Authentication in a multi-access IMS environment

Do van Thanh – Telenor & NTNU, Norway – thanh-van.do@telenor.com
Ivar Jørstad – Ubisafe, Norway – ivar@ubisafe.no
Paal Engelstad – Telenor, Norway – paal.engelstad@telenor.com
Tore Jonvik – Oslo University College, Norway – tore.jonvik@iu.hio.no
Boning Feng – Oslo University College, Norway – boning.feng@iu.hio.no
Do van Thuan – Linus, Norway – t.do@linus.no

Abstract – The standard ISIM-based authentication mechanism of IMS is only intended for mobile phones and cannot be used for fixed IMS clients on stationary devices without SIM cards. This paper presents the authentication schemes dedicated for fixed IMS clients. Such schemes are necessary in order to extend the usage of IMS to fixed environments. Authentication solutions for other applications than the IMS client are also described. These applications are assumed to be located on the same stationary device as the IMS client, and might for example be browsers, contact lists and email clients. Finally, a Single-Sign-On mechanism is proposed. It is designed to simplify the authentication process without compromising the security.

Keywords: Authentication, Single-Sign-On, Identity Management, User Identification, User Subscription, User Management, Identity Federation

I. INTRODUCTION

The IP Multimedia Subsystem (IMS) [1][2] was developed by the 3rd Generation Partnership Project (3GPP) [3]. Telecom operators have successfully used it as a renovating SIP (Session Initiation Protocol) [4] and IP based signalling technology in the replacement of circuit-switched (CS) network elements.

IMS was originally designed for mobile phones in mobile networks and did not take into account other types of networks and devices. In fact, no other IMS clients than mobile phones are supported by current IMS technology. However, IMS does have the potential of becoming a core infrastructure that couples together different networks, such as GSM/GPRS/UMTS, PSTN, xDSL and WLAN.

There is now a wish to go one step further and use IMS to provide a unified subscription plan that includes mobile, fixed and broadband services. A big obstacle is that the authentication of IMS clients must rely on the ISIM (IP Multimedia Services Identity Module) [5] located on a SIM (Subscriber Identity Module), but in fixed environments devices normally do not carry any SIM [6] card. Thus, other authentication solutions must be provided for stationary devices.

Another limitation of current IMS authentication, is that it is supporting authentication only for the IMS client. However on any device, fixed or mobile, there will normally be other applications that an IMS client needs to interact with. Such applications include browsers, contact lists, SMS (Short-Message Service) [7] clients, email clients, etc. These applications also need support for authentication.

Finally, in a changing environment, where the user might change dynamically between using different applications, networks and devices, current IMS authentication will be cumbersome. Each time a user for example is changing IMS-based application, the user has to be involved in a new re-authentication procedure. Instead, a Single-Sign-On (SSO) mechanism should be provided, so that the user only needs to be involved in the authentication procedure once, e.g. when booting his device or when initiating his IMS client. Such a Single-Sign-On mechanism is necessary for successful deployment of IMS in a mobile-fixed convergent environment.

This paper presents some of the authentication schemes proposed by the EUREKA Mobicome project, which is aiming at providing a unified subscription plan for a Fixed-Mobile Convergent IMS environment.

The paper starts with related works in Section II, and a brief summary of the standard authentication mechanism of IMS in Section III. In Section IV, the different authentication schemes for IMS clients on stationary clients are thoroughly explained. Section V addresses the need for authentication solutions for other applications on the device than the IMS client. Here, different authentication schemes are described. In Section VI, a Single-Sign-On mechanism is proposed in order to simplify and speed up the registration and authentication process. This solution will enable SSO across different service instances and across different service types. Finally, directions for further work and conclusions are provided in Sections VII and VIII.

II. RELATED WORKS

TISPAN [8] works together with 3GPP to extend the reach of IMS to fixed networks, as well as to other wireless access networks. The authentication approaches for IMS covered by TISPAN Release 1 are:

1 The EUREKA Mobicome project (Nov 2007-April 2010) has as partners: Telenor, Telefonica, HuaWei, HyC-Ericsson, Polytechnical University of Madrid, Oslo University College, Blekinge Institute of Technology, Linus, Ubisafe and WIP.
• NASS (Network Attachment Subsystem) Bundled Authentication (NBA): With this solution, the access level authentication is re-used for the IMS/application level.

• IMS Residential Gateway (IRG): With this solution, an adapter for legacy terminals is equipped with an ISIM, so that the adapter can authenticate on behalf of the user. The user equipment (PC, SIP phone etc.) communicates using IMS/SIP towards the IRG.

• Residential GW/Access GW: With this solution, the legacy terminal does not communicate using SIP at all. The authentication is based on the fixed line identification, and the IP traffic is transported only in the operator’s domain.

One of the drawbacks of all these solutions is that they do not authenticate the actual user of the IMS service, but they authenticate only one subscription, i.e., either the subscription of the fixed line or of the SIM inserted into the IRG.

III. STANDARD AUTHENTICATION FOR IMS

The standard authentication for IMS is based on the ISIM (IP Multimedia Services Identity Module) [9][10]. The foundation for the ISIM authentication is the IMS identifiers stored in, and used by, the ISIM application. The ISIM application is kept on a Universal Integrated Circuit Card (UICC). The data stored by the ISIM constitutes public and private user identities, home network domain URI (Universal Resource Identifier) and a long-term secret (key). The user can have one or more public user identities. These are the identities used by others when they want to contact you, and they are represented by a SIP URI or a TEL URI (e.g. sip: ivar.jorstad@ubisafe.no or tel:+47-12345678).

The actual authentication of an IMS client is based on the long term key associated with the private user identity, and this is stored on in the ISIM and in the HSS of the home network of the user. IMS adopts the Authentication and Key Agreement protocol (AKA) [11] for the actual authentication process. The IMS AKA is conceptually similar to UMTS AKA used for access authentication in 3G networks, but the transportation of the parameters used in the process is slightly different. In UMTS, the authentication response from the user equipment, called RES, is sent in the clear, whereas in IMS AKA, it is combined with other parameters and the resulting data is protected and sent as an authentication response instead. The ISIM Authentication procedure is shown in Figure 1.

It is worth emphasising that the standard authentication procedure is intended for the IMS client and tightly coupled with the SIM card. It is hence unusable neither for other applications nor for an IMS client on a stationary device without a SIM card.

IV. AUTHENTICATION ON STATIONARY DEVICES

The usage extension of IMS to fixed environments requires the implementation of IMS clients on stationary devices such as PCs, Set-Top Box, IPTV, etc. and authentication schemes for these IMS clients. The authentication can e.g. be performed by using a USB SIM dongle attached to the PC or by accessing the SIM across a Bluetooth connection when the SIM is still inserted in the mobile phone.

A. Authentication for PCs using USB SIM dongle

To accommodate the use of IMS clients also on ordinary PCs, authentication using the SIM card is the first step, since IMS inherently uses a SIM card in the authentication process. In “Full-IMS”, an ISIM is mandatory (as described in Section II), while in “Early-IMS” [12] allows for using an ordinary SIM card instead. In “Early-IMS” there is no IMS level authentication. Instead, IMS relies on the bearer level security at the GPRS or UMTS PS (Packet Switched) level. The procedure does not include key agreement either, so there is no IPSec security association between the UE (User Equipment) and the P-CSCF (Proxy Call Session Control Function) of IMS.

In the solution described in this paper, a SIM card is used for authentication on the IMS level, by inserting it into a USB SIM dongle. A supplicant is introduced on the PC, which is able to coordinate authentication requests back and forth between the IMS client and the SIM card. Possible mappings of the GSM authentication procedure onto IMS AKA have been described in [13]. These mappings require changes to no other network elements than the IMS client and the S-CSCF. The architecture of this solution is shown in Figure 2.
One of the advantages of this solution is that it reuses the ordinary SIM-card, which is well adopted and in widespread use.

Figure 2 Components of the IMS SIM authentication solution

B. Authentication for PC using mobile phone with Bluetooth

Another option, which is similar to the previous one, is to use the SIM for authentication while the SIM is still inserted into the user’s mobile phone. A supplicant is also here introduced on the PC, and this supplicant is able to communicate with the SIM on the mobile phone across a Bluetooth connection. To access the SIM card, the SIM Access Profile (SAP) is utilised [14]. The architecture of this solution can be seen in Figure 3.

Figure 3 Components of the IMS SIM authentication with mobile phone

When accessing the SIM card using SAP, the security association on the Bluetooth link between the client on the PC and the mobile phone needs to be stronger than the default level. A 16 bytes key is required when establishing this link, and this further improves the security of the complete solution and reduces the risk of eavesdropping.

C. Authentication for Set-Top Box using Soft SIM

It is envisaged that many consumer electronic devices, such as Set Top Boxes, home gateways, door monitors, etc., might be equipped with IMS clients that will require authentication. It is, of course, possible to equip such devices with SIM cards as in mobile phones, but this requires the tedious task of installing the SIM card. To remedy the situation, the 3GPP has initiated several activities to explore the implementation of soft SIM or downloadable SIM [15][16] that can be downloaded over the air and installed on embedded secure devices, such as ARM® TrustZone™. With the existence of the soft SIM, the standard IMS authentication using the ISIM can be employed in consumer electronic devices.

V. AUTHENTICATION OF OTHER APPLICATIONS

Initially, IMS services were supposed to be accessed by users through dedicated IMS clients. However, to provide a seamless experience for the users, some services might in fact be initiated through other types of clients, while still employing IMS as a service platform. For example, an IMS messaging session might be initiated through a Web-browser, but if the user wants to switch to a voice service instead, the switch could be performed through the Web-interface. This allows for reusing the already authenticated session, and provides a more seamless service experience for the user. The service will in this case trigger the IMS voice client on the actual device to handle the voice communication, while the Web-browser and HTTP are used as a an overlay signalling channel. The most crucial part of realising this scenario is to enable seamless authentication across various applications and service platforms (in this case Web, IMS and SIP).

A. Authentication of the browser using GBA

The goal of the Generic Bootstrapping Architecture (GBA) [17] is to establish a shared secret between a client and a service provider, and in the process of establishing this secret, the credentials for the mobile network is used (i.e., the ones stored on the user’s U/ISIM).

In the establishment phase, referred to as the GBA Bootstrapping authentication procedure [17], the user is authenticated using the SIM card. It is the Bootstrapping Server Function (BSF) that is responsible for this procedure. The BSF is connected to the HSS and performs the standard AKA (Authentication and Key Agreement) authentication procedure using the U/ISIM card. After the user has been successfully authenticated, a shared key is established between the client and the service provider. This is a short-term security association, and it is specific and unique for the client and service provider in question (it is identified by a Bootstrapping Transaction Identifier, B-TID). The CK (cipher key) and the IK (integrity) of the AKA procedure are concatenated in order to establish the shared key $K_s$. The actual key used between the client and service provider is derived from $K_s$ using a key derivation function. The service provider retrieves the final key from the BSF, whereas the client derives it on its own upon service access. A simplified view of the process is shown in Figure 4.
B. Authentication of the browser using SIM Strong Authentication

In StrongSIM [18], solutions for authenticating a user towards Web-based services using SIM cards have been proposed. The basic architecture can be seen in Figure 5. A Supplicant is present in the Web-browser (or the browser is able to communicate with a standalone Supplicant), and this Supplicant can communicate both with the SIM card and the Authenticator in the operator network.

In the illustrated solution, the Supplicant communicates with an Authenticator, which again is connected to the HLR/HSS (usually through a AAA/RADIUS-server [19]). When the AAA confirms that the user has been properly authenticated to the Authenticator, the Authenticator will provide the Supplicant with an authentication token that is set as a cookie in the Web-browser. Upon returning to the service provider site and presenting this token to the service provider, a new authenticated session and security association is immediately established between the client and the service provider.

The Web-server of the service provider is also connected to the P/S-CSCF, and the user is thus able to control IMS services through his Web-browser.

The main advantage of this solution compared to GBA is that it requires less changes to the existing solutions both on the client and server side.

VI. SINGLE-SIGN-ON BETWEEN IMS CLIENT AND OTHER APPLICATION CLIENTS

The previous section shows how it is possible to make SIM authentication a more generic authentication mechanism, and how to use it for other types of services than it was designed for. To make the solution even more flexible, we now show how to put the authentication mechanism into a more general system, i.e., how to embed it into an identity management framework with the purpose of enabling Single-Sign-On (SSO), across both service instances as well as across service types.

For most of the users, authentication is a cumbersome and time-consuming task that one would prefer to be exempted for. The re-authentication for each application should hence be avoided as much as possible and Single-Sign-On mechanisms should be introduced.

Figure 6 shows the current authentication architecture being designed and implemented as part of the European Eureka-project Mobicome. The authentication architecture for Mobicome consists of the following components:

- **IMS client**: This is a client supporting the standard IMS protocols, but which is adapted to fit with the Mobicome-architecture and its particular functionality.
- **IMS Core Components**: These are standard IMS components, except the S-CSCF which has been extended with a connection to the identity provider to allow SSO.
- **SIP client**: This is an ordinary SIP client, adapted to communicate with the Supplicant.
- **Web client** – This is an ordinary Web-browser, which can either incorporate a Supplicant, or be able to communicate with a standalone Supplicant.
• **Supplicant**: This component is responsible for performing the actual authentication on behalf of the various clients. To perform authentication of the user, it communicates with the SIM card, as well as with the identity provider.

• **AAA** – This is a standard RADIUS-server, with extensions for EAP-SIM [20] and EAP-AKA [21].

• **HSS & HLR** – These are standard GSM/UMTS components.

• **SIP Registrar** – This is a standard SIP server, extended with a connection to the identity provider.

• **Service Provider on the WWW**: This will typically be a service provider with a Web 2.0 service, where integration of IMS type of services is desirable. The Mobicome-project has designed and developed a Family Portal where family members can easily initiate, terminate and transfer phone calls through a Web 2.0 interface, both from an ordinary PC as well as from a mobile phone [23].

• **IdP**: This is an identity provider supporting e.g. the Liberty Alliance [22] standards. However, through the Mobicome-project [23] we are studying the integration of other emerging identity management frameworks and protocols like e.g. OpenID [24] and CardSpace [25] from Microsoft.

In the current solution, the IdP is an OpenSSO [26] server that has been extended with an authentication plug-in by subclassing the AMLoginModule. The Supplicant communicates with this using EAP-SIM, and the plug-in communicates with the AAA using EAP-SIM, so it acts like a proxy. However, it is integrated with the IdP, so that upon successful authentication, it notifies the IdP and retrieves a valid Single-Sign-On token (SSOToken) for the current user. This is forwarded to the Supplicant. See Figure 7 for a more detailed illustration of the architecture.

As shown in Figure 7, the architecture also supports the use of SMS authentication, which can be useful for many types of services accessed through the mobile phone. It is possible to either run the complete EAP-SIM protocol on top of SMS, or to use a more simple procedure e.g. based on user acceptance. For the IMS part, the Identity Provider (IdP) is introduced between the S-CSCF and the HSS, in order to capture the authentication status of the user, and thus generate, store and supply SSO-tokens upon successful authentication. The IdP will check if an SSO-token exists for the user in question, and use this for authentication if it exists. If it does not exist, it will contact the HSS and perform the standard authentication procedure.

The SSO token is used as a short-term key, and the same authentication algorithm can be used as with standard authentication, i.e., the IMS AKA for the IMS client and HTTP Digest authentication for the SIP client. Another option is to use as key the Kc established through the A3/8 algorithm instead. This improves security, since the key never passes across any network. However, this option requires additional changes to the AAA, which is not equipped to expose this key through the current protocols.

**VII. FUTURE WORKS**

The current Mobicome authentication architecture covers the SSO between services running on several different platforms (Web, IMS and SIP). An extension to this work, which will also be considered in Mobicome, is the study of challenges and solutions to SSO in the vertical direction, i.e., the reuse of identities and credentials from access level authentication in middleware and application level authentication.

Many IMS services will also have strict QoS requirements (e.g. voice services), and these will pose requirements on the authentication process (authentication delay), in particular in the handover procedure between different access technologies. These challenges will also be studied in the continuance of Mobicome.

**VIII. CONCLUSION**

In this paper it is shown that the extension of IMS to a fixed-mobile convergent environment requires new solutions for authentication and identity management. Some of the limitations of current standardisation work are discussed, and possible solutions to these challenges are proposed and described. The paper proposes solutions for authentication of stationary devices, for authentication of other applications than the IMS client and for Single-Sign-On by utilising an identity management framework.

The presented work is a result of the ongoing Eureka-project **Mobicome**, which is working with challenges related to multi-access IMS-services. The solutions presented in this paper will be further analysed, implemented and evaluated within the scope of the Mobicome project.
REFERENCES

[5] 3rd Generation Partnership Project: Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103 version 7.3.0 Release 7
[7] 3GPP/ETSI, Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) (3GPP TS 03.40 version 7.5.0 Release 1998)
[8] TISPAN, online: http://www.etsi.org/tispan/
[9] 3GPP/ETSI, Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203 version 7.8.0 Release 7)
[10] 3GPP, Security considerations regarding IMS access with SIM authentication, T-Mobile, 2002
[12] Early IMS 3GPP TSG SA WG3 Security
[14] Bluetooth Special Interest Group (2005), SIM Access Profile (SAP)
[17] 3rd Generation Partnership Project: 3GPP TR 33.920 V7.4.0 (2008-01) Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); SIM card based Generic Bootstrapping Architecture (GBA); Early implementation feature (3GPP TR 33.920 version 7.4.0 Release 7)
[18] StrongSIM, online: http://www.simstrong.org/
[22] Liberty Alliance, online: http://www.projectliberty.org/
[23] The Mobicome Project, online: http://www.mobicome.org
[24] OpenID, online: http://openid.net/
[26] OpenSSO, online: https://opensso.dev.java.net/