Future Network & MobileSummit 2010 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2010
ISBN: 978-1-905824-18-2

A 3GPP Open-ID Framework

Rodolphe MARQUES[1], Ricardo AZEVEDO[2], Rui L. AGUIAR[1], André ZUQUETE[3]
[1]*Instituto de Telecomunicações, Universidade de Aveiro, 3810-193 AVEIRO, Portugal*
Tel: +351 234 377900, Email: rmarques@av.it.pt, ruilaa@ua.pt
[2]*Portugal Telecom Inovação, 3810-106 AVEIRO, Portugal,*
Tel: +351 234 40 32 00, ricardo-a-pereira@ptinovacao.pt
[3]*Universidade de Aveiro, 3810-193 AVEIRO, Portugal*
Tel: +351 234 377200,andre.zuquete@ua.pt

Abstract: Currently Mobile Network Operators (MNO) rely on an authentication, authorization and profile management architecture which has proved, by its generalized use and acceptance, as being appropriate. The use of a secure component, the SIM-Card, provides a set of capabilities not seen in other access architectures and an advantage for MNOs. Nevertheless upcoming requirements in terms of open interfaces, new services and customer demands are questioning the actual architecture. This paper presents a novel approach to authentication and profile management that can be reused by both MNOs and 3rd party providers to answer the upcoming requirements. Here, a user is able to store his own identity information in different places, while taking advantage of the strong authentication mechanisms provided by the MNO. Furthermore, by integrating MNOs' generic authentication architecture with user-centric identity management, we are creating a generic way for service providers to reuse this authentication infrastructure, providing both single sign-on and strong authentication.

Keywords: 3GPP, Mobile Operators, Identity Management, Virtual Identity, Authentication.

1. Introduction

In mobile networks, authentication and authorization mechanisms are currently built based on traditional, fixed telecommunication's logic, but enhanced to handle roaming issues, providing a way for customers to change their access networks. To provide roaming, a set of bilateral business agreements must exist between operators. This comprises the kernel of the Mobile operator industry's trust model. The idea is that if a subscriber's home operator provides guarantees for its subscriber's resource consumption (i.e. network usage), then a trusted visited operator will also offer its resources. Cross-operator payments are transparent for customers and a private matter between the home and foreign operators. The information stored in the customer's profile (of increasingly value) always remains confined to the home operator, even during roaming operations.

This mechanism has been working for several years, but current trends are underlining its limitations. Users' identification, associated identifiers and attributes, are still controlled and limited to the operator's domain: MNOs maintain all the authentication/authorization functions closed, without external interactions. This fact affects user privacy and autonomy: all the information about the user is stored and known by a single entity. No other provider (a 3rd party provider) can reuse the users' identifiers and attributes, stored in MNO's AAA services, in order to offer new services to the users, thus reducing the set of services that could otherwise be available to users. Consequently, 3rd party providers are overcoming this problem by simply creating and maintaining their own AAA systems. This (simple) solution has serious disadvantages for MNOs business: from an "owner of the customer"

starting point, the MNO is being completely removed from the revenue chain – and as services become available across multiple technologies, the MNO is risking losing even its transport role. Of course, even from the users' point of view, this is not a good scenario as well: it introduces *well-known* issues for the users' Identity Management e.g. lack of support for SSO (Single Sign-On) between operators and 3rd party services, identity silos, etc...

To tackle the referred problems, MNOs should provide a set of open interfaces to their AAA domain – this information per se has business value, as it is well recognized already in Internet service provisioning. More than just solving a revenue-related problem, MNOs can introduce advantages for all the players. They have a commercial relation with the users and own an important, widespread, and accepted secure token – the SIM card[1], implemented by an Integrated Circuit Card (ICC) device. With the use of the SIM card and the related infrastructure, a MNO can provide *strong authentication* mechanisms *as a service* for external players to use, giving advantages for all. Moreover, if willing, a MNO customer can also have his identity information spread along different trusted providers and use MNO's strong authentication mechanisms to access such (and different) services, thus transforming a previous closed system into a user-centric IdM framework with added security mechanisms.

In this paper, we describe an architecture that repositions MNOs as central players in the revenue chain, provide SSO for users and addresses privacy concerns by allowing users to have their identity data spread along many trusted providers. In section 2, we present related work on identity management. Section 3 presents a basic overview on the 3GPP AAA mechanisms and associated identifiers, upon which we aim to base our proposal, while section 4 discusses our solution to the problem. Section 5 concludes our paper.

2. Related Work

There are several ideas already for addressing Identities in a consistent way both in the telecommunication and Internet domains. Of special relevance for the telecommunication world, are efforts inside standardization organizations.

GSMA has recently started the work to standardize a set of high level interfaces to allow MNOs to expose their services (Charging, Identity, Messaging …) to 3rd party providers, through the OneAPI [2] initiative. This initiative tries to integrate, both Operators and Web domains, making it easier for new players to appear. The OneAPI work is stills immature – the MNO is considered only as a producer of information, rather than also a consumer. Nevertheless this is an interesting step to open MNOs interfaces to bring telecommunication and Internet worlds together.

Another joint effort, between Liberty Alliance (LA) and 3GPP, proposed a set of mechanisms to allow the integration of LA – Identity Federation and the Web Services Framework with the Generic Bootstrapping Architecture, the reference for 3GPP [3]. This integration offers a simplified sign-on and session management for complex web service business interaction protocols over a mechanism that provides shared secret and certificates to two communicating entities for mobile applications. This work is a real progress towards the integration of the telecommunication and Internet world. Nevertheless it lacks some important points. It doesn't support identity attributes split across different entities. Customers still have to maintain all their attributes in the MNO domain – hindering privacy. Another important issue is the lack of support for attributes sharing between telecommunications and Internet domains – Only the telecommunication domain provides strong authentication mechanism.

[1] SIM-card is a popular, short expression for "ICC device with Subscriber Identity Module"

An interesting proposal extends the cellular authentication mechanism as a service. In [4] the authors discuss the 3GPP Generic Authentication Architecture (GAA) solution, its implementation options, advantages and applicability. According to the authors, by reusing cellular authentication we are eliminating the critical step of provisioning the security credentials, or the distribution of smart cards, while proving a stronger authentication when compared to the normal username and passwords.

3. 3GPP Generic Bootstrapping Architecture

2.1 Architecture

The mobile world supports its AAA functions split in two different locations: in an ICC device (the SIM card for 2G and USIM card for 3G networks); and in network-side elements, the HLR (Home Location Repository) and AuC (Authentication Centre) functional entities. The first one contains and manages all subscriber identifiers, while the second maintains and handles security and authentication information (authentication vectors and roaming access keys). If an IMS (IP Multimedia Sub-system) is added to the cellular system, a new function called HSS (Home Subscriber System) appears to include some functions of the HLR.

3GPP GAA (Generic Authentication Architecture) VI has been defined by 3GPP to accomplished advanced authentication and security procedures in GPRS/UMTS networks. This development started in the 3GPP Release 6 [5]. Note that the GAA by itself does not provide services such as SSO, only secrets sharing between users and network.

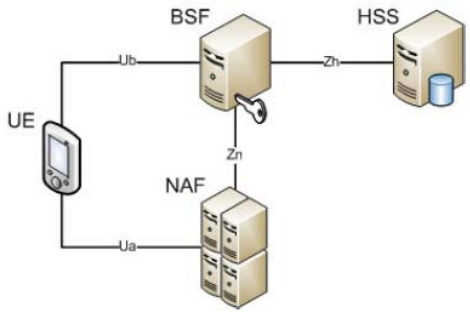

Figure 1: Generic Authentication Architecture

Figure 1 shows GAA entities and their interfaces. The UE (User Equipment) and the Bootstrapping Server Function (BSF) use the HTTP Digest AKA protocol for mutual authentication, over the Ub interface. They also agree on session keys that are afterwards applied between the UE and the Network Application Function (NAF) over the Ua interface. Those keys are restricted to a specific NAF. The Zn interface enables the NAF to verify if a UE was correctly authenticated against the BSF. NAF represents the HTTP or HTTPS service that requires 3GPP authentication. NAF can be divided in two parts – Authentication Proxy (AP) and the Application Server (AS). In such a case, the AP is only responsible for the authorization of the client, while the AS implements the application's functionality, relying in the authentication provided by the AP.

BSF uses the Zh interface to retrieve users' profile information from the HSS entity. That information is part of the users' identity (Figure 2 and Figure 3).

2.2 Identifiers

Associated with the subscriber there are several identifiers used for different purposes, stored and maintained by different entities [6]. Figure 2 provides a graphical view of the distribution of the most important identifiers among different components. The IMSI is the subscriber number; the ICCID is the SIM-card's serial number; the IMEI is the handset serial number. The IMSI and the ICCID, along with OTA (over-the-air) keys used for management operations, are stored in the HLR and in the SIM-Card. The IMEI is stored in the handset (typically it is also stored in the HLR for maintenance purposes).

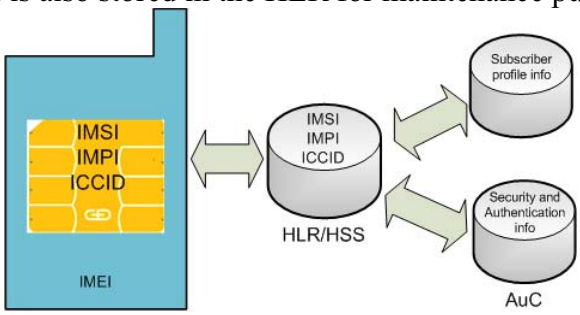

Figure 2: Generic Identifiers Distribution

The AuC mainly stores security data, the authentication vectors and a set of keys used to authenticate the client and to protect the radio link between the handset and the base-stations. In IMS-enabled networks, the HSS is an enhanced HLR which stores the IMPI and IMPUs. Those are the IP Multimedia Private (IMPI) and Public identifiers (IMPUs) of the subscriber. A subscriber has an IMPI and can have several IMPUs. The idea is to protect the subscriber private identifier. One or more Service Profiles may exist associated with each IMPU to specify the service's subscription a user has contracted (Figure 3). Full mapping between all identifiers and the subscriber is only available to the MNO.

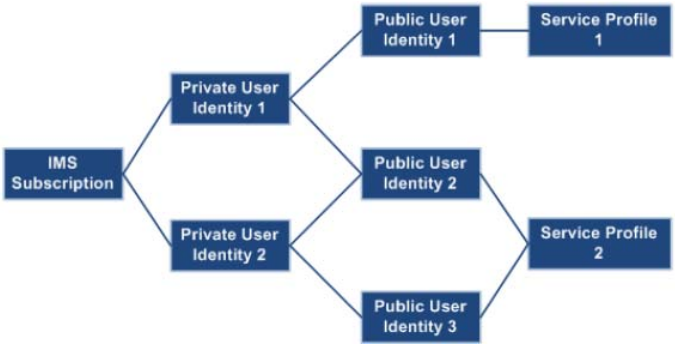

Figure 3: Relation between IMS identifiers, subscription and service profiles [7]

2.3 3GPP bootstrapping

The GAA describes the framework for the AAA mobile network architecture. Within the GAA, the Authentication Bootstrapping Procedure [9] (GBA) VI describes the functions and the process used for user authentication.

When the UE wants to interact with the NAF, it starts communication with NAF over Ua interface without GBA parameters (Figure 4). If the NAF requires the use of shared keys obtained by means of GBA, but the request from UE does not include GBA related parameters, the NAF replies with a bootstrapping initiation message.

After this the UE sends an HTTP request to the BSF and the BSF retrieves the complete set of GBA user security settings and one Authentication Vector (AV) over the reference point Zh from the HSS. Part of the values retrieved from the HSS is sent to the UE in the 401 message. The UE verifies if the challenge is from an authorized network and calculates a session key. A key is also generated in the BSF, which receives a HTTP request with the Digest AKA response. The BSF authenticates the UE by verifying the Digest AKA response. The BSF generates key material and the B-TID (Bootstrapping Transaction Identifier) which is used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn. Finally, the BSF shall send a 200 OK message, including the B-TID to the UE to indicate the success of the authentication and the key's lifetime.

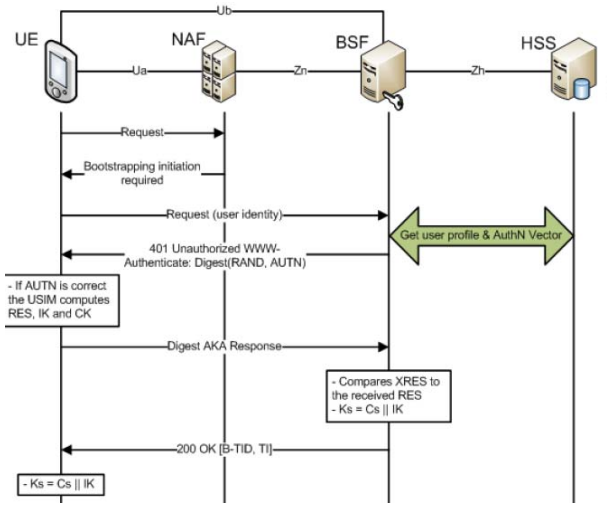

Figure 4: Authentication Bootstrapping Procedure

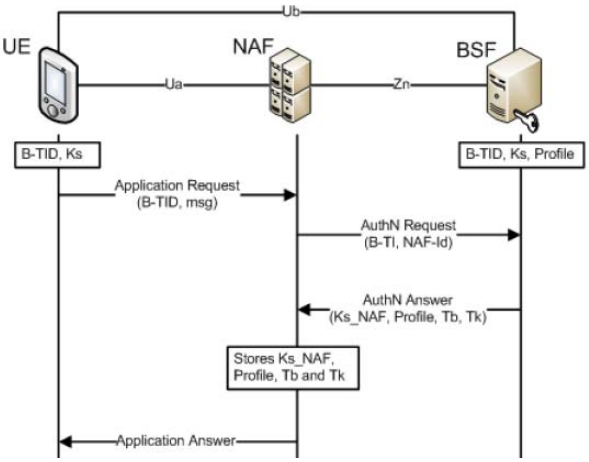

Figure 5: Bootstrapping application

If the UE and the NAF agree on using bootstrapping, the UE starts communication over reference point Ua with the NAF by supplying the B-TID to the NAF to it to retrieve the corresponding keys from the BSF (Figure 5). The NAF requests to the BSF, key material corresponding to the B-TID supplied by the UE. With the key material request, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able to verify that NAF is authorized to use that hostname. The NAF may also request one or more application-specific USSs for the applications, which the request received over Ua from UE may access.

4. IdM Open Systems Integration/Interworking with 3GPP

The 3GPP GAA, albeit powerful, has several limitations, as we have identified in previous sections. However, the integration of an open Identity Management system into 3GPP, in a path along the lines suggested by LA, may be a powerful mechanism for MNOs.

4.1 Virtual identities and virtual identifiers

The framework proposed here provides users with the ability to define profiles that can aggregate authentication credentials and attributes from different identity providers. This group of information is called a user profile or virtual identity. Users can refer to this profile by means of a Virtual Identifier (VID) when accessing a target service [8].

Figure 6 shows the relationship between VID, User Profile, authentication credentials and user attributes.

A User Profile references to one Authentication ID (AuthN ID), and therefore to the authentication credentials requested during the authentication process. Moreover, it might contain references (AttrIDs) to several attributes held by different attribute providers. For example, Alice might define a User Profile referring her identity defined in her home network provider, such as alice@homeprovider.com. At the same time, this profile can hold the attribute *connection_type* defined in her home network as *premium*, and the *attribute role* defined as *vipclient*, held by another attribute provider where Alice has another account.

The VID can be seen as a piece of information that references to a user profile, and includes information about the domain where the VID was created. In the example given above, alice@aggregator.org may represent a VID from the domain aggregator.org pointing to the profile identified by Alice. For privacy reasons, when an end user requests access to some services, the user profile pointer will be replaced by a protected (encrypted) identifier or artifact, so only the Aggregator ID will be disclosed to Service Providers.

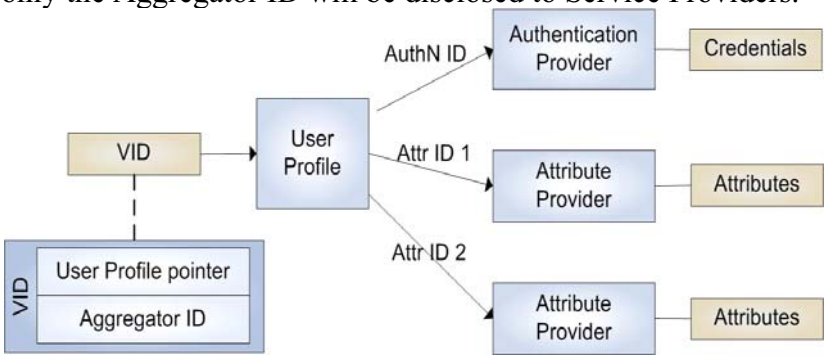

Figure 6: User Profile content

4.2 IdM Framework Elements

The Identity Management framework defines elements that can be seen as roles potentially played by one or different parties, depending on the business model. That is, we do not provide a specific instantiation of these elements but just a description of their functionality.

An **End User** is an entity who has at least one subscription with an Authentication Provider or Attribute Provider. Relatively to that provider, the end user has an identifier and a set of attributes associated with that identifier. For authentication reasons, the end user has to know some authentication credentials.

A **Service Provider** protects the resources being shared across the federation. They make use of Identity Providers (authentication, attribute or aggregator) in order to verify the identifiers (including VIDs) presented by the end users and to retrieve the attributes needed to determine an authorization decision.

An **Authentication Provider** is used to prove the identity of the end users. Therefore, users must have a previous subscription with this provider and must share some kind of authentication credentials, which will be used by the end user for proving a legitimate ownership of a given VID.

An **Attribute Provider** is responsible for managing user attribute data. The information managed by these providers can be related to specific services or can be for general purpose.

The **Identity Aggregator** is responsible for the management of user profiles, VIDs and SSO mechanisms and statements on behalf of the user. Identity Aggregators can maintain different federation agreements with the Authentication and Attribute Providers related to the Virtual Identities.

Moreover the Identity Management framework builds upon a federation between trusted parties, belonging to different domains, were service agreements are established and all

security related countermeasures are deployed with the main goal of always preserving users privacy, by assuring the unlinkability of users identities/pseudonyms across all interactions performed by the user inside the framework.

4.3 3GPP GBA/ IdM Interworking

For the interworking of such an Identity Management (IdM) framework with the 3GPP GBA, we need to define the functional interrelations. The Authentication Provider will be used as a Network Application Function (NAF) that provides identity and SSO services. It behaves as a NAF using the 3GPP GAA and related interfaces to authenticate the End User, and then generating the necessary credentials needed by the End User to access a Service Provider. Here a federation has to exist between the IdM and MNO domain where 3GPP interfaces and related protocols are used in the interactions between the IdM framework elements and 3GPP entities. Do to the nature of this IdM framework, where functional entities are separated in a fine grained structure, it provides a flexible way for mapping IdM related interactions on top of existing network architectures, although such mapping is out of scope of this paper.

Figure 7 details this operation, based on the identity management system defined inside the SWIFT (Secure Widespread Identities for Federated Telecommunications) project [1] SWIFT aims to design a user-centric identity and privacy framework, which improves the LA approaches in terms of where attributes are stored and shared, thus enhancing overall user's privacy.

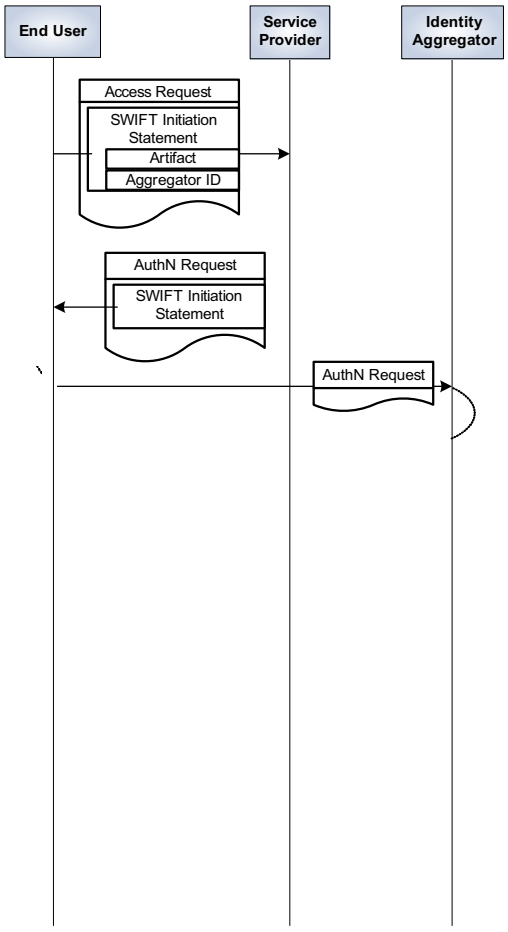

Figure 7: Identity Management/GBA Interworking

Overall, the interoperation can be described as:

1. The End User starts by sending an Access Request to the Service Provider.
2. The Service Provider redirects the End User to the Identity Aggregator with an Authentication Request Message.
3. At the Identity Aggregator, the End User is redirected to the Authentication Provider, that plays the role of a Network Application function, with an Authentication Request message.
4. The Authentication Provider receives the message and starts the authentication process. Now the Authentication Provider, playing the role of a NAF, makes use of the 3GPP GAA to authenticate the End User.
5. The Authentication Provider/NAF uses the 3GPP GAA to request credentials needed to create the Authentication Response.
6. The Authentication Provider redirects the EU to the Identity Aggregator, with an Authentication Statement for the Identity Aggregator.
7. After receiving the Authentication Statement, the Identity Aggregator redirects the End User to the Service Provider, with an Authentication Response, a SWIFT SSO Statement, and an Authentication Statement for the Service Provider.

In a user-centric IdM environment, like SWIFT, the end user should be able to have complete control over who authenticates him, who manages his VIDs and user profiles, where his attributes are stored, and policies for attribute sharing. Current IdM frameworks already support these features providing a simple SSO user experience. However, most IdM frameworks nowadays lack support for strong authentication of end users VID, relying only on user name and password. IdM frameworks can overcome this problem by simply interworking with the 3GPP GBA. By doing this, the IdM can eliminate the need for provision of security credentials, and can rely in a well-know, widely deployed, strong authentication mechanism. In this case the MNO is used as a provider of authentication services, which open a new business area for MNOs.

The main advantage of co-allocating the Network Application Function with the Authentication Provider is to allow the end user to have several Authentication Providers for the same VID. Thus, the end user can use the GBA for strong seamless authentication when using a 3GPP enabled device; or can make use of GBA for a two level authentication when, for instance, the level of assurance calculated by the Service Provider is too low (then it can ask the End User to prove his identity by using a stronger authentication method, in this case 3GPP GBA). This would also enable split-terminal functionalities: the end user could still perform a GBA authentication when using a terminal that does not include a UICC (such as a laptop). In this case the end user would use another 3GPP terminal (for instance a mobile phone) and GBA to provide the necessary credentials to access the Service Provider while using the service in a laptop.

5. Conclusion

This paper presented a way in which Mobile Network customers can use their identity information, stored in different providers, while taking advantage of the strong authentication mechanisms, provided by MNOs. This proposal brings the flexibility of Internet-style IdM systems with the trust of 3GPP GAA systems, opening a new business area for MNOs. The complexity of the solution seems to be minimal, and mostly a matter of interface specifications.

The presented architecture and mechanisms are being studied within the IST-SWIFT project, where a set of prototypes is being develop to evaluate the solution. The proposed solution presents a novel approach backed up by the SWIFT IdM framework which allows a user to maintain its attributes across several Attributes Providers as well as the ability to

use multiple authentication methods through Authentication Providers associated to a given VID. These unique characteristics of the SWIFT IdM framework, together with the fact that this is a new field of research, makes it difficult to perform a comparative quantitative analysis with the reduced number existing proposals.

References

[1] Girao, J. (ed.), "SWIFT, Deliverable 203, First Draft of the Identity-driven Architecture and Identity Framework," 2008.

[2] "GSMA OneAPI Reference Implementation", http://oneapi.aepona.com/

[3] 3GPP TR 33.980: " Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic authentication Architecture (GAA) (Release 7)", (2006-03).

[4] Laitinen, P.; Ginzboorg, P.; Asokan, N.; Holtmanns, S.; Niemi, V., "Extending cellular authentication as a service," Commercialising Technology and Innovation, 2005. The First IEE International Conference on (Ref. No. 2005/11044) , vol., no., pp.0_90-D2/4, 14-15 Sept. 2005

[5] 3GPP TR 33.919 V8.0.0: "Generic Authentication Architecture (GAA); System Description", 2008

[6] ETSI Standard EN 301 243 V4.0.1: Digital cellular telecommunications system (Phase 2); Enhanced Full Rate (EFR) speech processing functions; General description (GSM 06.51 version 4.0.1)

[7] 3GPP TS 23.228 V9.1.0: "IP Multimedia Subsystem (IMS)", 2009

[8] A. Sarma, A. Matos, J. Girão, and R. Aguiar, "Virtual identity framework for telecom infrastructures", in Wireless Personal Communications, (Netherlands), Springer, February 2008. ISSN 0929-6212

[9] 3GPP TS 33.220 V8.5.0: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture", 2008