Strong authentication for Web services with Mobile Universal identity

Do van Thanh – Telenor & Norwegian University of Science & Technology

Snarøyveien 30 1331 Fornebu, Norway
Thanh-van.do@telenor.com

Ivar Jørstad – New Generation Communication

Rådhusgaten 9 Oslo, 0151 Norway
ivar.jorstad@newgencom.com

Do van Thuan – Linus

Martin Linges vei 15, 1364 Fornebu, Norway
t.do@linus.no

Abstract. To access services on the Web, users need quite often to have accounts, i.e. user names and passwords. This becomes a problem when the number of accounts keeps increasing at the same time password is a very weak form of authentication exposing the users to fraud and abuses. To address both mentioned issues we propose a Mobile Universal identity, which by combining Internet identifiers with mobile identifiers is capable of delivering strong authentication for Internet services. By introducing an identity provider, the solution enables the user to employ the Mobile Universal identity for multiple service providers. By federation with other identities, Mobile Universal identity can be used with service providers worldwide.

Keywords: Identity management; strong authentication; identity federation; mobile identity; mobile ID

1 Introduction

In the current digital age the Internet or more precisely the World Wide Web, is playing a central role in most individual's life. The preponderant position is probably due the immense number of fancy and diverse services that everyone can access and enjoy. However, in order to get granted access to services users are quite often required to create an account with an identity, i.e. to define a user name and a password at the service provider. As the number of identities, i.e. user names and passwords is increasing it is more and more challenging for users to remember them. Most critical is

the weakness of passwords as authentication scheme. Indeed, passwords are exposed to cracking, sniffing, phishing, spoofing, etc. which can lead to identity theft and other serious economic consequences both for the user and the service provider. Stronger authentication is urgently required.

Contrastingly, in the mobile network, mobile users enjoy of the great protection all over the world thanks to by the SIM (Subscriber Identity Module), a tamper resistant device which hosts the International Mobile Subscriber Identity (IMSI) and is equipped with advanced cryptographic functions, is capable of carrying strong authentication towards the mobile network. In this paper we propose a new user identity, called Mobile Universal identity, which combines mobile identity and Internet identity to provide a strong and uniform authentication for access of both mobile and Internet services. The paper starts with a brief review of related works. Next is the investigation of identities and authentication in the Internet. The strong authentication used in the mobile network is examined thoroughly. The main part of the paper is the description of the proposed Mobile Universal identity.

2 Related works

There were previously proposed some solutions which make use of the SIM card to provide stronger authentication to Internet applications and services. The 3GPP GBA (Generic Bootstrapping Architecture) [1] authentication enables the usage of the USIM/ISIM (IMS SIM) authentication for other Internet application clients than the IMS client such as email client, IM client, presence client, etc. Basically, the GBA provides a mechanism for establishing a short-term authentication key between a client on the user equipment and a service provider. Unfortunately GBA only applies to USIM/ISIM and not the regular SIM. The second and probably the most serious limitation lies on the fact that GBA requires the presence of the GBA client on the mobile phone, which is quite difficult because handset manufacturers do not have incentive to implement it. To remedy the situation the Eureka Mobicome project proposed a few solutions called SIM strong authentication that provides strong authentication from a regular browser on a regular mobile phone carrying a regular GSM SIM [2][3]. Unfortunately, as their names suggest, the described solutions are focusing only on providing stronger authentications and do not constitute a complete identity system offering strong and user-friendly authentication to the users.

3 Identities and authentication on the Internet

In the Internet or more correctly the World Wide Web users can access a lot of information but to receive really useful and validated documents and services they usually need to have an account at the service provider. Such an account is tied to an identity, characterized by a user name and a password locally defined at the service provider Web site. As the number of identities increases the burden to remember the passwords is getting heavier for users. To address this problem Identity Providers (IDP) such as

Facebook connect [4], Google ID [5], Twitter [6], etc. start to emerge and offer the usage of their identities at other Web sites. This makes it easier for both the users and Web sites. Unfortunately there still is a big problem. Passwords are still too weak authentication and the risk to be abused is still there.

To improve security some players like Google, Apple, etc. introduced two step authentication or more precisely two factor authentication in which the first factor password i.e. something you know is complemented with a second factor, the mobile phone, i.e. something you have. Upon sign on the user receives a one-time code in an SMS (Short Message Service) that he/she has to type in. This authentication, although stronger, could be challenging when the user is accessing through his mobile phone with smaller screen and keyboard. Lately, there are emerging software security tokens i.e. software application capable of carrying out strong authentication functions e.g. RSA SecurID Software authenticator [7] which can be downloaded to smartphone and provide a two factor authentication. Unfortunately, these software tokens as any software application are subject to duplication and one can only be sure that the claimant does have the token but not that he/she is the only one.

4 Mobile identity and strong authentication in the mobile network

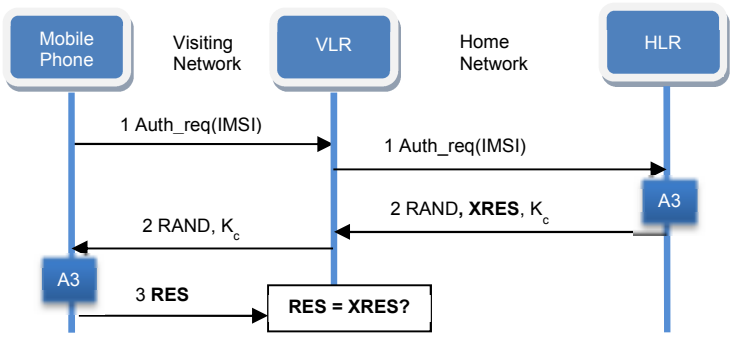

Fig. 1. GSM authentication

When subscribing to mobile services, i.e. voice and Short Message Service (SMS) the user receives a mobile identity consisting of two identifiers. The phone number, also called MSISDN (Mobile Subscriber Integrated Services Digital Network-Number) is a public identifier is used by the user to make and receive phone calls. The other one, IMSI (International Mobile Subscriber Identity) is a private identifier standardised to be recognized by every network in the world and used in the authentication of the subscriber. The IMSI is not confidential but should not be diffused too much because it reveals the identity of the subscriber and may pose privacy problem. The responsi-

bility of authenticating the subscriber is assigned to a software application called SIM (Subscriber Identity Module) [8]. For protection, the SIM application together with the IMSI, credentials such as secret key Ki, personal identification number (PIN) for ordinary use, personal unblocking code (PUK) for PIN unlocking and cryptographic functions securely stored in a tamper-resistant integrated circuit called UICC (Universal Integrated Circuit Card), which is actually the physical module, commonly known as SIM card.

The SIM application combined with the UICC can provide strong two factor authentication with the PIN code as "something you know" factor and the UICC as "something you have" factor. As shown in **Fig. 1** the strength of the GSM authentication is ensured by the use of a challenge-response mechanism. Upon power on the handset sends an authentication request with its IMSI to the Visitor Location Register (VLR) which forwards it to the Home Location Register. The Home Location Register (HLR) computes the 32-bit signed response (SRES) based on the encryption of a 128 bit random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki) and send the triplet to the VLR. The VLR passes the random number RAND and the ciphering key Kc to the mobile phone which delivers them the SIM. The SIM computes the result RES using RAND and Ki, and submits it to the VLR. If RES = XRES the mobile phone is authenticated and Kc is used for the encryption of the air channel.

Although rather sophisticated at its invention time the GSM authentication scheme does not provide authentication of the mobile network by the mobile phone and exposes the mobile phone for man-in-the-middle attack by rogue base stations. To address this weakness, UMTS employs a mutual authentication allowing also the authentication of the 3G network by the handset. As shown in **Fig. 2** , the additional parameter AUTN enables the verification of the authenticity of the mobile network and also the expiration of the response.

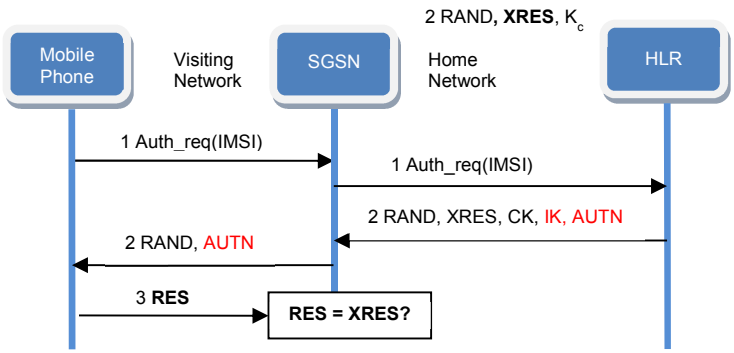

Fig. 2. UMTS authentication

5 From Mobile identity to Mobile Universal identity

5.1 Definition

The current Mobile identity as standardised with two identifiers: MSIDN and IMSI cannot be used in the Internet and has to be supplemented with one or more Internet identifiers. It could be a user name or a uniform resource identifier (URI) such an email, e.g.user@telenor.com that can be used for the authentication and authorisation of Internet services offered both by the mobile operator and third party service providers. Another major limitation of the Mobile identity lies in the fact that it is a subscriber identity and not really a user identity. There are many cases where the subscriber is not the user as follows:

- One subscriber may have multiple subscriptions distributed to multiple users: Typical example is a company or head of family that pays for a series of subscriptions which are distributed for use by employees or family members.
- One user can have multiple subscriptions and appear like multiple subscribers: This is the case of a user having multiple subscriptions for multiple devices: mobile phone, tablet, laptop, home alarm systems, etc.

We propose to introduce a Mobile Universal identity which is uniquely assigned to a user as a human being and lasts as long as the user likes. It must be sufficiently flexible to allow the inclusion, modification or removal of any mobile identifier or any Internet identifier that the user wants.

These identifiers can have different levels of assurance [9] from level 1 with full anonymity to level 4 with registration of user's name, address, nationality, picture and biometrics and the user is given the freedom to decide which identifier for each situation.

Since mobile identity, i.e. phone number and IMSI will be used in the authentication of the user and the user may have more than one it is necessary to have an enrolment process which registers the mobile identity for authentication. The user can run the enrolment process whenever he/she wants to change the phone number.

5.2 Mobile phone Enrolment process

The enrolment process although sufficiently secure is rather simple as follows:

1. The user signs on at the Mobile Universal identity provider (which could be the mobile operator) Web site using password
2. He/she enters the number of the mobile phone to be used in the authentication.
3. Mobile Universal identity provider verifies that the number is legitimate, i.e. in operation and not reported as lost or stolen.
4. If it is the case the mobile phone can be used and an SMS containing a one-time password is sent to the user's mobile phone.
5. By entering this one-time password at the Mobile Universal identity provider Web site the mobile phone is enrolled as authentication token.

5.3 User's requirements

To be really useful and accepted by the users the Mobile Universal identity must fulfil the following requirements:

1. The user must experience a seamless authentication, i.e. no sign-in required when accessing from his/her mobile phone Internet services that do not require high level of security, e.g. social networks, net shops, etc.
2. For Web sites federated with the Mobile Universal identity service provider the user must be able to use his/her Internet identifier for sign in.
3. For Web sites having their own account, i.e. own user identity the user must be able to use strong authentication provided by his/her mobile identity.
4. The user will be asked to enter pin or select yes when accessing from his/her mobile phone Internet services requiring higher level of security, e.g. governmental services, health services, net banks, etc.
5. The user will be asked to enter pin or select yes when accessing from another device than his/her mobile phone all Internet services.
6. The user must be able to use his/her identity at service providers worldwide.

5.4 Overall architecture

To realise the Mobile Universal identity fulfilling all the requirements mentioned in previous section, the mobile network has to be complemented with additional network element as shown in **Fig. 3**

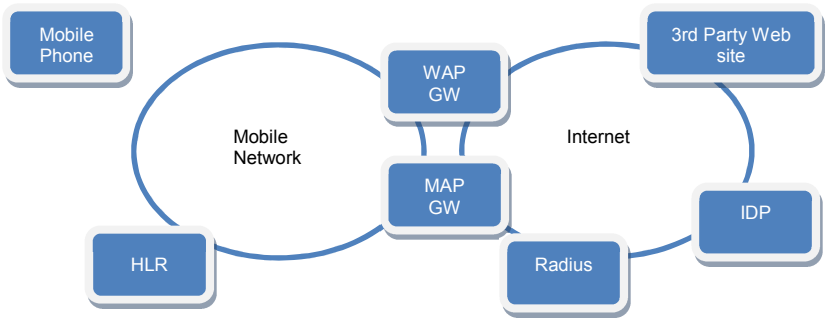

Fig. 3. The Mobile Universal identity overall architecture

- **Identity Provider (IDP):** is in charge of authentication and authorization for Internet services. In order to offer services to a wide range of 3rd party service providers the IDP supports several technologies and can act as a Liberty Alliance IDP [10], OpenID IDP [11], OAuth Authorization server [12]. It is communicating with

the Radius server to request SIM or AKA authentication. This IDP can federate with other IDP including the ones of other operators to enlarge the usage of the user's Internet

- **Radius server:** This is a standard server that supports the EAP-SIM [13] and EAP-AKA [14] protocols. It can be used in the authentication of IP devices such as PC, Laptop, tablets, etc.
- **MAP gateway:** has on one side IP interface and on other side an SS7 interface allowing it to communicates with the HLR using the MAP (Mobile Application Part) protocol [15]. In fact it is viewed by the HLR as a VLR that sends authentication requests.
- **WAP gateway**: When offering Internet access Most of operators do have a WAP (Wireless Application Protocol) [16] gateway that translates Web pages onto adequate formats for mobile phones. For our solution, modifications have to be done to make the WAP gateway intercepting all the http requests and redirect to the IDP.

5.5 Typical use cases

To clarify how the Mobile Universal identity is working let us now consider a few typical use cases.

Use case 1: Sign on from mobile phone

1. The user browses on his/her mobile phone and visits a 3rd party Web site
2. The WAP Gateway intercepts http request and insert the mobile ID (MSISDN) in the header
3. The operator's WAP gateway redirects browser to Mobile Universal IDP
4. The Mobile Universal IDP sends an authentication request containing mobile ID to the MAP Gateway
5. The MAP Gateway forwards the authentication request to the HLR
6. The HLR returns an authentication vector to the operator's MAP Gateway
7. The MAP Gateway forwards authentication vector to operator's IDP
8. The Mobile Universal IDP sends authentication request with challenge to the user's mobile phone
9. The user's mobile phone sends challenge to SIM card and gets back response
10. The user's mobile phone sends response to the Mobile Universal IDP
11. The Mobile Universal IDP checks the response. If correct the Mobile Universal IDP inserts a security assertion in the browser and redirects it back to the 3rd Party Web server.
12. The user gets granted access to 3rd Party Web site without having to type anything.

Use case 2: Sign on from PC.

1. The user browses on his/her PC and visits a 3rd party Web site. A sign in page is presented.
2. The user enters his/her username at 3rd Party Web site and clicks on sign on.

3. The browser on the user's PC is redirected to the Mobile Universal IDP
4. The Mobile Universal IDP translates username to mobile ID sends an authentication request containing mobile ID (MSISDN) to the MAP Gateway
5. The MAP Gateway forwards the authentication request to the HLR
6. The operator's HLR returns an authentication vector to the MAP Gateway
7. The MAP Gateway forwards authentication vector to the Mobile Universal IDP
8. The Mobile Universal IDP communicates with the Short Message Service Center (SMS-C) to send an SMS to the user's mobile phone. The headers of this SMS ensure that the SMS is terminated on the SIM-card on the user's mobile phone.
9. On the SIM-card, a SIM Toolkit Application is triggered and a pop up appears in the display of the user's mobile phone. It asks the user if he wants to proceed with the authentication.
10. If the user accepts, an SMS is returned to the Mobile Universal IDP,
11. The Mobile Universal IDP inserts a security assertion in the browser and redirects it back to the 3rd Party Web site.
12. The user gets granted access to the 3rd Party Web site.

5.6 Making the identity really universal

The Mobile Universal identity as described so far can only be used with service providers that trust the Identity Provider and are hence willing to use the Mobile Universal identity provided by this IDP. This is typically the case of local service providers in one country that build alliance with a national IDP. The IDP together with its service providers form a circle of trust in which the user can employ the same identity. Unfortunately, such a circle of trust has boundaries and there are certainly service providers that belong to other circles of trust. The user cannot use his/her Mobile Universal identity with these service providers.

To enable the usage of the Mobile Universal identity of one circle of trust in another one, federation of the two circles of trust has to be done as shown in **Fig. 4**. Federation is the exchange of metadata necessary for the mapping of one identity to the other.

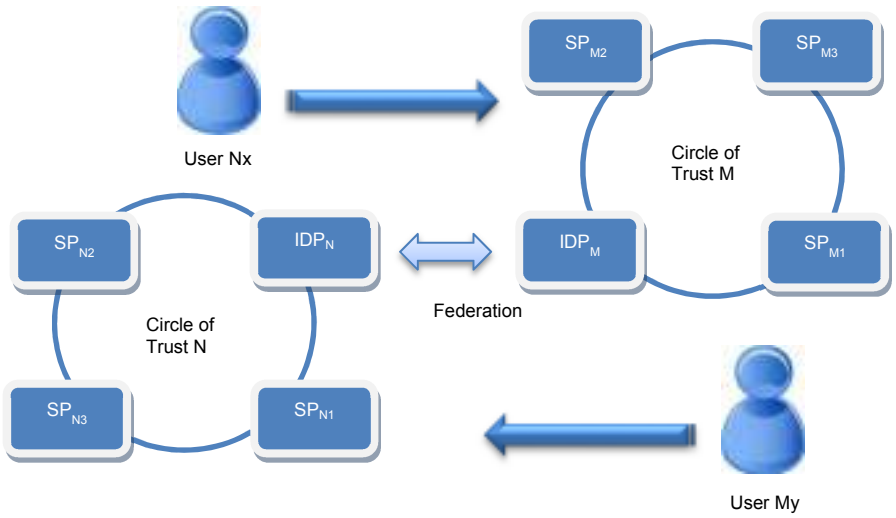

Fig. 4. Federation of identities

There are two federation methods and to explain them let us consider two circles of trust N and M with respectively IDP_N and IDP_M.

- **Federated identifier:** When user Nx of Circle of trust N visits a service provider SP_{M2} in Circle of trust M. IDP_M acts as a service provider in the Circle of trust N. For user Nx an account at IDP_N is created and federated both with SP_{M2} and IdP_N.
- **One Time identifier:** The visited SP_{M2} does not store any local account for the user. After being authenticated by the home IDP_N user Nx will be authorized by the SP_{M2} A new one-time identifier must be generated at access and the user can use her IDP_N identity.

For the travelling user accessing from mobile phone the sign-on is seamless as indicated previously in Use case 1. When the user is browsing from her laptop it is a little bit more challenging because the Internet identifier might not be recognizable for the visited SP. There are two solutions as follows:

- **Universal unambiguous Internet identifier:** IDP and SP have to agree on a common naming convention for identity that enables the identification of the home IDP.
- **User's assistance:** On the visited Web site there should be facility allowing users to indicate their origin.

6 Conclusion

In this paper, we propose an identity called Mobile Universal identity which can be used everywhere in the mobile networks and the Internet. The Mobile Universal identity is realised by including both mobile identifiers and Internet identifiers. Strong authentication is provided by using the mobile identity and the SIM. A proof-of-concept of the proposed solution has been implemented and tested to ensure feasibility. Some usability tests have been performed and the sign-on both mobile phones and PC are in the range of few seconds which is quite negligible for users. However, to really prove the usability of the Universal mobile identity it is necessary to carry field trials with real users. A federation trial between multiple circles of trust has also to be carried out for validation. Last but not least, to ensure the success and adoption by the market it is important to elaborate a sound business model such as for international roaming.

References

1. 3rd Generation Partnership Project: 3GPP TS 33.220 V8.2.0 (2007-12) Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA) Generic bootstrapping architecture (Release 8)
2. Do Van Thanh, Tore Jønvik, Do Van Thuan & Ivar Jørstad: Enhancing Internet service security using GSM SIM authentication, Proceedings of the IEEE Globecom 2006 conference – ISBN 1-4244-0357-X – San Francisco, USA, Nov 27 - Dec 1, 2006
3. Do van Thanh, Tore Jønvik, Boning Feng, Do van Thuan & Ivar Jørstad: Simple Strong Authentication for Internet Applications using mobile phones, Proceedings of IEEE Global Communications Conference (IEEE GLOBECOM 2008), ISBN 978-1-4244-2324-8, New Orleans, LA, USA, Nov 30 – Dec 4, 2008
4. Facebook Inc.: Facebook login; https://developers.facebook.com/docs/facebook-login/
5. Google: Google account; https://developers.google.com/+/features/sign-in
6. Twitter: https://twitter.com/
7. EMC^2 http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators.htm:
8. 3rd Generation Partnership Project: 3GPP TS 11.11 V6.0.0 (1998-04); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface (Release 97)
9. NIST: National Institute of Standards and Technology; Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline, April 2006
10. T. Wason, et al., “Liberty ID-FF Architecture Overview; Version: 1.2-errata-v1.0”, Liberty Alliance Project, 2005.
11. OpenId: http://openid.net/
12. oAuth: http://oauth.net/
13. The Internet Engineering Task Force: Network Working Group, H. Haverinen, J. Salowey, “EAP-SIM Authentication”, RFC 4186, IETF, January 2006.
14. The Internet Engineering Task Force: Network Working Group, RFC 4187 Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
15. ETSI TS 100 974 V7.15.0 (2004-03). Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification - (3GPP TS 09.02 version 7.15.0 Release 1998
16. Open Mobile Alliance (OMA): Wireless Application Protocol Architecture Specification - WAP Architecture Version 30-Apr-1998