways in SPICE possess the following characteristics:

- Reside on the border of platform operator networks with all inter-platform SPICE traffic passing through them. Note that user-platform traffic flows via different channels (cf. AAS in the SPICE access control architecture).
- They provide the necessary security services (1-4). I.e., a pair of SEGs (at operator A and B, respectively) establishes a point-to-point secure channel between operators A and B.
- At each operator, there is one logical SEG per foreign operator. This allows for clean and easy configuration of SEGs, in accordance with the pair-wise legal agreements between the platform operators.
- SEGs are transparent to the upper layers.

The selection of the concrete technology for implementing the SEGs (whether it should be IPSec,

HTTPS, XML Security or something else, or some combination of them) remains to be specified later.

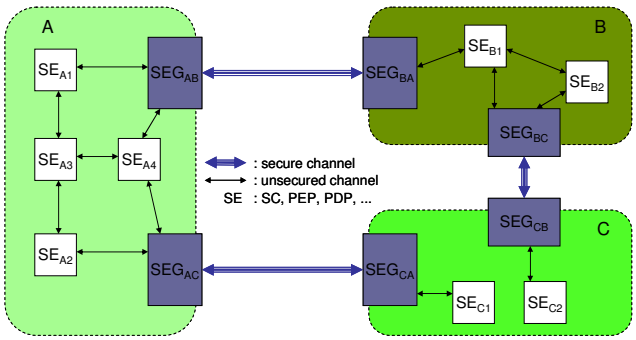

Figure 4 Security Gateways (SEGs)

Erreur ! Source du renvoi introuvable. illustrates the SEG concept. SE denotes a SPICE Element, including service components (SCs), PEPs, PDPs, etc. SEs within a platform communicate via unsecured channels; SEs in different platforms always communicate via secure channels provided by the SEGs.

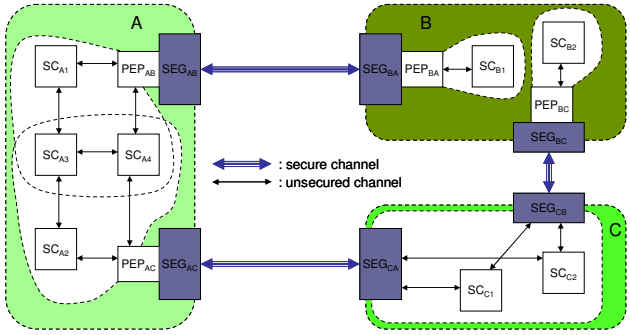

Figure 5 SEGs and trust domains

Figure 5 illustrates how SEGs and PEPs are used for opening up just a part of a platform for a partner operator. Operator A opens up part of its platform for B and another part for C, and the two sub domains overlap. The sub domains opened up by B for A and C, respectively, do not overlap. Both A and B achieve this by PEPs dedicated to each of the foreign operators. Operator C does not deploy dedicated PEPs to the SEGs; as a consequence, the whole platform is opened up for both A and B. Note that even in this third case PEPs around the SCs (not shown in the figure) may distinguish between A and B, and so may deny access from an SC at A and at the same time allow access from an SC at B.

3. Service Delivery in SPICE

To illustrate the service delivery process in SPICE , we will follow an example scenario: *A SPICE User is on holiday and she wants to order a movie from her Video on Demand (VoD) service provider in the SPICE platform and watch it on her hotel room TV (which is SPICE enabled, i.e. the TV is part of a SPICE account and is known to the SPICE platform). The User is charged for the service by her home SPICE platform operator on her mobile bill.*

SPICE offers multiple methods to realize such a use case based on the capabilities of the device on which the service is to be consumed. In this paper, we consider two cases: one where the TV set is an IMS enabled device (i.e. it contains a smartcard with appropriate IMS credentials) and the other where the TV uses the IMS credentials from another 3GPP compliant device (the "GBA split terminal" case).

3.1 Case 1: TV with own IMS Credentials

Here the requirements are that the following. The User and the hotel each have a SPICE subscription. The TVs are connected to the network (e.g. via a DSL line) and are directly addressable via their IP address. The TVs have their own ISIM information (e.g. as part of the set top-box smartcard) which are used to register/identify them on the SPICE platform and are linked to hotel's IMS and thus also SPICE subscription.

When the user checks into her hotel room, she is provided with the access code/PIN for accessing the TV in her room. At the same time, the hotel updates the access code in the policy governing access to the TV in the SPICE platform. Figure 6 shows a typical scenario.

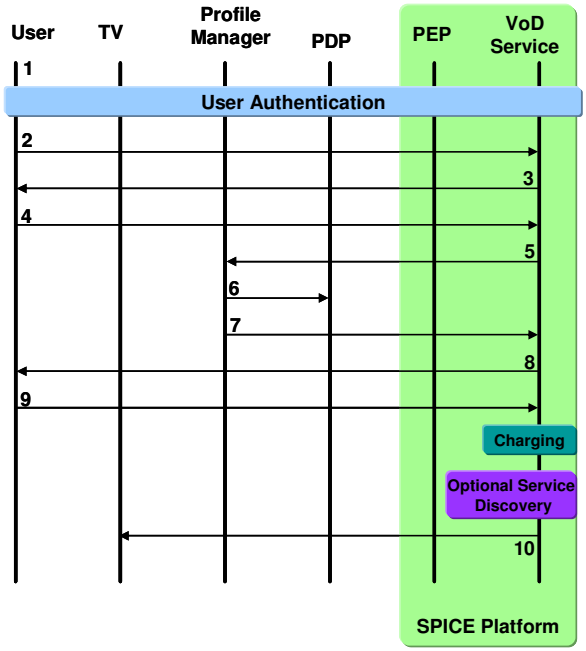

Figure 6 TV with own IMS credentials

The steps depicted by Figure 6 are the following:

1. User authentication by the SPICE platform. This can

happen via any SPICE-enabled equipment possessed by the User, and the means of authentication can be any of the three options listed in section 2 (IMS, GBA/HTTP, GBA+Liberty).

2. The User accesses the VoD service in her SPICE platform.

3. The VoD service responds with movie options and asks for device information.

4. The User chooses the movie and enters the device information (e.g. the IM Public ID of the TV and access code).

5. The VoD service requests profile information of the given TV device from the SPICE platforms Profile Manager. The TV ID and access code are passed along with the request.

6-7. The Profile Manager consults the service PDP, presenting the TV ID and access code. The PDP permits access to (possibly just a subset of) the device profile information.

8. The Profile Manager responds to the VoD service with the requested device profile information.

9. The VoD service presents the User with further options based on device information.

10. The User chooses streaming options and confirms the selected payment option. The VoD service then initiates a charging process.

11. The VoD service streams the requested movie to the selected TV device.

3.2 Case 2: TV Using Credentials from another Device

The requirements in this slightly different scenario are the following: the User has a valid IMS, SPICE and VoD subscription. The User's mobile device is GBA-enabled and also implements the "GBA split terminal" case (UE part). The TV set in the hotel room is connected to the network (e.g. via a DSL line) and is able to play a video stream — delivered by means of e.g. RTSP [8]— given its URL. The TV set in the hotel room is capable of communicating with the User's mobile device via a secure local channel (e.g. Bluetooth, infrared combined with security mechanisms) and implements the "GBA split terminal" case (TE part).

When the User checks into her hotel room, she is provided with an access code to the TV (for accessing the TV from the mobile device). Figure 7 illustrates a typical scenario.

The steps depicted by Figure 7 are as follows:

1. the User authenticates to the SPICE platform (e.g. as in step 1 in section 2).

2. The User accesses the VoD service in her SPICE platform with her device.

3. The VoD service responds with movie options and asks for device information i.e. the characteristics (resolution, color depth, etc.) of the device to which the video is going to be streamed.

4. The device profile is retrieved from the TV via Bluetooth, Near Field Communication, or their combination. For this purpose, the access code provided at check-in is also presented to the TV.

5. The movie selection and the device profile are returned to the VoD service.

6. The VoD service presents the User with further options (e.g. resolution, frame rate, subtitles) based on the device information.

7. The User chooses streaming options and the choice is returned to the service.

8. The VoD service responds with a URL of the movie.

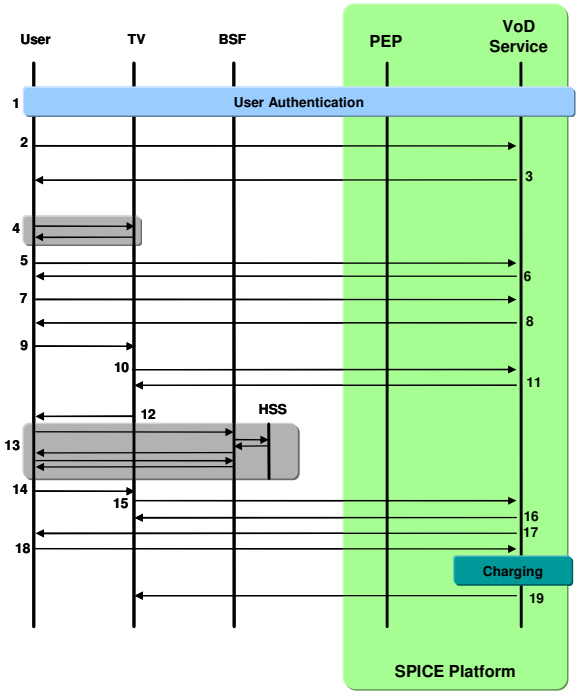

Figure 7 TV using credentials from another device

9. The URL of the movie is passed on to the TV.

10. The TV requests the movie at the URL.

11. The VoD service requests authentication from the TV.

13-14. Authentication in the "GBA split terminal" manner (steps 3-14 in Figure **2** with the TV as TE and the User's device as UE).

15. The TV responds to the authentication request.

16. The VoD service starts streaming the movie to the TV.

17. A few seconds after the movie started, the VoD service asks for confirmation of payment.

18. The User confirms payment.

19. The VoD service continues streaming the movie to the TV.

3.3 Charging

For the support of chargeable composed services, there will also be a solution provided within the SPICE project, which again makes use of the possibility to connect to existing charging infrastructures of operators. In accordance with the OMA Charging Requirements [10], there are four roles defined within the charging framework of SPICE: customers, merchants (the entity who actually delivers the service to the customer), issuers (the entity that provides the customer with payment credential) and acquirers (the entity to which the merchant provides the transaction credentials in order to receive the funds). The SPICE platform's central element for catering to all charging aspects of services is the Charging & Mediation module (C&M) which takes care of the interaction with external rating functions and the various billing domains that allow for settlement of paid services (e.g. the billing domains of telecommunication operators but also banks or credit card systems). The C&M module will offer a means of collecting information for non-real-time services in offline charging processes for a later settlement, but will specifically also support the settlement of real-time services and of course for services that have been created as composed services.

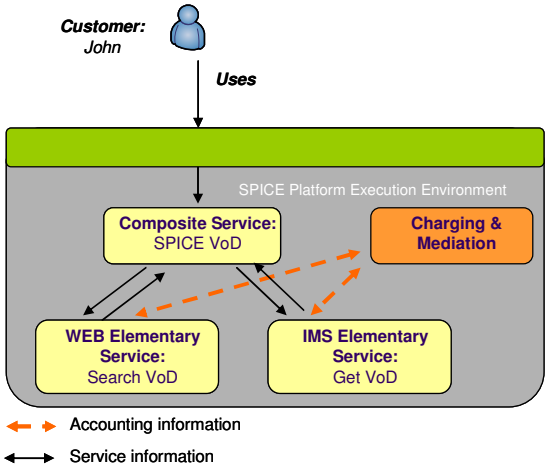

Figure 8 Charging in SPICE

The C&M will communicate via Web Services with the SPICE platform components and will do the settlement via FTP or in case of real-time/online charging cases via the Ro interface [12] of the IMS operator.

4. Conclusion and Outlook

Standardization bodies have just started the process of bringing identity management concepts from the telecommunication and the Internet world together. The SPICE project's trust framework introduces the interworking between Liberty Alliance concepts for federated identity management and telco-based HTTP authentication processes based on smartcards. This paper outlined how the two concepts can be combined in two detailed service access scenarios and showed the SPICE trust model. This interworking based on GBA has been validated in a demonstrator which shows the benefits of single sign-on from various access devices and networks. The SPICE project will continue until mid 2009 and further investigations and demonstrator extensions are envisioned in the direction of Personal Network Management (PNM) [9] which is currently under discussion at 3GPP.

5. Acknowledgment

This work has been performed in the framework of the IST project IST-2005-027617 SPICE, which is partly funded by the European Union. We would like to thank all SPICE project partners for the useful discussions and contributions to this paper.

6. References

[1] SPICE project homepage, http://www.ist-spice.org
[2] SPICE Deliverable D1.3, Initial architecture design, http://www.ist-spice.org, Sept 2006.
[3] SPICE Deliverable D6.3, Initial Access Control Architecture, http://www.ist-spice.org, Dec 2006.
[4] 3GPP TS 33.220, Generic bootstrapping architecture, http://www.3gpp.org/ftp/Specs/archive/33_series/33.220/
[5] Liberty Alliance Project, http://www.projectliberty.org/
[6] 3GPP TR 33.980, Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA), http://www.3gpp.org/ftp/Specs/archive/33_series/33.980/
[7] Fokus Open IMS Core, http://www.openimscore.org/
[8] IETF RFC 2326, Real Time Streaming Protocol (RTSP), http://www.ietf.org/rfc/rfc2326.txt
[9] 3GPP TS 22.259, Service requirements for Personal Network Management (PNM), http://www.3gpp.org/ftp/Specs/archive/22_series/22.259/
[10] Charging Requirements. Candidate Version 1.0 – 18 Nov 2004. Open Mobile Alliance, OMA-RD_Charging-V1_0-20041118-C, http://www.openmobilealliance.org/release_program/charging_v1_0.html
[11] 3GPP TS 33.210, 3G Security; Network Domain Security; IP network layer security, http://www.3gpp.org/ftp/Specs/archive/33_series/33.210/
[12] 3GPP TS 32.299, Telecommunication management; Charging management; Diameter charging applications, http://www.3gpp.org/ftp/Specs/archive/32_series/32.299/