Mobile Provided Identity Authentication on the Web

Jonas Högberg
jonas.k.o.hogberg@ericsson.com
User Management Evolution & Customer Engagement Unit, Madrid R&D Centre
Ericsson

Position Paper for W3C Work-shop on Identity in the Browser

Introduction

One of the key elements to improve the user experience on the Web is the enhancement of the user security, however not compromising the usability of the solutions. In that sense, the take-off of the mobile Internet, with users always carrying (in a way that was only equaled previously by keys, watches or wallets) a personal device, i.e., the mobile phone, equipped with a Subscriber Identity Module (SIM) card leads to a natural consequence: it is possible to take advantage of the two-factor authentication mechanisms supported by the SIM card, for example, using the mechanisms of the Generic Authentication Architecture/Generic Bootstrapping Architecture (GAA/GBA).

An interesting development is that with new mobile technologies, such as 3rd Generation mobile telecommunications (3G) or Long Term Evolution (LTE), SIM cards are propagating to laptops. Therefore, the number of SIM-equipped devices the users own increases, thus opening the way to implementing security functionalities based on such kind of authentication techniques. Some of them also allow key distribution. Additionally, user location can be used as an extra authentication factor when considering user security technologies based on the SIM card.

Ericsson sees a positive industry trend and therefore participates in the development of so-called federated identity systems, particularly in Kantara Initiative. Some technologies being used in federated identity systems are Open Identity (OpenID), Open Authorisation (OAuth) and Data Portability in the social area, Security Assertions Markup Language (SAML) and Liberty Alliance Identity Web Services Framework (LAP ID-WSF) in the enterprise area, Global System for Mobile Communications (GSM) Association (GSMA) One Application Programming Interface (API) (GSMA OneAPI) in the Telco area. However, both OpenID and OAuth are now entering the Telco area as well.

Some areas of interest for Telcos are:

- SIM-based authentication regardless of the network operator/carrier giving service to the user. For instance, GAA/GBA and Short Message Service (SMS)-based One-Time Password (OTP). Such authentication mechanisms should be available to any site by means of different protocols such as OpenID, SAML and so on.
- Other strong authentication mechanisms not under the control of network operators. For instance Wireless Public Key Infrastructure (WPKI) and electronic (smart card-based) identity documents.
- User location regardless of the network operator giving service to the user. User location should be also available as an enhancement of user authentication (thus allowing that authentication is only valid if the user being authenticated is in a given location or nearby). The emerging GSMA Access API could be used in the relationship with network operators.

One way of enhancing the user security, however not compromising the usability of the solutions nor deteriorating the user experience, is to use a strong authentication on the web. GBA is good example of this.

Why GBA?

Juniper research [Juniper] predicts that 1.7 billion users will access Internet from their mobile phone (half of the total Internet users) by 2013. Potentially, they could use GBA.

Also, by showing some other available options and their weaknesses compared to GBA, the advantages of GBA can be shown:

- Traditional username/password: it is often weak, hard to remember and being re-used across different web sites.
- Client certificate (and associated private key) stored on the device: it is possible to extract the key from a compromised client (no hardware protection) and there is no easy way of distributing the certificates; and
- Hard tokens: they are hard to distribute and require extra hardware.
- GBA: it is considered strong authentication and the User eXperience (UX) is good.

Use Case[1]

The following use-case illustrates how the authentication done within the operator domain can be seamlessly exposed to a Web application provided by an external party on the Internet. This enables the provision of a consistent and efficient user experience, wherever the resource is stored and independent of the current type of network connection.

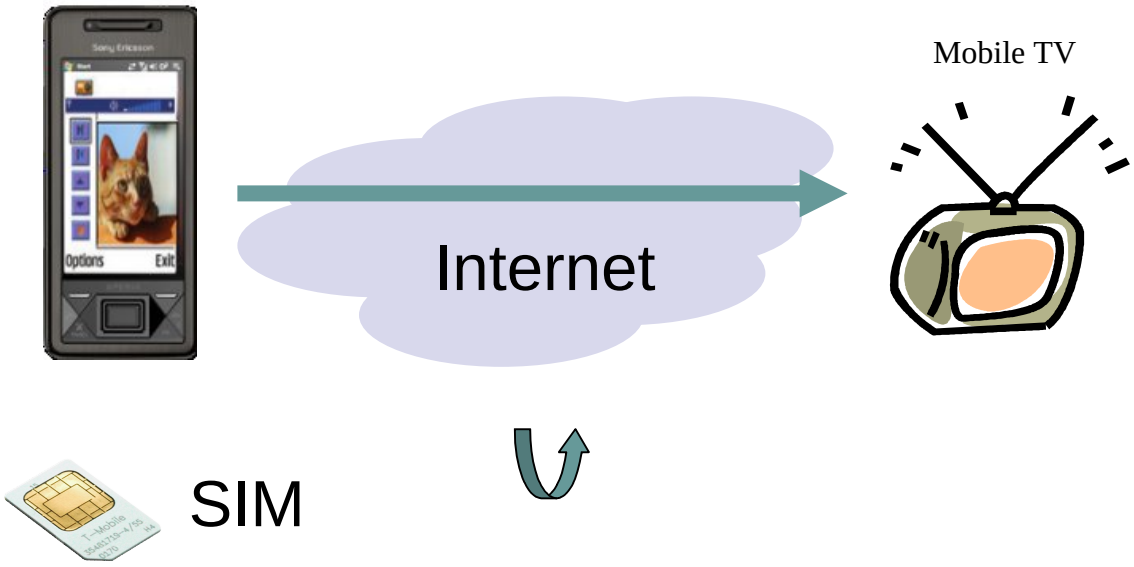

Figure 1: Mobile TV use-case illustrating Single Sign-On from a Telco to the Web.

1. A User has authenticated with his/her operator/carrier. The access could be GSM/3G/LTE or Wi-Fi.
2. At some point in time, the User decides to watch some Mobile TV.

[1] This use case is influenced by work done in the Telco Work Group in Liberty/Kantara. Please refer to: http://projectliberty.org/liberty/content/download/4315/28869/file/WP-BridgingIMS_AndInternetIdentity_V1.0.pdf.

3. The User is seamlessly authenticated to his Mobile TV service (not provided by the Telco operator/carrier) due to the re-use of the already existing network authentication (GSM, 3G or LTE). The user gets access to the service in a convenient way.
4. The User watches, e.g., a program about cats.

The key benefits of this use-case are:

- Both users are provided with a consistent user experience without entering any credentials.
- Users are able to seamlessly utilize resources that are outside of the operator's domain (Mobile TV) but also outside of the operator's domain (independent third-party service provider).
- The operator/carrier does not have to disclose the users real IDs to third-party. Instead, they provide their strong SIM authentication service towards originally much weaker security.

Solution on Authentication from a Telco to the Web

OpenID is becoming one of the frameworks (FWs) of choice for Identity Management (IdM) and Single Sign-On (SSO) for Web-based services. The combination of OpenID with the GBA enables the leveraging of SIM-based, accepted, strong and mutual authentication to the Web. However, there are other IdM FWs as well. The Security Assertions Markup Language (SAML) (from Organization for the Advancement of Structured Information Standards (OASIS) and International Telecommunication Union Telecommunication Standardization Sector (ITU-T)) being one of them. Conceptually, SAML can be exchanged for OpenID in the use case and its following discussion.

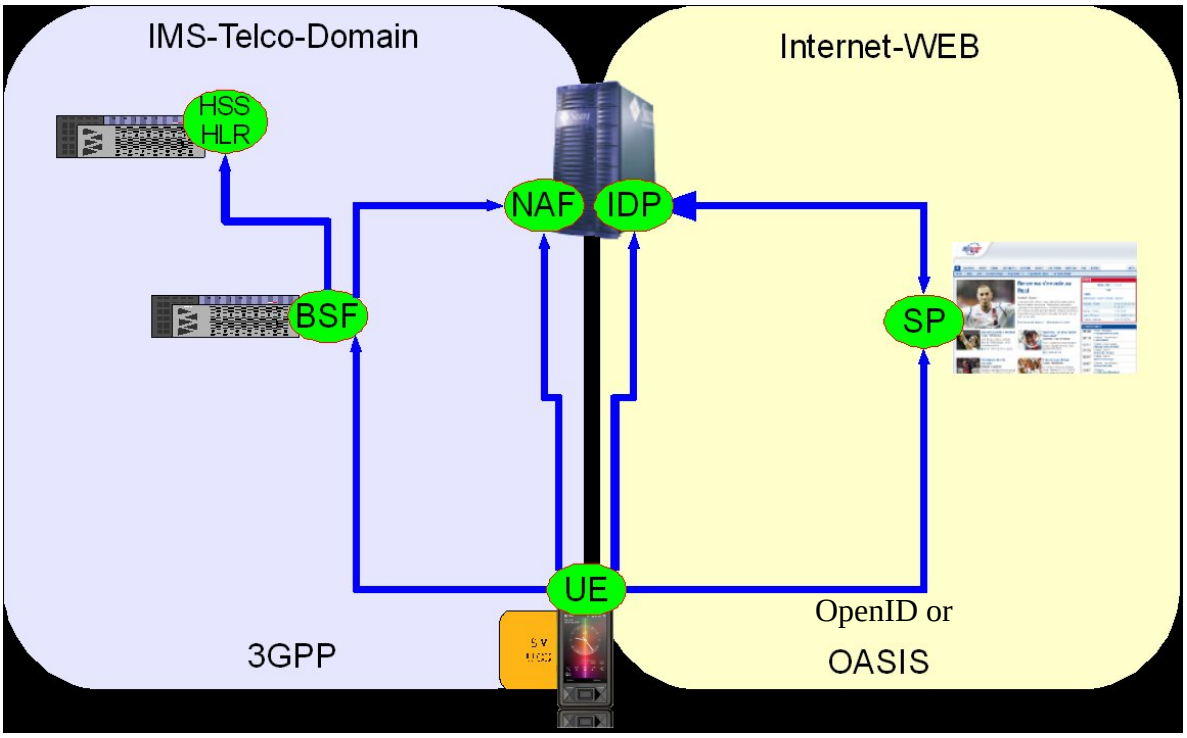

Figure 2: Exposure/Re-use of Telco Authentication to Third-parties on the Internet

Overview 3GPP GBA

The Network Application Function (NAF) constitutes the HTTP or HTTPS-based service that requires (3GPP) authentication. The Bootstrapping Service Function (BSF) is the authenticator against which the User Equipment (UE) has to do (3GPP) authentication. The BSF enables the NAF to verify whether a UE was correctly authenticated against the authentication vector located in the Home Subscriber Server (HSS) or Home Location Register (HLR).

Here, the bootstrapping procedure in combination with the HTTP Digest authentication option is briefly described. Our setup co-locates the IdP and NAF. Please note that other options are possible, especially the co-location of the IdP and the BSF. For clarity, this example describes the solution in the user's home network. Nevertheless, IdP discovery or GBA roaming could be leveraged to address more complex scenarios. For more details see the Technical Specification of GBA and Inter-working of GBA and OpenID [3GPP TR 33.220, 3GPP TR 33.924].

OpenID Part 1

The UE contacts the SP to gain access to a service. This request contains the GBA-based authentication support indication ("User Agent: 3ggb-gba").
The UE's request is redirected to the IdP. If the UE is not yet authenticated with the IdP, the IdP then switches its function. As a NAF it sends an HTTP response with a "401 Unauthorized" status code to the UE.

AKA Part

The UE recognizes from the HTTP 401 response that it is requested to supply NAF-specific keys. Since it has not yet authenticated against the BSF it initiates the so called Authentication and Key Agreement (AKA) procedure by sending a request to the BSF.

The BSF fetches a set of authentication information from the HSS and sends back a derived user Message-Digest algorithm 5 (MD5) challenge. The UE checks the challenge and calculates the corresponding response and sends it to the BSF. The BSF compares the response with the expected values and, if everything is fine, sends some parameters to the UE.

OpenID Part 2

The UE answers with a HTTP GET request. The IdP responds and the UE contacts the SP again. The SP sends a request to the IdP and the IdP replies with an assertion. The SP verifies the assertion and answers with the requested content.

Sharing the Authentication Context

In the above solution, a coupling of the GBA client and the Web client is assumed. This is where the link to 'Identity in the Browser' becomes clear.

Browser Vendors

The GBA client could be loosely coupled to the browser. By having different authentication modules in the browser that can easily be added and removed, e.g., traditional username/password, windows authentication, certificate store, hard-token, GBA module etc. we can allow for a number of different authentication schemes. W3C could decide on the common characteristics of the modules.

Life Cycle of the Identity and Relation with the SIM Card

Following the SIM-based authentication phase, the authentication session is usually maintained between the IdP and the Web browser relying on the HTTP cookie mechanism. In such case, from a Telco perspective, the authentication session (as well as credentials derived from the initial SIM-based authentication) should however be valid only if the SIM card used for the authentication is still present in the device. This requirement is related to security reasons as in the Telco world, the change of the SIM on a device is usually considered as a change of identity on that device.

Things to Think About

OpenID is not perfect; some issues are interoperability and User UX. The OpenID Foundation (OIPF) and Kantara are working on both issues.

Developers

At Ericsson Labs [Labs] developers can find an IdM FW for download.

Conclusions

It has been shown that a strong, Telco-backed authentication can help enhancing the user security, however not compromising the usability of the solutions nor deteriorating the user experience. Inter-working between OpenID and GBA is **one** model for this. Some browser implications have been high-lighted. Finally, things to think about for the future have also been mentioned.

References

[Labs] https://labs.ericsson.com/developer-community/blog/identity-management-framework-now-available-download

[3GPP TR 33.220] http://www.3gpp.org/ftp/specs/html-info/33220.htm

[3GPP TR 33.924] http://www.3gpp.org/ftp/specs/html-info/33924.htm

[Juniper] http://juniperresearch.com/reports.php?id=119