Liberty ID-WSF Advanced Client Implementation and Deployment guidelines for SIM/UICC Card environment

Version 1.0

Editors:
Gaël Gourmelen, OrangeLabs.
Laurent Coureau, France Telecom.

Contributors:
Gil Bernabeu, Global Platform
Conor P. Cahill, Intel
Peter Davis, NeuStar
George Fletcher, AOL

Abstract:
This document defines some recommended implementation and deployment guidelines for implementors of a Liberty Advanced Client Trusted Module targeted for the SIM/UICC card environment.

Filename:
liberty-guide-adv-client-SIM-v1.0.pdf
Notice

This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS," and no participant in the Liberty Alliance makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review the Liberty Alliance Project's website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.

## Contents

1. Introduction .......................................................................................................................... 5
2. Guidelines for the provisioning and instantiation of a Trusted Module in the SIM/UICC card ....... 7
3. Guidelines for the acquisition of delegation rights from Mobile Network Operator's IDP Service ... 10
4. Guidelines related to the invocation of a Trusted Module hosted in the SIM/UICC card ......... 15
5. Security Considerations ......................................................................................................... 16
6. References .............................................................................................................................. 18
1. Introduction

The Liberty Alliance has defined some specifications that introduce new actors/entities (referenced by the generic term of "Advanced Clients") that can be instantiated in users' devices (without restrictions on the type of devices).

One of these entities, instantiated in users' devices, is the "Trusted Module" (TM) which can be seen as an extension of the "Network" Identity Provider (IDP).

![Figure 1. Actors referenced in Advanced Client specifications](source: Liberty ID-WSF Advanced Client Technologies Overview [1])

As described above, the TM, once instantiated in a trusted environment on user's device, is involved in interactions with local applications and service providers (via the browser) that delegate the authentication of the user to the TM (and no more directly to the "Network" IDP).

The main benefits of this model are the following:

1. It enables off line scenarios (cases where the network connection with the "Network IDP" is no more available).
2. Once the authentication has been performed and associated delegation rights obtained from the "Network IDP" through one access network, authentication assertions can easily be delivered to Service Providers (SPs) even if a different access network – Wifi, Bluetooth, … - is used to contact these SPs.
3. It limits interactions with the "Network IDP" (especially relevant when using local personal applications, verifying rights attached to local contents, …).
4. It can also improve some privacy aspects (as some interactions with SPs might not be known by the network IDP and thus not centralized any more).

1 The notion of trust is here related to the hosting environment.
For Mobile Network Operators, one obvious "trusted environment" is the SIM/UICC card. As this environment has some specificities and constraints, it appears that some guidelines for the implementation and deployment of a Liberty Trusted Module in that context would be relevant.

The aim of this document is thus to propose such guidelines for the implementation and the deployment of a "Trusted Module" in the SIM/UICC card (considered in this context as the trusted environment).

The main phases from the provisioning of a Liberty Trusted Module in the SIM/UICC card to its use are covered in the following chapters of this document:

1. The provisioning, instantiation and further life-cycle management of a "Trusted Module" in the SIM/UICC card.
2. The acquisition of delegation rights (SSO credentials) that will enable the “Trusted Module” to act as an extension of the Mobile Network Operator's IDP.
3. The Invocation of the "Trusted Module" to facilitate Single Sign On operations.

As a prerequisite, it is assumed that the reader is familiar with the Liberty ID-WSF Advanced Client concepts presented in the “Liberty ID-WSF Advanced Client Technologies Overview” document (see [1]).

Moreover, this document provides some recommendations referencing existing specifications from Liberty Alliance, Global Platform, 3GPP, ETSI, etc. It is not the aim of this paper to substitute for these specifications. The implementors should refer to these referenced specifications for more details.
2. Guidelines for the provisioning and instantiation of a Trusted Module in the SIM/UICC card

The Liberty Advanced Client specifications define a set of specifications (see [2], [3]) to handle the provisioning of a TM and its full life-cycle management in a generic way (whatever type of device or environment is targeted).

Figure 2. Liberty Advanced Client provisioning components

Source: Liberty ID-WSF Advanced Client Technologies Overview [1]

However, in the context of the Mobile Network Operator, optimized and existing provisioning mechanisms can be used. Indeed, TM provisioning in the SIM/UICC card can be resolved thanks to Over The Air (OTA) mechanisms as defined in GlobalPlatform Card specification (GlobalPlatform Card Specification v 2.1 – [5]) and adopted by ETSI (ETSI TS 102.225 and TS 102.226) and 3GPP (3GPP 31.115 and 31.116).

OTA provisioning permits a secure download of the application (i.e. the TM in our case) inside the SIM/UICC card.
Generic entities involved in OTA transactions are described in the figure above. The transport layer can be ensured by various technologies such as SMS, CAT/TP over BIP, BIP over TCP/IP or HTTP. For the purpose of comparison, the following table provides a mapping between functions exposed by a Liberty PMM (for use by a Provisioning Service) and functions provided by the OTA infrastructure to provision and remotely manage a card application - also named cardlet - in the SIM/UICC card.

<table>
<thead>
<tr>
<th>Liberty Advanced Client operations through PMM (Provisioned Module Manager)</th>
<th>Operations defined in Global Platform Card specifications (v2.1) and adopted by ETSI (TS 102.225 and 102.226) and 3GPP (31.115 and 31.116)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Provision”</td>
<td>“LOAD” + “INSTALL”</td>
</tr>
<tr>
<td>“PMDelete”</td>
<td>“DELETE”</td>
</tr>
<tr>
<td>“PMActivate”</td>
<td>“SET STATUS”</td>
</tr>
<tr>
<td>“PMDeactivate”</td>
<td>“SET STATUS”</td>
</tr>
<tr>
<td>“PMUpdate”</td>
<td>“DELETE” + “LOAD” + “INSTALL”² (to update the TM engine)</td>
</tr>
<tr>
<td>“PMGetStatus”</td>
<td>“STORE DATA” (to update the data managed by the TM)</td>
</tr>
</tbody>
</table>

² This sequence of operations will update the TM engine (i.e.: executed code of the cardlet application) but the data managed by the updated TM will be lost (whereas the Liberty “PMUpdate” operation allows the update of either or both TM engine and data; even distinguishing init and real-time types of data). If the lost of the managed data on TM-side at the end of the engine update process is an issue, two workarounds can be envisioned:

- "GET DATA" + "DELETE" + "LOAD" + "INSTALL" + "STORE DATA" sequence of operations,
- or design of TM core engine and TM data access as two different applications (so that the update of the TM Core engine application has no impact on data managed by the TM data access application).
Based on these mechanisms, the TM would thus be installed as a cardlet application.

In order to be accessible through HTTP and HTTP-S requests by other applications, this cardlet application MUST be exposed through a Smart Card Web Server as defined in OMA specifications (OMA-TS-Smartcard_Web_Server-V1_0-20080421-A).

To manage life cycle of applications, GlobalPlatform introduces the concept of Security Domains which are the on-card representatives of the application provider and verification authority. In our context, the TM cardlet MUST be installed in the same Security Domain than the one which includes the Smart Card Web Server application. As the Smart Card Web Server is managed in a particular Security Domain, called Issuer Security Domain, which is the Security Domain managed by the card issuer (i.e. the MNO in the mobile context), the TM cardlet MUST be installed in the Issuer Security Domain (ISD) as well.
3. Guidelines for the acquisition of delegation rights from Mobile Network Operator's IDP Service

Once provisioned, to be able to act as an extension of a “Network” IDP and facilitate SSO operations with relying parties, the TM needs to interact with the IDP Service (as defined in the "Advanced Client Liberty IDP Service Specification" [4]) to:

- obtain “SSO credentials” from that IDP,
- identify the relying parties with which that IDP has a relationship (i.e. provider information so that the TM can select the providers with which it will interact),
- report the creation of federations to the IDP.

In the context of a Mobile Network Operator, the TM MUST rely on GBA (Generic Bootstrapping Architecture) security mechanisms to interact with the Mobile Network Operator's infrastructure services in order to obtain the required SSO credentials on behalf of the implicitly authenticated mobile user.

Two GBA-based security profiles are detailed in this chapter. They are both adaptations of the Liberty / GBA interworking as described in [9]. They both provide the following features:

1. mutual authentication between the SIM/UICC-based TM acting on behalf of the mobile subscriber and the ID-WSF AS or IDPS (hosted by the Mobile Network Operator) reusing the existing security relationship between the Mobile Network Operator and the SIM/USIM of the user,
2. implicit identification/authentication of the user (the mobile subscriber who is the owner of the SIM/UICC card) on behalf of whom the TM will obtain delegation rights.

Note: the examples below only present the "GetAssertion" case but it can be indifferently applied to "GetAssertion"/"GetProviderInfo"/"CreatedStatus" IDPS operations.

GBA overview:

GBA is a method for using the existing security relationship between the Mobile Network Operator and the SIM/USIM of the user, which is primarily for establishment of security on the 3GPP or GSM bearer layer, for Application layer purposes. It is specified in 3GPP TS 33.220 – ‘Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (Release 7)’ [7].

With reference to Figure 4 below:
- Authentication vectors for the user’s SIM/USIM are stored in the Home Subscriber Server (HSS, the IMS equivalent of the HLR)
- The Bootstrapping Server Function (BSF) is an Operator-owned server that acts as the interface between the HSS and other entities for purposes of GBA.
- The Network Application Function (NAF) is a server owned by an Operator or 3rd party that wishes to conduct secure Application layer communications with the user.
The main steps within GBA are:
- The Bootstrapping Server Function (BSF) and the UE SHALL mutually authenticate reusing the existing security relationship between the Mobile Network Operator and the SIM/USIM of the user. A secret key is generated on BSF and SIM/USIM side.
- The BSF and the SIM/USIM derive this secret key to obtain a session key which is shared by the BSF to the Network Application Function (NAF).
- After the bootstrapping, the UE and NAF can run some application-specific protocol where the authentication / encryption of messages will be based on those specific session keys (possibly relying on HTTP-Digest over TLS or TLS-PSK mechanisms to provide mutual authentication and encryption as specified in [8]).

Two variations of GBA have been defined: GBA_U (GBA with UICC-based enhancements) and GBA_ME (Mobile Equipment-based GBA). GBA_U provides enhanced security with GBA keys that do not leave the SIM/UICC card environment.

To be consistent with other security considerations (SIM/UICC card considered as the trusted environment), the **GBA_U** (GBA with UICC-based enhancements) mode MUST be the only mode considered in the context of this document.

"**GBA_PSK/TLS-based security profile**": The TM invokes the Liberty ID-WSF IDP Service (IDPS) through HTTPS / PSK TLS. IDPS and GBA NAF functions are collocated to benefit from GBA authentication mechanism.
1. If the no valid bootstrapping session or the freshness of the key material is not sufficient for the IDPS/NAF, then a new bootstrapping procedure will executed with the BSF.

2. A PSK (Pre-Shared Key) TLS tunnel is established between the TM (acting as a TLS client) and the Mobile Network Operator's IDPS based on the key derived from GBA mechanisms (the IDPS playing the role of a GBA NAF). This security mechanism provides mutual authentication and encryption of the exchanges between the TM and the IDPS. The IDPS also receives from the BSF information that enables it to identify the mobile subscriber.

3. The TM sends a HTTP request, within the established PSK TLS tunnel, to the IDPS containing a `<idp:GetAssertion>` SOAP request (with a "purpose" attribute either set to "urn:liberty:idp:2007-09:purpose:minting" or "urn:liberty:idp:2007-09:purpose:SSO").

4. The IDPS processes the `<idp:GetAssertion>` request. The Target Identity is obtained from the underlying security mechanism (GBA mechanism initialized at step 1). The IDPS responds with an `<idp:GetAssertionResponse>` containing NameIdentifiers corresponding to the GBA authenticated user and an AuthenticationContext referring to that authentication method. The TM has then obtained all the "SSO credentials" required to act as an extension of the Mobile Network Operator's IDP (for either minting or hoarding scenarios) for this authenticated user (mobile subscriber) without requiring any subsequent user authentication.

"GBA TLS-based security profile at an ID-WSF AS": The TM first reaches the Liberty ID-WSF Authentication Service (AS) to obtain the credentials required to invoke the Liberty ID-WSF IDP Service (IDPS). ID-WSF AS and GBA NAF functions are collocated to benefit from GBA authentication mechanism.
Figure 6. Message flow for ID-WSF AS with GBA authentication mechanism and IDPS

1. The TM (LUAD-WSC) sends an HTTP request to the Mobile Network Operator's ID-WSF AS. The request contains a <SASLRequest>, where the "mechanism" parameter is filled with a list of one-or-more client-supported SASL mechanism names. The TM shall indicate to the NAF/AS that GBA-based authentication is supported by adding a specific value to the "User-Agent" HTTP header.

2. The AS sends an HTTP response to the TM. The response contains a <SASLResponse>, where the "serverMechanism" parameter is filled with the appropriate SASL mechanism name (i.e. DIGEST authentication) in order to trigger the GBA authentication mechanism.

3. If the no valid bootstrapping session or the freshness of the key material is not sufficient for the AS/NAF, then a new bootstrapping procedure will executed with the BSF.

4. The TM re-sends an HTTP request to the AS. The request contains a <SASLRequest>, where the "mechanism" parameter is filled with the returned SASL mechanism in step 2 and digest response computed as defined in [9] (GBA derived key used as credential) to be able to authenticate to the AS/NAF.
5. The AS acting as a NAF processes the digest response conveyed in the `<SASLRequest>` and validates the authentication with materials provided by the BSF. It also obtains information that enables it to identify the mobile subscriber.

6. The AS responds with `<SASLResponse>` in the HTTP Response. The `<SASLResponse>` contains an ID-WSF EPR (EndpointReference) which refers to the Mobile Network Operator's IDPS instance. The `<SASLResponse>` also contains some necessary credentials for the TM to invoke that IDPS.

7. The TM sends a HTTP request to the IDPS containing a `<idp:GetAssertion>` SOAP request (with a "purpose" attribute either set to "urn:liberty:idp:2007-09:purpose:minting" or "urn:liberty:idp:2007-09:purpose:SSO"). The request also contains a `<wsse:security>` header which includes the credentials returned in step 6.

8. The IDPS processes the `<idp:GetAssertion>` request. The Target identity is obtained from the security header. The IDPS responds with an `<idp:GetAssertionResponse>` containing NameIdentifiers corresponding to the mobile subscriber (target identity) and an AuthenticationContext referring to that authentication method. The TM has then obtained all the "SSO credentials" to act as an extension of the Mobile Network Operator's IDP (for either minting or hoarding scenarios) for this authenticated user (mobile subscriber) without requiring any subsequent user authentication.
4. Guidelines related to the invocation of a Trusted Module hosted in the SIM/UICC card

Once instantiated and delegation rights obtained from the IDP for the authenticated user, the TM instantiated in the SIM/UICC card can be invoked through the Smart Card Web Server in the same way as described in [1], by:

- The device's browser (or plug-in that implements the ECP profile),
- Local applications.

![Diagram of actors involved in TM usage]

To enable these use-cases, the SIM/UICC-based TM MUST support the following IDP interfaces:

- The SAMLv2 IDP Enhance Client or Proxy (ECP) profile as defined in [12] (for browser-based use-cases),
- The ID-WSF Authentication and SSO Services as defined in [11] (for application-based use-cases).

In the context of a Mobile Network Operator, the discovery of the endpoints of these interfaces SHOULD be based on well-known location principles with the following URLs defined:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAMLv2 IDP ECP SOAP endpoint</td>
<td><a href="http://127.0.0.1:3516/tm/ecp">http://127.0.0.1:3516/tm/ecp</a></td>
</tr>
<tr>
<td>ID-WSF Authentication Service endpoint</td>
<td><a href="http://127.0.0.1:3516/tm/as">http://127.0.0.1:3516/tm/as</a></td>
</tr>
</tbody>
</table>

These interfaces provide implicit authentication of the mobile subscriber thanks to the GBA mechanisms prior used to obtain the SSO credentials as described in the previous chapter.
5. Security Considerations

Provisioning phase

OTA mechanisms recommended in this document rely on secure channel protocols that ensure secure provisioning of the TM application in the SIM/UICC card. It provides end to end security from the OTA platform (hosted in the Mobile Network Operator infrastructure), which outputs the application, to the SIM/UICC card. This secure channel is established with a shared secret between the OTA platform and the SIM/UICC card. Thanks to this symmetric key cryptography architecture, both integrity and confidentiality of the TM are maintained.

Acquisition of SSO credentials at IDPS

In the context of a Mobile Network Operator, two GBA-based security profiles described in this document are recommended to secure the interactions between the TM and IDPS in order for the TM to obtain the required SSO credentials.

The "GBA PSK/TLS-based security profile" directly provides mutual authentication at transport level between the SIM/UICC-based TM and the IDPS (hosted by the Mobile Network Operator), reusing the existing security relationship between the Mobile Network Operator and the SIM/USIM of the user (Pre-Shared keys). It also enables implicit identification/authentication of that user (the mobile subscriber which is the owner of the SIM/UICC card) for which the TM will obtain delegation rights.

It corresponds to the ID-WSF security mechanism: "urn:liberty:security:2003-08:ClientTLS:null" (with specific TLS CipherSuite such as TLS_PSK_WITH_3DES_EDE_CBC_SHA or TLS_PSK_WITH_AES_128_CBC_SHA used to establish the SSL tunnel).

In the case of "GBA TLS-based security profile" at an ID-WSF AS:

• The authentication of the ID-WSF AS/NAF by the TM relies on SSL/TLS ("urn:liberty:security:2003-08:TLS:null" ID-WSF security mechanism). The TM shall verify that the server certificate corresponds to the FQDN of the ID-WSF AS/NAF it established the tunnel with. No client authentication is performed as part of SSL/TLS (no client certificate necessary).

• The authentication of the TM by the ID-WSF AS is based on the GBA SASL Digest mechanism, reusing the existing security relationship between the Mobile Network Operator and the SIM/USIM of the user (Pre-Shared keys).

The ID-WSF AS will then generate an ID-WSF EPR targeting the IDPS with a SAML Bearer assertion as credential for the IDPS (assertion with the GBA authenticated user as Subject). On IDPS-side, it thus corresponds to the ID-WSF security mechanism: "urn:liberty:security:2005-02:TLS:Bearer".

The risk of interception of such a "bearer" token is in that case mitigated by the fact that it is only conveyed through secure channels (SSL/TLS) and used on client-side in the SIM/UICC that can be considered as a secure and trusted environment.

In the end, these two GBA-based security profiles enable the IDPS to securely generate SSO credentials targeted for the principal that is the owner of the SIM/UICC card hosting the TM and thus to provide to that TM all the information required to act as an extension of the Mobile Network Operator's IDP for that authenticated principal.
That means that:

• in minting scenarios: the `<GetAssertionResponse>` returned by the IDPS will convey a `<MEDInfo>` element with `<NameID>` element(s) that correspond to the principal authenticated through GBA mechanisms (mobile subscriber owner of the SIM/UICC card).

• in hoarding scenarios: the `<GetAssertionResponse>` returned by the IDPS will convey `<Assertion>` element(s) with a `<Subject>` that corresponds to the principal authenticated through GBA mechanisms (mobile subscriber owner of the SIM/UICC card). These assertions MUST convey a `<AuthnContext>` element referring to GBA authentication contexts as defined in [10]:
  - urn:3gpp:gba:ac:saml:2007-08:classes:GBAOneFactorUnregistered (derived from SAML authentication context class MobileOneFactorUnregistered)
  - urn:3gpp:gba:ac:saml:2007-08:classes:GBATwoFactorUnregistered (derived from SAML authentication context class MobileTwoFactorUnregistered)
  - urn:3gpp:gba:ac:saml:2007-08:classes:GBAOneFactorContract (derived from SAML authentication context class MobileOneFactorContract)
  - urn:3gpp:gba:ac:saml:2007-08:classes:GBATwoFactorContract (derived from SAML authentication context class MobileTwoFactorContract)

**Invocation of the TM**

General SAML security recommendations towards IDPs as defined in [13] should apply to the TM in that case (the TM acting as an IDP).
References


[10] 3GPP TS 29.109 – “Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3”

