Bridging IMS and Internet Identity

Version: **1.0**

Date: May 6, 2010

Editors:

Ingo Friese (Deutsche Telekom)
Jonas Högberg (Ericsson)
Mario Lischka (NEC)
Gaël Gourmelen (Orange)
Fulup Ar Foll (Sun)
Joni Brennan (IEEE-ISTO)

Contributors:

José Luis Mariz, Jesús de Gregorio and Carolina Canales (Ericsson)
Peter Weik (Fraunhofer FOKUS)
Joao Girao and Naoko Ito (NEC)
Shin Adachi (NTT)
Martin Meßmer (T-Systems)

Status: This document is a **Kantara Initiative Draft Recommendation**, created and approved by the XXX WG (see section 3.8 of the Kantara Initiative Operating Procedures)

Abstract:

Digital Identity has grown separately in IMS and Internet. While the one offers walled garden services the other is focused on openness and third party integration. However, for future Telco-business an inter-working of IMS and Internet is needed. A methodology where real use cases are used shows the benefits for operators, SPs and end-users by bridging these two worlds. These use cases cover the exposure of IMS authentication to Web services, exposure of Web federations to IMS networks and exposure of IMS resources to Web 3rd parties. In an IMS domain, for SSO, SAML assertions are conveyed in SIP messages. In a multi-domain world, the SSO solution is based on a GAA/GBA solution. For attribute sharing, LAP ID-WSF messages are used. When a Web Service Provider (WSP) exposes user data being retrieved from the IMS a resolution of the mapping between the SAML identifier and the IMPU is needed. The working assumption is that the user experience should be seamless while keeping attention to security and privacy. The main findings and conclusions is that

no new technologies are needed. It is enough for IMS and DigId technologies to complement each other. The technical details are explained in the annexes.

Filename: Kantara_Bridging_IMS_Draft_Recommendation_v1.0.doc

Table of Contents:

1 Introduction

These days it is agreed that Identity Management (IdM) is a crucial component in a service environment although the term identity is perceived differently in different domains. This is true especially between the Internet and the telco domain where fundamental differences could be identified. In the Internet environment, an identity is usually associated with a username, while in the telco domain an identity is, for example, an access customer.

Family members using the same fixed line telephone cannot truly be provided with personal services since the users simply cannot be differentiated. On the other hand, users of classic telco services like voice, fax and SMS do not need to handle and maintain passwords, since they are authenticated by the network. In fact, they already have seamless access.

Both the Internet and the telco-world have evolved their own identity solutions, protocols and frameworks, because they have grown separately. On the way from the Plain Old Telephony System (POTS) to the Next Generation Network (NGN) the telco community developed and standardized the IP Multimedia Subsystem (IMS) as a framework to describe the implementation of telco services based on the Internet Protocol (IP). Although IMS standards foresee the development of advanced identity mechanisms, they still specify a separated and rather closed world. Therefore, interoperability between the Internet and IMS is still an issue and there is a growing need for inter-working. Telcos develop Application Programming Interfaces (APIs) to offer their assets to the Web community or to a 3rd party service provider. Furthermore, they implement complex service scenarios containing Internet and telco elements.

The Kantara Initiative Telecommunications Identity Work Group (TIWG) works towards bridging those different worlds in order to enable convenient and seamless service usage while maintaining security and privacy for the user. The capabilities that Liberty Alliance Project federated IdM technology add to IMS for authentication and user data exchanges have a positive influence for the telecom operator. Aided by these capabilities, telco operators can manage their current business in a more efficient way. New business opportunities will also arise that could generate new revenues.
Instead of proposing yet another framework the target of this white paper is to identify the potential to leverage existing technologies and standards. The main focus is on Liberty Identity Web Services Framework (ID-WSF) and Security Assertion Markup Language (SAML) on the one side and 3GPP IP Multimedia Subsystem (IMS) on the other. The leveraging of other standards, such as OpenID, is out of the scope of this white paper.

In this paper we introduce examples of inter-working on the cross-roads of the Internet and telco domain. Different approaches to seamless authentication and service usage as well as attribute exchange across domains are discussed motivated by business requirements and illustrated through use-cases. We briefly introduce the

related technical specifications and standards and provide the details in a technical annex.
This paper is the first step of the SIG Telco to bundle identity issues that are relevant to the telecommunication industry.

2 Problem Statements

Both IMS and Web frameworks have to provide authentication and authorization services. Both frameworks need to answer questions like: "Who are you? Are you authorized for this? Where are you coming from? …" Nevertheless, while they must answer the same class of questions, the chosen identity models are quite different.

1. Root of identity: IMS's identities are traditionally based on a reachable address (ex: telephone number or sip address) when most Web applications expect identity to be a pointer on some form of user profile (e.g. LDAP DN, User-ID, Customer number).
2. Source of identity: IMS's identities are mostly provided by some form of trusted element on the networks (e.g. mobile SIM/ UICC card) where Web applications identities are created at server level, and are mapped to the device through a network session (TCP) or through some form of application session (e.g. cookies, session-ID).
3. Connectivity model: IMS devices will rarely connect directly to a given application. Typically they pass through intermediaries (SIP proxy). On the other hand, for Web applications intermediaries are limited to network equipments and are invisible from the application.

IMS identities were base on the assumption that everything runs inside a well contain and trusted environment. Alternatively, modern Web applications are designed upfront with the assumption that the Internet cannot be trusted. In IMS one sticks one or a few IMPU (IP Multimedia Public Identity) inside a device's SIM card/UICC (**Universal Integrated Circuit Card)**, and then exports those IMPU to every application. When on the Internet each application has its own identity for a given user. The direct result is that in IMS there is no "Single Sign-On (SSO)" issue. However, because of the exported "public identity" (e.g. a unique TELURI or SIPURI) a strong privacy constraint is inherited preventing the leveraging of 3rd parties services.

On the Internet SAML2/Liberty solved the "Single Sign On" issue. Internet applications now have a working model to address both usability (seamless end-user experience), and privacy handling. Alternatively, IMS and telcos in general had a tradition of handling everything in a closed and self contained circle of trust. Until recently IMS and telcos were in a position to largely ignore the external world. Privacy was well considered and 'protected' as nothing was sent out to external 3rd parties. In such a closed world providing users with a smooth experience was almost simple. Nevertheless today people agree that leveraging to external services is a "must have" feature. Telcos like many other players of the industry (ex: TV) need to find a way to leverage this to external services providers.

3 Business perspectives

It is obvious that both IMS and Web will continue to co-exist for some time. While full convergence may occur in the long term future, operators need a working solution to leverage both technologies sooner to make this co-existence seamless to customers. If we look at a global mobile communication world, we can divide it into two parts:

Internal vs. external services (South - North): Internal services are very secure and get a very fine grain visibility on customer profile (e.g. presence, geo-location, pre/post paid), but these services are time consuming and expensive to develop. Furthermore, it is harder each day for operators to impose new services (e.g. instant messaging, social networking) in a walled-garden approach, without taking into account external services and communities. External services on the other hand are moving at Internet appropriate speeds to respond to customer demands. Nevertheless, these external services are often not trusted and as a result rarely get access to customers' Telecom internal profile.

IMS vs. Web protocols (West - East): If we spend time arguing the pro/cons of each protocols stack, it is very clear that customers are not interested in which protocol a given service uses. They simply want a seamless and fully transparent zapping experience from one to the other. Most people agree that Web protocols are best suited for user graphical interface and easier to integrate for external service providers, While IMS, on the other hand, has a smarter method to handle multimedia real-time streams and is better designed to interoperate with operators' backbones and thus get better access to customer dynamic profiles (e.g. presence).

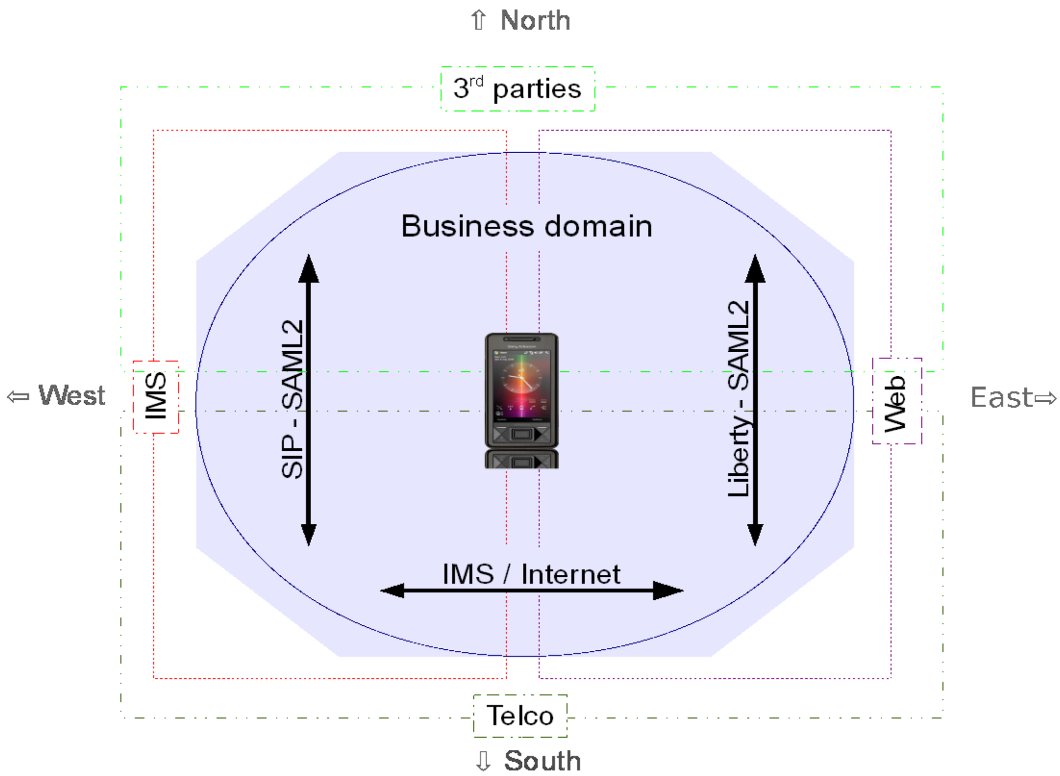

Figure 1: Zones of Services

The global picture of mobile communication as sketched in Figure 1 is split by two axis and we get 4 zones of services. In these, the directions:

South -> North: represents Telecom giving 3rd parties services access to their customers. While this access needs to be seamless to end-users, it is understood that the level of trust and control within 3rd parties is lower than for internal services imposing strong privacy protections.

North -> South: either a 3rd party service leverages telco internal customer information (e.g. presence, billing) or external users (non-customers) accessing some internal services (e.g. a photo services that your friends/family can see even when they are coming from another operator).

West -> East: IMS is accessing a Web service.

East -> West: A Web service is initiating an IMS service (e.g. starting a media streaming).

While Web applications operators have an answer to address 3rd party services outside of an operator trusted domain through Liberty/SAML 2.0 (South-North), they have nothing to address this issue in IMS; additionally, they have no options for IMS/Web (West-East) interoperability. This paper addresses the IMS North-South issues by demonstrating how SAML 2.0 assertions can be embedded inside SIP protocol messages without significant impact on the IMS network. On the West-East axis it is shown how to leverage internal IMS attributes from 3rd Web applications.

The capabilities that LAP federated identity management technology adds to IMS for authentication and user information exchange, as well as for service components interaction on protocol layer among the HTTP and SIP services worlds, have a positive influence in a number of operator business areas as follows:

Increased effectiveness in managing their current business:

- **Network operation simplification;** The standardization efforts for creating a simpler network to manage (all-IP, all-packet, one converged switch, one converged user-centric DB) are nicely complemented in the architecture by having user-centric access control functions, such as authentication and authorization for all services and network accesses. LAP mechanisms integrated with IMS and core network technologies provide an effective way of implementing subscriber-centric functions as they unify the exposure of those to all applications by utilizing widely accepted and standard application developers techniques.
    - The operator business case for this is measured mostly in terms of Operating Expenditure **(**OPEX) reduction by the ability to centralize operations on consolidated subscriber-centric infrastructure in the network. Over time, a simpler network containing those functions also delivers Capital Expenditure (CAPEX) savings by reducing the number of network nodes necessary to be deployed as compared to a service silo situation.
- **Fast Service Launch;** A Service Creation Environment (SCE) that leverages mostly on operators' network capabilities and provides optimal service management routines requires a combination of IMS (mostly SIP technology based) and SDP (mostly HTTP technology based) capabilities. Additionally, for that SCE to be fully horizontal across applications and accesses, some common support functions shall be shared by the SDP and IMS enablers. Among those users identity and data management is the key. The utilization of LAP mechanisms bridges IMS and HTTP capabilities, and also enables the use of common federated user identity management functions in that service creation environment. Utilization of LAP mechanisms also enables formatting IMS information in terms of HTTP and offers unified HTTP-based application integration mechanisms for all services.

The operator business case for this scenario is measured mostly in terms of OPEX reduction average time and efforts to integrate a new application and launch a new service.

Enabling new revenue generation and new business opportunities:

- **New business models;** once a user’s identity, personal and content information is exchanged through standard mechanisms across the Internet, service delivery value chains are opened. This opening enables creativity for new business models, as technology issues become less complex and less expensive. Among possible new business roles, the role of the Identity Provider (IdP) is crucial to the retention of current ownership of your final customer. Additionally, the IdP role can serve as a building block towards achieving other roles such as security provider, attribute provider and/or payment provider. Operators can become brokers in the Internet for other businesses through exploitation of some of their existing assets with regard to Business to Consumer (B2C) Telecom services delivery.
    - The operator business case in this scenario is measured mostly in terms of new revenues through services commission (brokerage) and has some strategic impact in terms of customer loyalty and marketed values of their consumer-facing commercial brands

- **Increased service usage;** enriching customer experience of services and increasing the ability to be reachable by a critical mass of services are ways to increase the Average Revenue per User (ARPU). Exposing the network user-centric views and context information to applications is the key to achieving these improvements. Finding the right data model to be exposed to applications through operator network information bits, and perhaps other actors too, involves maximizing reach ability for many "raw" data sources. This can be achieved through distributed infrastructures inside and outside operators. Choosing the appropriate data model depends on the business model that is used for delivering final user services, and both internal and external federation capabilities such as those in LAP specifications are key mechanisms to be able to share that data across infrastructure domains.
    - The operator business case for this is measured mostly in terms of new revenues for ARPU increase, and to some extent in reduction of churn through current improvement of customer services experience.

Personalization of End User's Services; Knowing the customer by any consumer facing brand such as the Telecoms operator becomes a key strategic activity, especially in saturated markets. Tailoring applications based on user preference significantly improve the user’s experience and will increase customer loyalty. Context information and user attributes contribute to personalizing services provided by Business Support Systems (BSS). LAP mechanisms integrated with IMS and other network DBs as well as network nodes containing dynamic information on user behavior and service rendering enable exposure of aggregated meaningful data models that can be easily integrated with many profiling applications. These mechanisms can be easily added and changed at a low cost as they use ‘friendly’ application integration technologies and main stream (low cost) Web services mechanisms.

The operator business case can only be measured in 2 ways:

- Indirectly in terms of improvements in the evolution of customer loyalty/churn rates; and
- Strategically in terms of improvements in their consumer brand value.

These capabilities being used by operators in turn provide some benefits to end-users and other service providers as:

End-Users:

- **Higher security and privacy protection;** The ability to reuse the network embedded security mechanisms of operators for user interactions with all services inside the operator realm and across the Internet increases the level of security and privacy protection compared to what exists today. As well as enabling end-users to utilize a transaction broker brand like an operator that is trustable and that can legally be responsible for the security level involved in the transaction.
- **Richer services experience;** The ability to exchange more information across and combine service capabilities among operators and other service providers will offer end-users with a larger variety of services as well as richer service experiences across various terminals and access networks, with a common service look and feel, with personalization and having the service delivery adapted and optimized for the end-user contextual situation in real-time.

Service Providers:

- **Focus on core business;** The ability to exchange capabilities in an interoperable and secure manner opens up value chains and provides more opportunities for final service providers to outsource some of these capabilities to new business mediation actors. So focus can be on their truly core business processes, therefore saving costs and getting a more competitive edge through more dedication to their business differentiation.
- **Utilization of richer and wider delivery channels;** Networks with enriched capabilities from operators that become easily accessible to service providers widen significantly the distribution channel of any service. This is as end-users move more of their daily interactions to the online world and become more and more mobile and multi-terminal in all their services usage. Additionally, some of those capabilities are quite unique in terms of information available within a network operator domain. So, it becomes also a much richer service delivery channel compared to existing ones and so allowing the service provider to build additional service differentiation.

4 Use-Cases

This section presents concrete use-cases illustrating inter-working between IMS and Web worlds as introduced in the previous section. While the first coming use-case is more related to IMS in mobile operators' context, the next ones apply to both fixed and mobile contexts.

4.1 Exposure of Authentication from IMS to Web

The following use-case illustrates how we seamlessly expose the IMS authentication done within the operator domain to access a Web application provided by an external party on the Internet ("South-West->North-East" direction as depicted in chapter 3). 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.

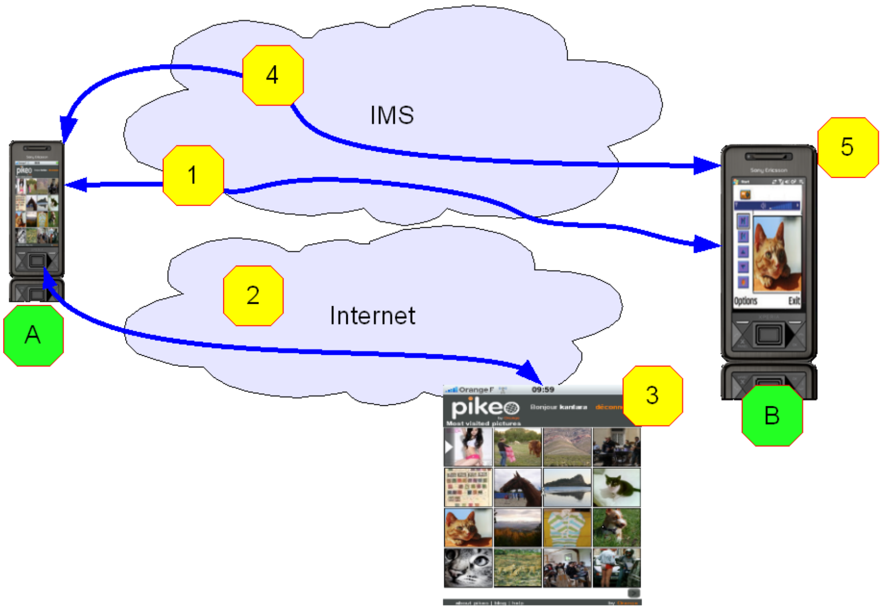

Figure 2: Photo-sharing use-case illustrating Single Sign-On from IMS to Web.

1. User-A has an IMS voice communication with User-B.
2. In the middle of the communication User-A is willing to share a photo located on his Internet photo service and thus decides to access to this Internet service in order to retrieve that photo.
3. User-A is seamlessly authenticated to his photo service (not provided by the telco operator) thanks to the re-use of its IMS authentication. He can select the photo to download to his mobile phone.
4. User-A shares the downloaded picture with User-B through the IMS content sharing service.
5. User-B sees User-A's photo.

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 not only are outside of IMS (Web photo service) but also outside of the operator's domain (independent third-party service provider).
- Operator 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.

The technical details of this use-case are described in section 5.1.

4.2 Exposure of Web Federations to IMS Networks

The second use-case emphasizes the security and privacy concerns of the telecom operators when integrating IMS services provided by third-parties (both "South->North" and "North->South" directions mixing IMS and Web domains as depicted in chapter 3). In the given case, the operator does not disclose user's real IDs (ie phone number) to third-party applications.

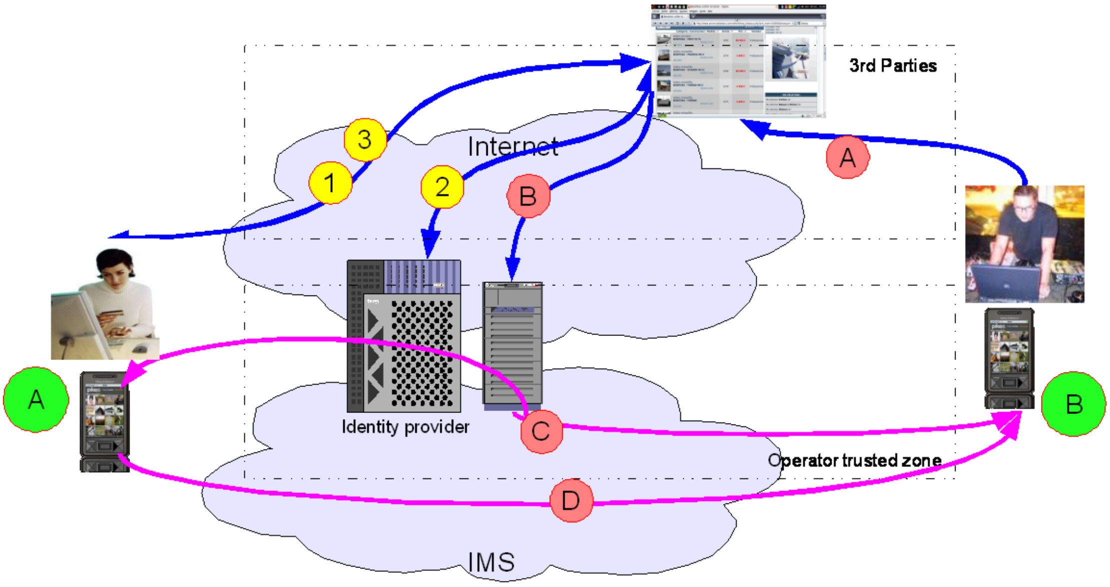

Figure 3: Ads website (provided by a third-party) use-case illustrating consistent user-experience in both Web and IMS contexts as well as privacy concerns.

1. User-A wants to sell an item through an online ads website. Before posting his advertisement, User-A needs to create an account at that site. He can either fill in all the requested information or opt for a one-click privacy-enabled registration, leveraging existing partnership between his telecom operator and this third-party website.
2. User-A chooses the one-click process and is requested to authenticate with his telecom operator (acting as an Identity Provider) in order to federate accounts. During this process, the telecom operator will provide an alias instead of real user IDs (i.e. phone number). The benefit for users is that the website cannot publish User-A phone number as it does get it. The website only relies on aliases provided by the telecom operator in order to reach users.
3. User-A can now edit and then post his new ad. Depending on his preferences, "click to call" / "click to contact" buttons are automatically added in order to reach him by phone, instant messaging or email, this without revealing his real IDs (either fixed or mobile phone number, email address, …).

Other users can now search and access to this new ad through the ads website.

A. User-B is browsing on this ads site and is interested by User-A's ad.
B. In order to get more information, User-B clicks on the "click to call" button to initiate a phone call with User-A.
C. The ads service acts as an intermediary in order to bootstrap the connection between User-B and User-A based on the alias.
D. This call is automatically routed to the right device for User-A either fixed or mobile (thanks to the telecom operator infrastructure) and the telecommunication is established between User-A and User-B.

The key benefits of this use-case are:

- Users are provided with a consistent user experience when accessing third-party Web and IMS services, while preserving privacy and security aspects.
- The operator does not need to disclose the users' real IDs.
- Users can be identified in a consistent way from both IMS and Web worlds.

The technical details of this use-case are described in section 5.3.

4.3 Exposure of IMS resources to Web third-parties

This use-case shows how third-party Web sites can leverage IMS resources (e.g.: presence) exposed by the telecom operator to offer an enriched experience ("North-East->South-West" direction as depicted in chapter 3).

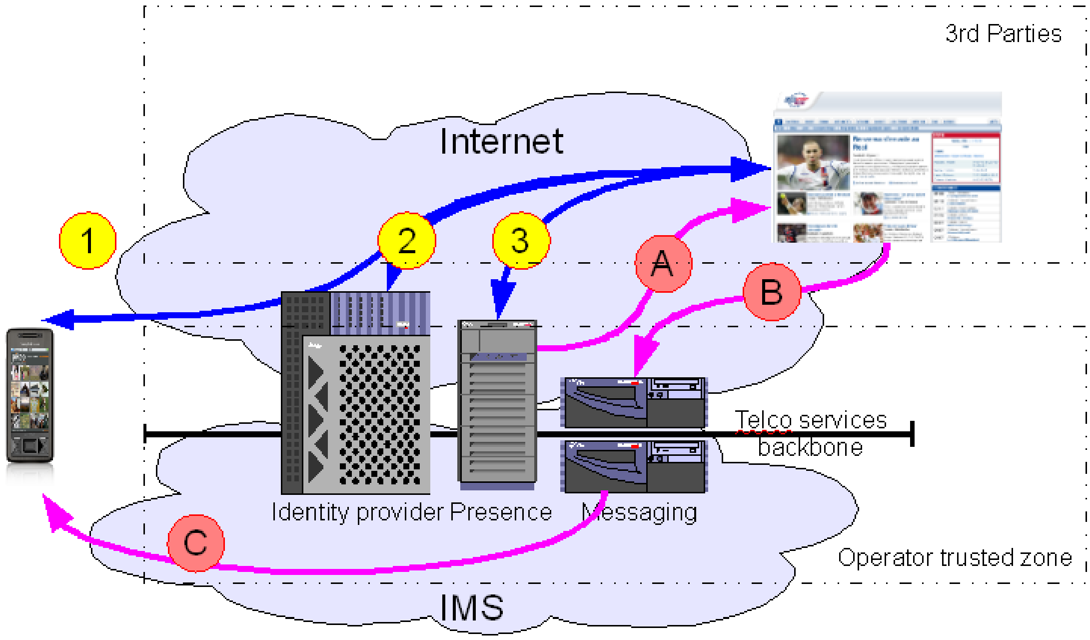

Figure 4: Exposure of IMS presence and messaging capabilities to Web third-parties.

1. User-A browses to his preferred sport news Web site. He wants to subscribe to the new notification service to receive score updates for games involving his favorite soccer team. The Web site informs him that he can benefit from advanced features in cooperation with telecom operators: notification messages only sent based on its "presence" status and conveyed to whatever device he is connected through (phone, PC…).
2. User-A chooses to use these advanced features and is requested to authenticate with his telecom operator (acting as an Identity Provider) in order to enable the Website to gather all required information to activate this feature.
3. User-A gives his consent to enable his preferred sport news Web site to access his IMS presence status and IMS messaging capabilities. Users-A can now configure the sport notification service and activate it.

Later on, during the soccer game event:

A. The sport news service is notified of the presence status of user A.
B. Depending on the presence status of user A, the sport news service will send him messages to inform him of updated scores.
C. The telecom operator routes the message to the right device and User-A is informed in real-time.

The key benefits of this use-case are:

- Users and third parties Web sites are able to leverage resources from the IMS in order to provide advanced features combining presence and messaging capabilities (routing to the right device).
- Users do not need to disclose their real IDs (phone number …) to third-party Web-sites.

The details of this use-case are described in section 5.4.

5 Technical solutions

This section aims to describe the technical solutions that correspond to each use-case presented in the previous section. The objective is to leverage existing technologies and standard specifications in both Web (such as Liberty/SAML ones) and IMS worlds. This section also aims to show how existing technologies can integrate together to provide solutions to the identified needs. These existing technologies and standard specifications are referenced here rather than explained in details in order to focus on the main inter-working concepts (though technical details can be found in annexes for each of the described solutions).

5.1 Solution on Authentication from IMS to Web

SAML 2.0 is the framework of choice for Identity management and SSO for Web-based services. The combination of SAML 2.0 with the Generic bootstrapping architecture of 3GPP enables the leveraging of SIM-based, accepted, strong and mutual authentication to the Web.

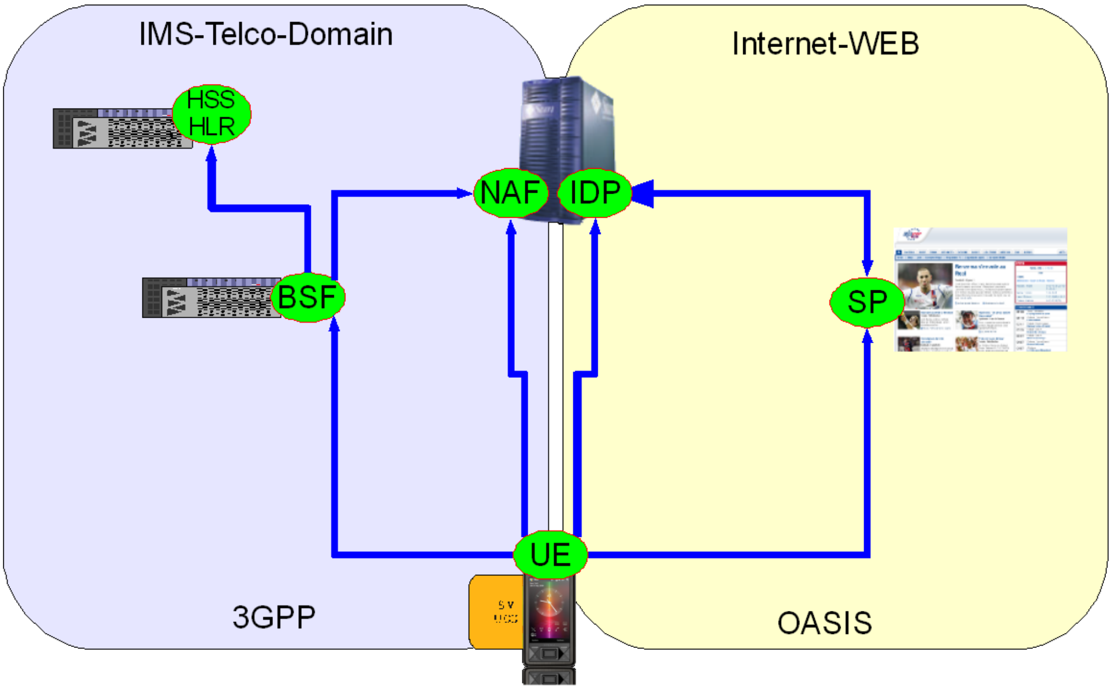

Figure 5: Exposure/Re-use of IMS authentication to third-parties in the Internet

5.1.1 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.

We will briefly describe the bootstrapping procedure in combination with the HTTP Digest authentication option illustrated in Figure 1. Our setup co-locates the IdP and NAF. Please note that other options are possible especially the co-location of IdP and 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 annex of this paper or the Technical Specification of GBA, Interworking of ID-FF and GAA [3GPP TR 33.220, 3GPP TR 33.980], or IdP Discovery [SAML2 Profile].

SAML 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 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 '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 ISIM/AKA authentication by sending a request to the BSF including its IMS Private Identity (IMPI).

The BSF extracts the IMPI and fetches a set of authentication information for that identity from the HSS and sends back a derived user MD5 challenge.

The UE checks the challenge and calculates the corresponding response by means of the application of the IP Multimedia Services Identity Module (ISIM) at the Universal Integrated Circuit Card (UICC) and sends them to the BSF.

The BSF will now compare the response with the expected values and will eventually derive a session key (Ks-NAF) and store it together with a self-generated BSF-Transaction Identifier (B-TID). It will then send back the B-TID and a key lifetime parameter to the UE.

SAML part 2

The UE answers with a HTTP GET request containing as a username the B-TID and as a password the Ks_NAF. The UE may include further LAP related user data (e.g. public user ID).

The IdP responds with a SAML artifact in the HTTP Response redirect URL. The UE contacts the SP again using this URL and the SAML artifact. The SP sends a request with the SAML artifact to the IdP.

The IdP can now construct and send the requested assertion. The SP verifies the message and answers with a HTTP Response and the requested content.
Further technical details could be found in the Technical Annex A: "GBA & ID FF Interworking".

5.2 Sharing the Authentication Context

In the above solution, a tight coupling of the GBA client and the Web client is assumed. As an alternative we introduce two solutions for supporting existing Web client applications. Both mechanisms use the cookie information to convey the authentication context from IMS domain which is accessed via the GBA Client to Web domain accessed by the browser. The basic concept is that a GBA client provides the IdP with the cookie information conveying the authentication context. Then a Web browser starts LA ID-FF based access to SP upon a successful GBA authentication and redirected to the IdP to retrieve the Authentication Assertion.

The first option is to let the Web Client application get the cookie information directly from the GBA Client belonging to the same user. The GBA Client retrieves the cookie information upon a successful GBA authentication and passes it to the Web Client. This option is possible only when a Web Client (browser) exposes such functionality for a plug-in to insert cookie information offline.

The second option is to pass the Web Client application a temporal URI under the Identity Provider domain to fetch the cookie information through. This URI is a dedicated URI to a specific successful authentication and only valid for a certain period after the successful authentication. The GBA Client retrieves the URL upon a successful GBA authentication and passes it to the Web Client. The Web Client will then access the URL injecting the cookie information subsequently. Further details are presented in the Technical Annex B: "Authentication context sharing between GBA and Web Client applications on UEs".

5.3 Solution on IMS authentication to IMS third-parties

SAML is a set of protocol specifications that provide, among other things, seamless SSO and attribute exchange in a distributed environment. In particular, once a user has authenticated towards a trusted entity called the IdP, the SAML protocols enable the IdP and the SPs to exchange information about the user's authentication status at the IdP in a secure manner and in a way that takes into account the user's privacy. We will discuss now how a SIP/SAML binding could be used to exchange information

5.3.1 Using Federated Identities for Pseudonymity

The Application Server tries to establish an incoming call towards User-A. The Application Server can be hosted in the same network as User-A. The Application Server could also be hosted in another IMS network or even outside of an IMS domain. It is assumed that there is an existing relationship between the user’s IdP and the Application Server. The establishment of this federation is described in [SAML2Core].
Any of these initial steps enable the Application Server to reach the user via a pseudonym, which could be resolved at the IdP.

Then the application server is able to initiate a session with this pseudonym as a callee. The message is routed through the IMS network towards the IdP given in the pseudonym of the user as indicated in Figure 6. The IdP is able to resolve the pseudonym used by the application server into the corresponding IP Multimedia Public Identity (IMPU) of the user. In order to provide user privacy a new session is initiated by the IdP. The corresponding message is routed via the IMS network to the registered UE of the user. The IdP in addition to its traditional role is acting as a back-to-back proxy. Alternatively, an additional box could play this role. All replies and the following messages are routed via the IdP, which exchanges the IMPU of the user and the pseudonym accordingly (c.f. [TR 33.980]).

In case the user wants to establish an outgoing call using a pseudonym towards the application server, the flow is inversed to the one shown in Figure 6.

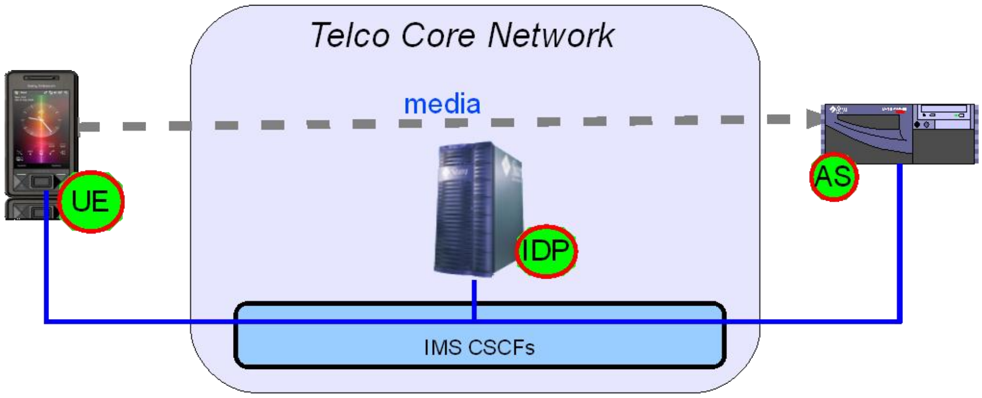

Figure 6: Incoming Call

5.3.2 Raise the Authentication Assurance and Acquiring Attributes

In the following use case the application server needs a higher level of authentication assertion from the user, or any other kind of attribute. One example scenario could be that the user is at home and line authentication has taken place based on the general subscription of his home.

The application server requires authentication of the specific user and related attributes.\

In case the user sends a SIP INVITE directly to the IMS application server in step 1, but is redirected to the IdP of the user in step 2. This IdP is specified in the initial message of the user. The redirected message contains a SAML request and the IdP sends back the corresponding SAML response in step 3 embedded in a SIP message. This flow is illustrated in Figure 9. A dedicated SAML-SIP binding is created for this purpose. Further details are discussed in the Technical Annex : "SIP/SAML Messaging".

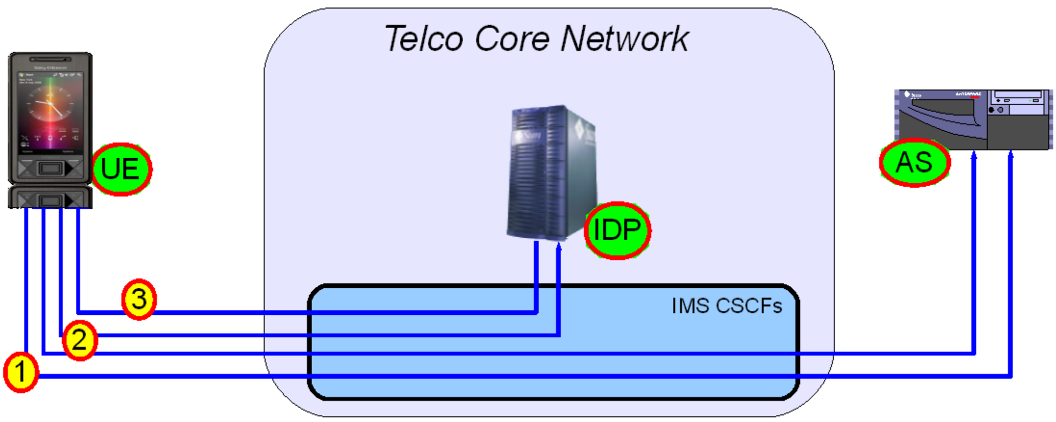

Figure 7: SIP SAML

5.4 Solution on Exposure of IMS Resources to Web 3rd Party

The third-party Service Provider (SP) wants to access to IMS resources (e.g. presence) exposed by the telecom operator through the Liberty ID-WSF Framework, or a similar standard, in order to offer an enriched service to its users.

From the SP standpoint, this can be seen as standard use of the ID-WSF framework: the mapping between ID-WSF resources (linked to SAML/ID-WSF user identifiers) and IMS resources (linked to IMS user identifiers) is fully managed by the telecom operator infrastructure behind the scene.

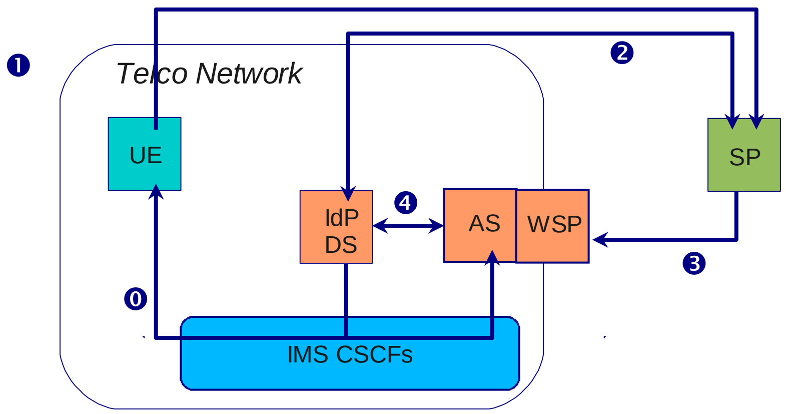

Figure 8: Access to IMS Resources Through ID-WSF

To access to the IMS resources managed by an IMS Application Server (AS) and exposed through ID-WSF framework as a Web Service Provider (WSP), the SP accessed by the user through his browser 1) first needs to establish a federation 2) with the IdP of the telecom operator. This can also include all discovery steps by querying the telecom operator ID-WSF Discovery Service (DS). The SP has then all the required materials to be able to invoke 3) the operator's AS/WSP. To be able to provide the requested resource (e.g. presence status of the identified user), the AS/WSP needs to map the targeted ID-WSF user resource (identified through the SAML/ID-WSF user identifiers) to the IMS one. Two options can be envisioned for that: either the AS/WSP already knows the mapping between the IMS and ID-WSF identifiers from step 0) with information pushed by the IdP part of the IMS flows (see Annex C “SIP/SAML Messaging”) or it needs to send a mapping resolution request to the IdP/DS 4.

The invocation of the AS/WSP can also include additional exchanges to gather user's consent if needed.

We can also imagine that the materials obtained by the SP at step 2) can be cached in order to later access to the AS/WSP even if the user is not browsing at the SP or the SP can subscribe at step 3) to change notifications to always cache up-to-date data (see presence and notification use-case in chapter 4.3). Further details can be found in the Technical Annex D: "Liberty ID-WSF and IMS inter-working".

5.5 Security

The proposed solutions leverage SAML2 and 3GPP security models and inherit their capabilities and limitations. [SAML2Core, 3GPP TR 33.980]

6 Conclusion

The IMS and Digital Identity worlds have grown separately offering two types of services, walled-garden and third-party. There is a need to bridge the two worlds. The idea is to do this in such a way that the user experience will be seamless while keeping attention to security and privacy. The assumption is that **no** fundamental changes are needed, i.e. existing technologies should be leveraged.

The business drivers for an operator bridging these worlds are:

- Increased effectiveness in managing their current business; and
- Enablement of new revenue generation and new business opportunities.

Benefits can be seen on various levels, e.g., OPEX, CAPEX, ARPU and new revenue streams.

To simplify the user experience, seamless access to third-party services across domains/IMS worlds is looked upon. This would be by offering seamless authentication across the domains/IMS worlds (SSO) and seamless service usage across domains by leveraging users' resources exposed in both worlds (attribute sharing).

Through some realistic use cases on how to expose IMS authentication and IMS resources to third-parties technical solutions are proposed. For SSO, the solutions are based on the idea to convey SAML assertions in SIP messages when the domain is IMS. When the domain is across worlds the proposed solution is based on the 3GPP security architecture GAA/GBA. For attribute sharing standard ID-WSF message flows are proposed. When an WSP exposes user data retrieved from the IMS, i.e., when the WSP acts as both a WSP in the Web domain and as an IMS AS in the IMS domain, a resolution of the mapping between the received SAML federation identifier and the IMPU is needed.

It has been shown that **no** new technologies are needed; it is enough to let IMS and digital identity complement each other to solve the mentioned problems. The aim is to continue and study how the IMS and digital identity worlds can complement each other.

7 References

3GPP TR 33.220	Generic Authentication Architecture (GAA); Generic bootstrapping architecture http://www.3gpp.org/ftp/Specs/html-info/33220.htm
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); http://www.3gpp.org/ftp/Specs/html-info/33980.htm

SAML2Core	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 Working Draft 12 February 2007 http://www.oasis-open.org/committees/download.php/22385/sstc-saml-core-errata-2.0-wd-04-diff.pdf
SAML2 Profiles	Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005

A. Technical Annex A: "GBA & SAML Inter-working"

Telcos are in an ideal position to become the Identity Provider of choice for consumers and business partners. Firstly, Telcos already have established relationships with millions of end customers. They administrate identities in the form of customer data sets with e.g. name, address and accounts. Integrated providers and wireless Telcos already have a widely deployed and established authentication instrument, basically the SIM/UICC card (Subscriber Identity Module/Universal Integrated Circuit Card) and have thus the basic technical requirement to be an authentication service provider and identity provider.

The Generic Bootstrapping Architecture (GBA) defined within 3GPP includes a solution for the reuse of authentication in the mobile world, on the basis of SIM/UICC. This type of smart card in mobile 3G devices contains all the required credentials and functionalities necessary for authentication. With GBA it is possible that a user also registers with web-based services via his UICC, which is typically used to sign-on to services like mobile telephony.

The reuse of the network authentication for web-based services is a valuable asset of a Telco and an important step to converged services. Reuse of network authentication is a convergent approach that brings the assets of the network into the service layer. It enables an easy and unhindered use of services based on a secure network authentication

This chapter describes the combination of the Generic Bootstrapping Architecture and Liberty Alliance Identity Framework based on technical report [3GPP TR 33.980] and the results of a Project Next Generation Network AAA of Deutsche Telekom Laboratories.

A.1 3GPP GBA

In UMTS Release 6 the 3GPP has started to define the GAA (Generic Authentication Architecture) as the framework for various peer authentication methods within the NGN world, in particular for Internet-based services (see [3GPP-TS33.919]). Within the GAA the Generic Bootstrapping Architecture (GBA) defines the functions that are required to authenticate a client to a Web-based service using his 3G subscription (see [3GPP-TS33.220]).

A.1.1 Architecture

Figure 9 gives an overview of how the GBA fits into the 3GPP world in comparison to the IMS environment. It highlights the new functions and interfaces introduced by the GBA.

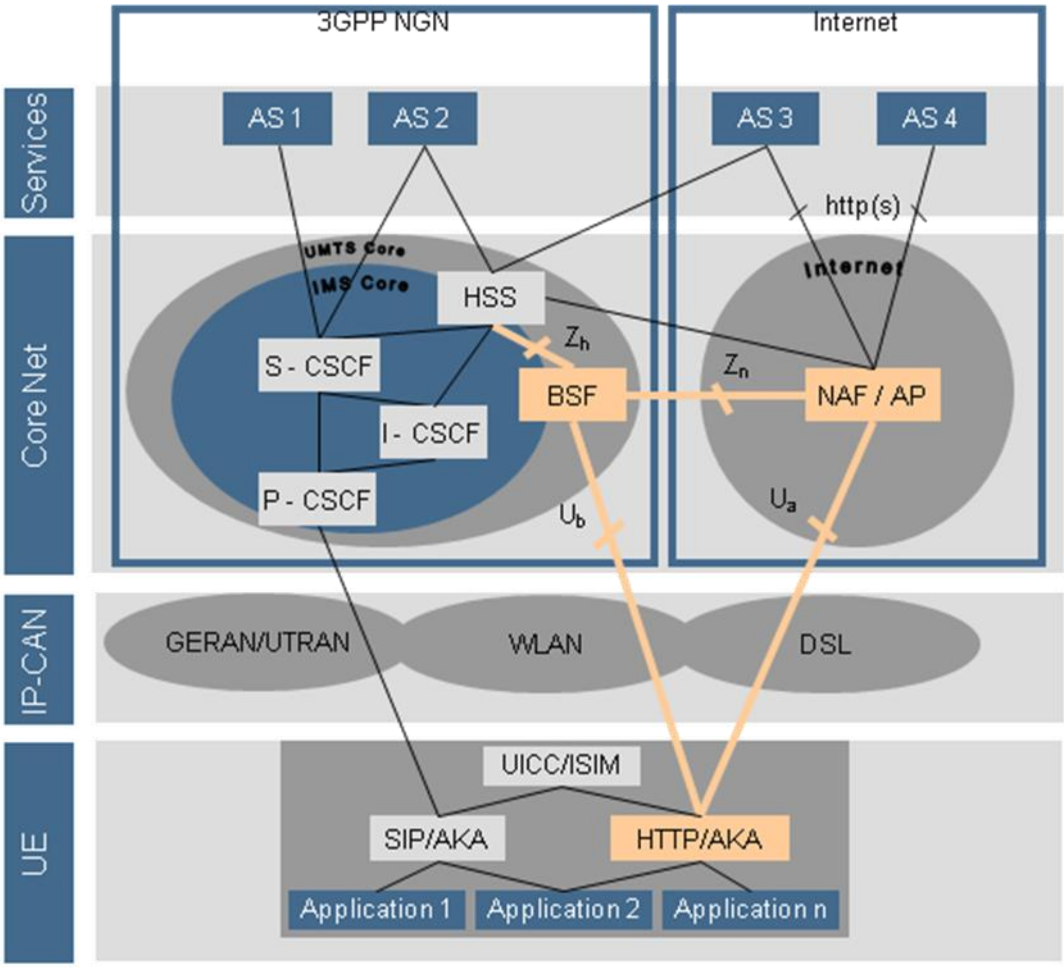

Figure 9: Generic Bootstrapping Architecture - Functions and Interfaces

The Network Application Function (NAF) constitutes the HTTP or HTTPS-based service that requires 3GPP authentication. The NAF may be divided into two parts, the Authentication Proxy (AP) and the Application Server (AS). In that case the AP is responsible solely for the authorization of the client, whereas the AS implements the application-specific functionality and relies on the authorization of the AP. Dividing the NAF into AP and AS is an interesting option in a scenario where the AS is operated by a third party Service Provider.

The Bootstrapping Service Function (BSF) is the authenticator, against which the user equipment (UE) has to do 3GPP authentication, i.e. the Authentication and Key Agreement (AKA) protocol using the IMS Subscriber Identity Module (ISIM) (see [3GPP-TS33.102]). The Zn-Interface (see [3GPP-TS29.109]) of the BSF enables the NAF to verify whether a UE was correctly authenticated against the BSF.

The ISIM/AKA authentication carried out over the U_b-Interface (see [3GPP-TS24.109]) between the UE and the BSF is transported over HTTP messages. Thus, the UE has to implement a HTTP-based ISIM/AKA authentication.

A.2 Advantages of a GBA Framework:

- NGN standards-based / FMC support: GBA is defined by 3GPP/ETSI-TISPAN and therefore fits perfectly into the NGN world. Since it can be deployed over any kind of access network including DSL, the architecture is also acceptable to fixed-line operators.
- Separation of Authentication and Authorization: The concept of separating the authentication (BSF) from the authorization (NAF/AP) can also be found in similar architectures like SAML 2.0 / Liberty Alliance (see [SAML2 Core] and ID-FF [LA-ID-FF]) or MS Card Space (see [MS-CSWeb]). It enables very flexible and scalable architectures, since the authorization service does not need to know any authentication details.
- Improved security through hiding of the user identities: The user identity (here: the IMPI) is only exchanged between the UE and the authenticating party (BSF), it is not visible to the NAF/AP.
- Accepted strong and mutual authentication mechanism: AKA is recognized as a strong and mutual authentication method with high security ratings and can be used with 2G (SIM) or 3G (Universal Subscriber Identity Module/USIM or ISIM) authentication material.
- Separation of authorization and application functionality: The concept of the AP enables scenarios where the Telco operator can offer authentication/authorization services to third party service providers (SP) in a way that the authentication complexity is hidden to the SP.

A.2.1 Procedures

The main procedure within the GBA is the bootstrapping procedure which realizes the 3G authentication via the Ub interface. The bootstrapping procedure is triggered by the NAF via Ua interface, for which there are different protocols defined:

- HTTP Digest authentication
- HTTPS with authentication of the underlying TLS connection
- PKI portal realizing the enrolment subscriber certificates

We will describe the bootstrapping procedure in combination with the HTTP Digest authentication option.

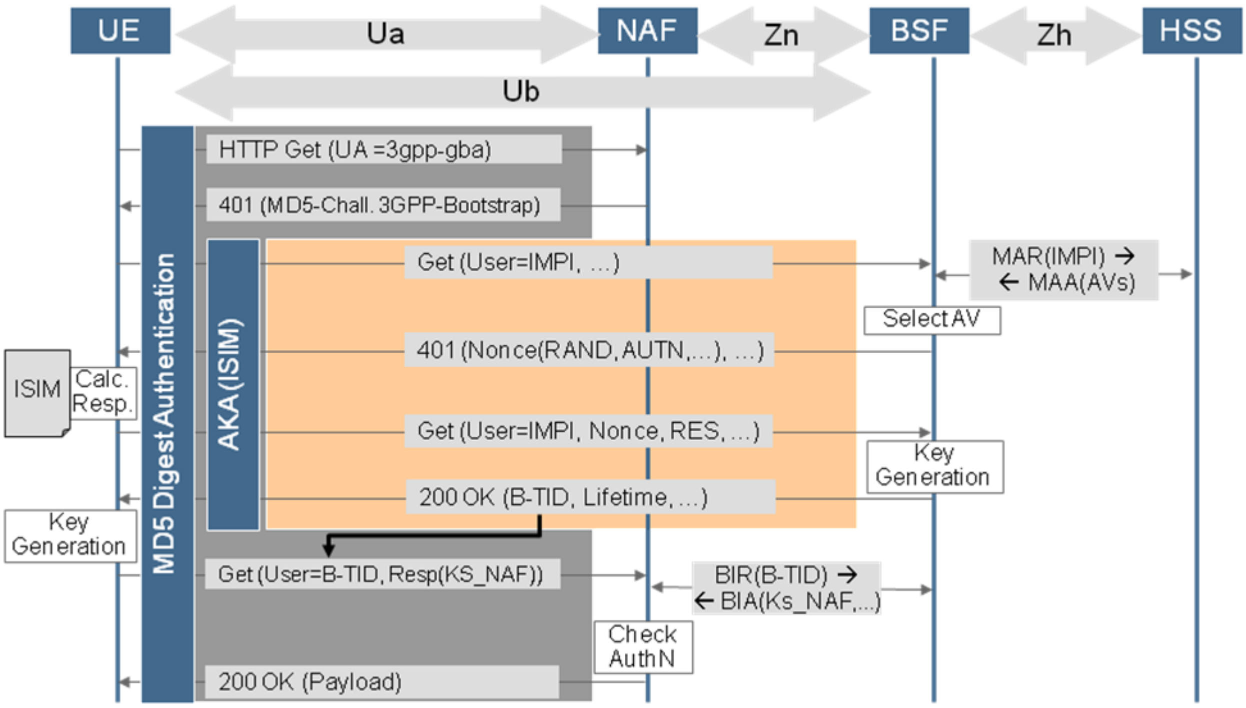

Figure 10: GBA - Bootstrapping Procedure

When a GBA-enabled UE initially tries to access a GBA-protected service via the NAF or AP, it inserts the string “3gpp-gba” into the User-Agent field within the HTTP header to indicate that it supports GBA authentication (see Figure 2). The NAF will verify that the client request contains an HTTP Authorization header carrying valid NAF session keys derived from an earlier 3GPP authentication. While this cannot be the case with the first request, it does include the indication of GBA support, so the NAF will initiate a HTTP Digest authentication by responding with “HTTP 401 Unauthorized” message. The response also includes within the WWW-Authenticate header the URL of the BSF to be used.

The UE recognizes from the WWW-Authenticate header that it is requested to supply NAF-specific keys derived from an authentication against the BSF. Since it has not yet authenticated against the BSF it initiates the ISIM/AKA authentication by sending a HTTP Get request to the BSF including – in addition to other parameters - its IMS Private Identity (IMPI) within the Authorization header.

The BSF extracts the IMPI from the request and fetches a set of authentication vectors (AVs) for that identity from the HSS. It selects one of the received AVs and continues the AKA protocol by sending back the user challenge within the WWW-Authenticate header of a “HTTP 401 Unauthorized” response. The UE checks the correctness of the challenge calculates the corresponding response parameters by means of the ISIM application and sends them to the BSF within the Authorization header of the second HTTP Get request.

The BSF will now compare the response with the expected values and will eventually derive a session key (Ks-NAF) and store it together with the self-generated BSF-Transaction Identifier (BTID).

It will then send back the B-TID and a key lifetime parameter to the UE within the “HTTP 200 OK” response.

The UE will now also derive the Ks-NAF and respond to the initial MD5 challenge of the NAF by using the B-TID as the username and the Ks-NAF as the password. When the NAF receives the MD5 response, it will fetch the Ks-NAF that belongs to the given B-TID from the BSF via the Zn interface. It verifies the MD5 response of the UE and finally responds to the initial request of the UE with the requested content. Succeeding requests of the UE will include the MD5 authorization header elements, so that the NAF will identify the UE as authenticated until the key lifetime expires.

A.2.1.1 SAML & GBA

We will briefly describe in figure 3 the bootstrapping procedure in combination with the HTTP Digest authentication option illustrated in Figure 2. Our setup co-locates the IdP and NAF. Please note that other options are possible especially the co-location of IdP and 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 annex of this paper or the Technical Specification of [3GPP TR 33.220], [3GPP TR 33.980], or SAML2 Discovery [SAML2 Profiles].

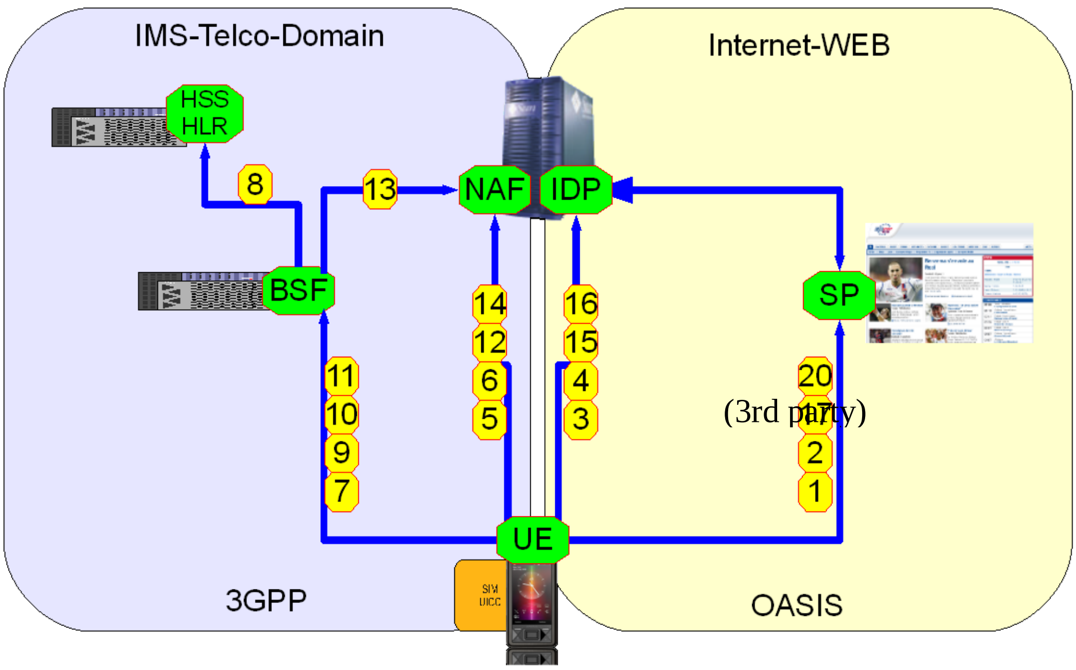

Figure 11: GBA & SAML Inter-working

A.2.1.1.1 SAML Part 1

1. The UE contacts the SP to gain access to a service provided by the SP by sending an HTTP-Request. This request contains the GBA-based authentication support indication (“User Agent: 3ggb-gba”).
2. The SP obtains the identity provider and sends a redirect HTTP Response with <lib:AuthnRequest> to UE according to [SAML2 Core].
3. The UE in turn contacts the IdP under the URL given in the Location header field and the UE must access the NAF/IdP URL with an HTTP Request with <lib:AuthnRequest> information (including “User Agent: 3ggb-gba”). If a bootstrapped security association between UE and IdP/NAF exists, then UE and IdP/NAF share the keys to protect reference point U_a and the UE possesses all necessary data to perform HTTP Digest Authentication from previous messages. In this case step 3 is combined with the request in step 5, and step 4 is omitted.
4. If the UE is not yet authenticated with the IdP, then the IdP sends a HTTP response with ‘Unauthorized’ status code to the UE as defined in [3GPP-TS33.220]. This will trigger the UE to do the bootstrapping procedure over with the BSF. This is transparent to the SP.

A.2.1.1.2 AKA-Part

5. When a GBA-enabled UE initially tries to access a GBA-protected service via the NAF or AP, it inserts the string “3gpp-gba” into the User-Agent field within the HTTP header to indicate that it supports GBA authentication. The NAF will verify that the client request contains an HTTP Authorization header carrying valid NAF session keys derived from an earlier 3GPP authentication. While this cannot be the case with the first request, it does include the indication of GBA support.
6. The NAF will initiate a HTTP Digest authentication by responding with “HTTP 401 Unauthorized” message. The response also includes the BSF to be used.
7. The UE recognizes that it is requested to supply NAF-specific keys derived from an authentication against the BSF. Since it has not yet authenticated against the BSF it initiates the ISIM/AKA authentication by sending a HTTP Get request to the BSF including – in addition to other parameters - its IMS Private Identity (IMPI) within the Authorization header.
8. The BSF extracts the IMPI from the request and fetches a set of authentication vectors (AVs) for that identity from the HSS.
9. It selects one of the received AVs and continues the AKA protocol by sending back the user challenge within the “HTTP 401 Unauthorized” response.
10. The UE checks the correctness of the challenge calculates the corresponding response parameters by means of the ISIM application and sends them to the BSF.

The BSF will now compare the response with the expected values and will eventually derive a session key (Ks-NAF) and store it together with the self-generated BSF-Transaction Identifier (BTID).

11. It will then send back the B-TID and a key lifetime parameter to the UE within the “HTTP 200 OK” response.
12. The UE will now also derive the Ks-NAF and respond to the initial MD5 challenge of the NAF by using the B-TID as the username and the Ks-NAF as the password.
13. When the NAF receives the MD5 response, it will fetch the Ks-NAF that belongs to the given B-TID from the BSF.
14. The NAF verifies the MD5 response of the UE and finally responds to the initial request of the UE with the requested content. Succeeding requests of the UE will include the MD5 authorization header elements, so that the NAF will identify the UE as authenticated until the key lifetime expires.

A.2.1.1.3 SAML Part 2

15. The UE answers with a HTTP GET request with Authorization header field containing as a username the B-TID and as a password the Ks_(ext/int)_NAF. The IdP/NAF can request the credentials and related material, if it does not have it stored already.
16. The IdP responds with a SAML artefact in the HTTP Response redirect URL.
17. The UE contacts the SP again using this URL and HTTP Request with the SAML artefact.
18. The SP sends an HTTP Request with the SAML artefact to the IdP. The request contains a <samlp:Request> SOAP Request message to the identity provider’s SOAP endpoint, requesting the assertion by providing the SAML assertion artefact in the <samlp:AssertionArtefact> element as described in [SAML2 Core].
19. The IdP can now construct or find the requested assertion and responds with a <samlp:Response> SOAP Response message with the requested <saml:Assertion> or a status code. The IdP sends the authentication assertion that corresponds to the artefact.
20. The SP processes the SOAP message with the <saml:Assertion> returned in the <samlp:Response>, verifies the signature on the <saml:Assertion> and processes the message and then answers with a HTTP Response.

A.3 References

[MS-CSWeb	http://cardspace.netfx3.com/; http://msdn2.microsoft.com/de-de/winfx/Aa663320.aspx
3GPP TR 33.980	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); http://www.3gpp.org/ftp/Specs/html-info/33980.htm
3GPP-TS24.109	3GPP TS 24.109; "Bootstrapping Interface (Ub) and Network Application Function Interface (Ua) – Protocol Details"; V7.5.0; December 2006
3GPP-TS29.109	3GPP TS 29.109; "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3"; V7.7.0; September 2007
3GPP-TS33.102	3GPP TS 33.102; "3G Security – Security architecture"; V7.1.0; December 2006
3GPP-TS33.220	3GPP TS 33.220; "Generic Authentication Architecture (GAA) – Generic Bootstrapping Architecture "; V7.6.0; December 2006
3GPP-TS33.919	3GPP TS 33.919; "Generic Authentication Architecture (GAA) – System Description"; V7.2.0; March 2007
LA-ID-FF])	Liberty Alliance Project; "Liberty ID-FF Architecture Overview"; Version 1.2; (draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf)
SAML2 Profiles	Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005
SAML2 Core	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005 http://docs.oasis-open.org/security/saml/v2.0/

B. Technical Annex "Authentication context sharing between GBA and Web Client applications on UEs"

As described in “GBA & ID FF Interworking” [3GPP-TS33.980]., the reuse of the network authentication for web-based services is a valuable asset of a Telco and an important step to converged services.

3GPP GBA Bootstrapping procedure with the enhancement of Interworking of SAML2 is being specified, while it assumes the tight relationship between GBA Client and Web Client applications.

This (informative) chapter describes the possible ways to use the secure SIM/USIM/ISIM based authentication mechanism for a wider set of applications.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216647.

B.1 Injection of Authentication context in a form of Cookie to Applications

In the case of “Using the GBA to access the 3GPP HSS as identity provider within the Liberty Alliance ID-FF” as identified in “GBA & ID FF Interworking” [3GPP-TS33.980]., for Interworking of Liberty Alliance ID-FF with 3GPP GBA, GBA Client and Web Client are considered as tightly coupled and sharing the authentication context . However, there is a strong demand for the use of IMS based authentication to a wider range of applications. Especially the support for the existing Web Clients (so-called web browsers) is desired.

To allow Web applications to start LA ID-FF based access to SP upon a successful GBA authentication, it is necessary to activate the cookie information conveying the authentication context, which should be provided to the IdP when redirected to retrieve the Authentication Assertion. The challenge here is how to activate such cookie information in generic web browsers. Two options for providing the Web applications with the cookie information are described in this document:

1. Passing the cookie information directly from GBA Client to Web Client application
2. Providing the one-time URL to access to retrieve the cookie information from IdP through network.

Option 1 might be preferable as the transfer can be locally done between two Clients. However, not all the browsers expose such a functionality for plug-in to insert cookie information offline. In that case, it is necessary to let a browser access to the IdP to activate the cookie information to share the authentication context as Option 2.

Note in both cases, only the communication between servers and clients are based on the well defined standardized procedure except the data returned from GBA servers, while the communication between GBA Client and Web Client application is rather abstract concept and the procedure shows one of the potential examples to achieve direct passing of the cookie information and injection of the cookie information by forcing the network access respectively.

Note in Figure 12 and Figure 13, IdP is described as a separate entity for the convenience of description, while this procedure allows the deployments cases where the IdP collocates either with BSF or NAF.

B.1.1 Direct transfer of the cookie information between GBA Client and Web Client

This option is to let the Web Client application to get the cookie information directly from GBA Client belonging to the same user. GBA Client retrieves the cookie information upon a successful GBA authentication and passes it to the Web Client. Figure 12 shows the detail procedure:

1. GBA Client performs the authentication.
2. Along the NAF authentication process as a part of GBA authentication, authentication context is shared with IdP.
3. IdP creates cookie information and returns it to NAF as a GBA server component.
4. Upon a successful GBA authentication, the cookie information will be returned to GBA Client to be shared with Web Client.
5. GBA Client registers this cookie information at Cookie registry.
6. When web client such as browser is invoked by the user, it access to the cookie registry to fetch the cookie information for the IdP domain.
7. This cookie information will be provided in a request whenever the access is redirected to the IdP.

Note Figure 13 shows the process with a client-side example where the component called Cookie registry stores the cookie data GBA Client retrieves which then will be fetched by the Web Client such as browser to be injected in its cookie manager upon a starting up process.

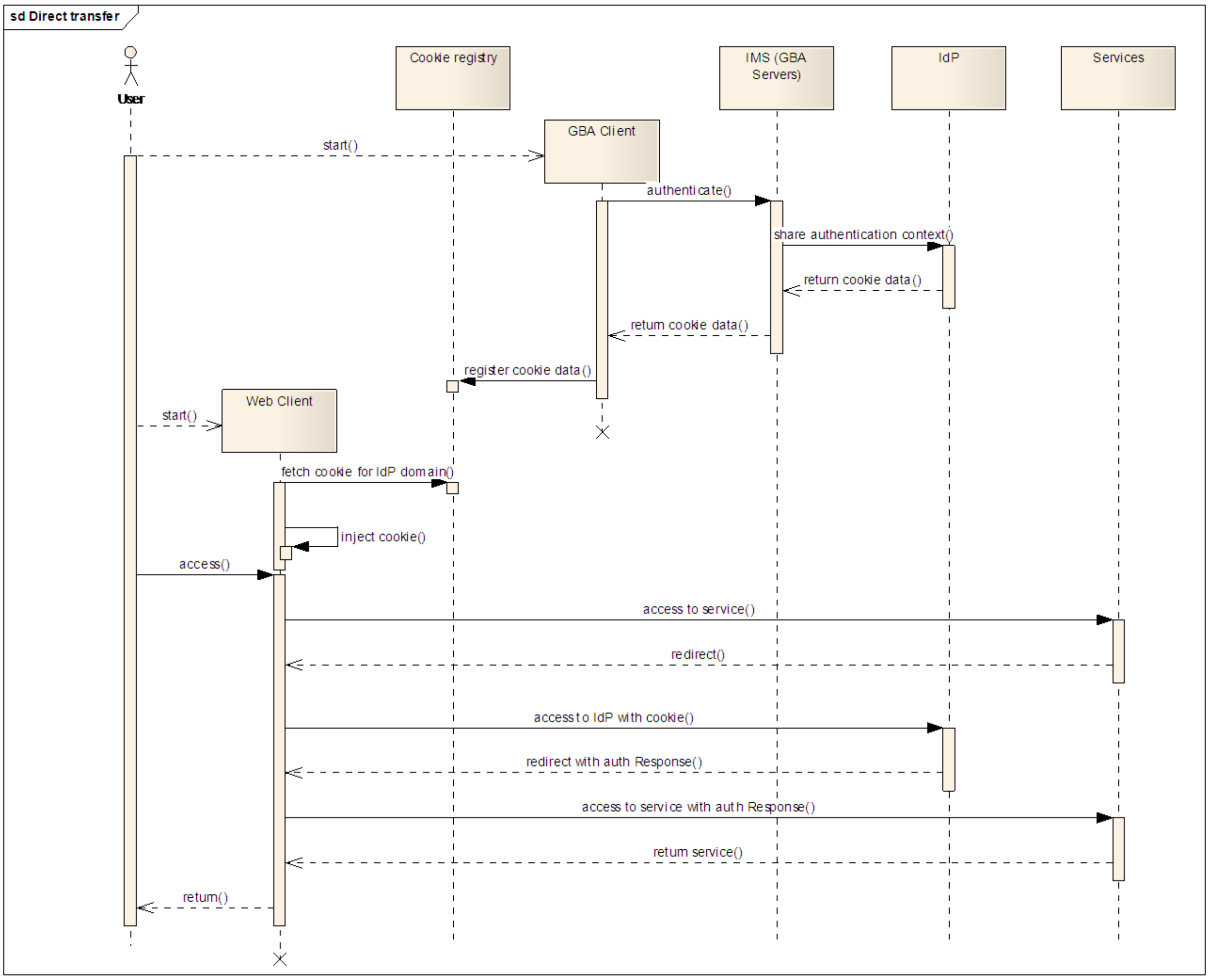

Figure 12 Direct transfer of cookie between GBA and Web clients

B.1.2 Cookie information retrieval from Identity Provider through Network

This option is to pass the Web Client application a temporal URI under the Identity Provider domain to fetch the cookie information through. This URI is a dedicated URI to a specific successful authentication and only valid for a certain period after the successful authentication.

GBA Client retrieves the URL upon a successful GBA authentication and passes it to the Web Client, which will then access to the URL and be injected the cookie information subsequently. Figure 13 shows the detail procedure:

1. Client Agent initiates GBA Client to perform the authentication.
2. Along the NAF authentication process as a part of GBA authentication, authentication context is shared with IdP.
3. IdP creates a temporal URI and returns it to NAF as a GBA server component.
4. Upon a successful GBA authentication, the URI will be return to GBA Client to be shared with Web Client.
5. GBA Client returns this URL to Client Agent which then invokes Web Client such as browser with this URI.

6. Web Client accesses to the URI under the IdP domain and fetch the cookie registry to fetch the cookie information for the IdP domain and store it its cookie manager.
7. This cookie information will be provided in a request whenever the access is redirected to the IdP.

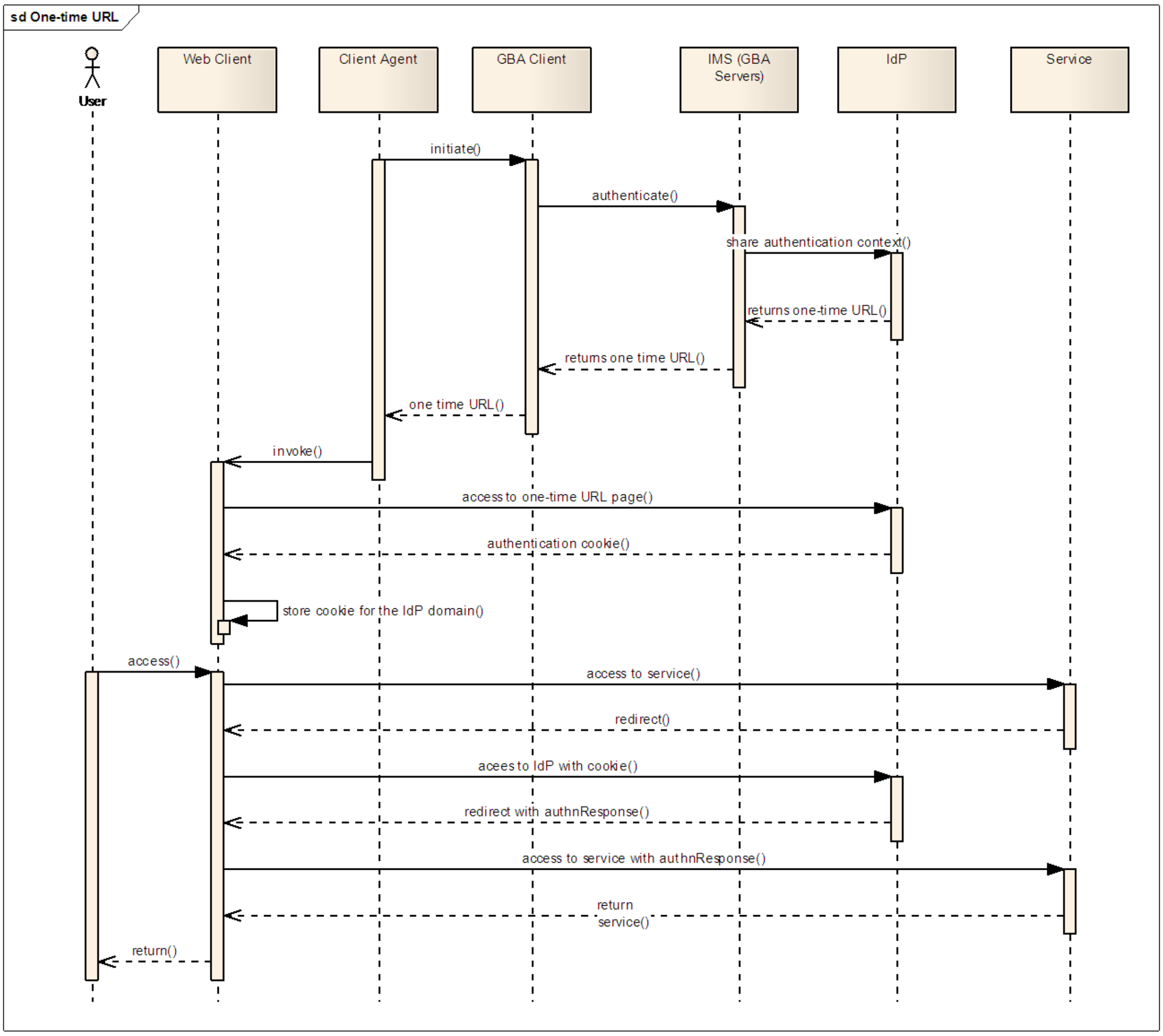

Figure 13: Cookie retrieval from Identity Provider

B.2 Consideration on Client deployment

As the procedure described in this document does not assume tight coupling of GBA Client and Web Client, Web Client applications can be deployed on different devices than UE where GBA Client is installed. Examples of those devices are PC, TV, etc. nearby the UE, which belong to the same user as UE. Obviously, the interaction between Clients must be secured. The communication methods which allow the interaction only in certain proximity such as RFID can be considered as one of the ways to ensure the security.

B.3 The relationship with ID-WSF Advanced Client

ID-WSF Advanced Client specifications define the provisioning mechanism. As this document focuses on the use of 3GPP GBA authentication context, the provisioning over the network as defined in ID-WSF Advance Client is out of scope. However, in the case of Option 1, the direct transfer of cookie information GBA Client to Web Client via Cookie registry, the communication among clients may be able to implement as a special case of the communication between RegApp and PM in ID-WSF Advanced Client. Cookie registry can be considered as one of the functionalities of PM, which is activated by GBA Client as one of the RegApps, and then is got status by the enhanced Web Client as another RegApp.

The necessity of such mapping as well as the preferable way of actual implementation is out of scope of this document.

B.4 Conclusion

The GBA is an authentication framework for 3G networks while Liberty Alliance ID-FF is a framework for Web-based applications. The interworking of these two frameworks is already being specified but the enhancement is necessary to support a wider set of Web applications which may not be tightly coupled with the GBA client.

In this document, the options for mechanisms to transfer the authentication context in a form of cookie are described. These mechanisms, together with additional secure data transfer mechanisms among on one or more devices belonging to the same user will enable a wider scope of applications to get the benefit of secure authentication mechanism provided GBA authentication.

C. Technical Annex : "SIP/SAML Messaging"

C.1 Overview

SAML is a set of protocol specifications that provide, among other things, seamless Single Sign-On (SSO) in a distributed environment where a user wishes to log into multiple Service Providers (SPs). In particular, once a user has authenticated towards a trusted entity called the IdP, the SAML protocols enable the IdP and the SPs to exchange information about the user's authentication status at the IdP in a secure manner and in a way that takes into account the user's privacy. Moreover, the SAML protocols enable the SPs and the IdP to exchange information about the user in the form of attributes. This feature is useful in the context of identity management systems that perform such attribute exchanges in an automated way, while enabling the user to exercise control over the dissemination of his personal information.

However, the SAML protocols are not self-contained in the sense that they require a transport mechanism. In particular, SAML messages need to be conveyed from one party to the other by some underlying transport protocol. The encoding of SAML messages in such transport protocols is called a SAML binding; multiple such bindings have been specified in the past. Examples are the HTTP REDIRECT binding, the HTTP POST binding, and the SOAP binding [SAMLBINDINGS]. To date, a SAML binding for SIP is still missing.

With each newly specified SAML profile and binding, the number and the diversity of applications and services that can interoperate with any given SAML-based IdP increases. This adds value to the overall system, because it enables the user to log into a larger and more diverse set of services in a seamless manner. Moreover, the number of services that can query the user's attributes from the IdP increases, resulting in a potentially more personalized experience for the user.

This section introduces the SIP/SAML profile. This profile can be used in a variety of situations, including the following.

- The authentication provider (IdP) is a SIP proxy or an IMS entity, and it is necessary to convey authentication or attribute information to other SIP or IMS entities.
- The authentication provider (IdP) is a SIP proxy or an IMS entity, and it is necessary to convey authentication or attribute information to relying web services over HTTP. In this case, the SAML assertions may travel over SIP until the use equipment or some intermediate proxy, and are there encapsulated into HTTP messages.
- The authentication provider (IdP) is a web-based service provider, and it is necessary to convey authentication or attribute information to some SIP or IMS entity. In this case, the SAML assertions may travel over HTTP towards the user equipment or some intermediate proxy, and are there encapsulated into SIP messages.

In the following, we outline two SIP SAML profiles, each with slightly different properties, but both consistent with existing HTTP SAML profiles.

C.2 Logical View

C.2.1 Domain View

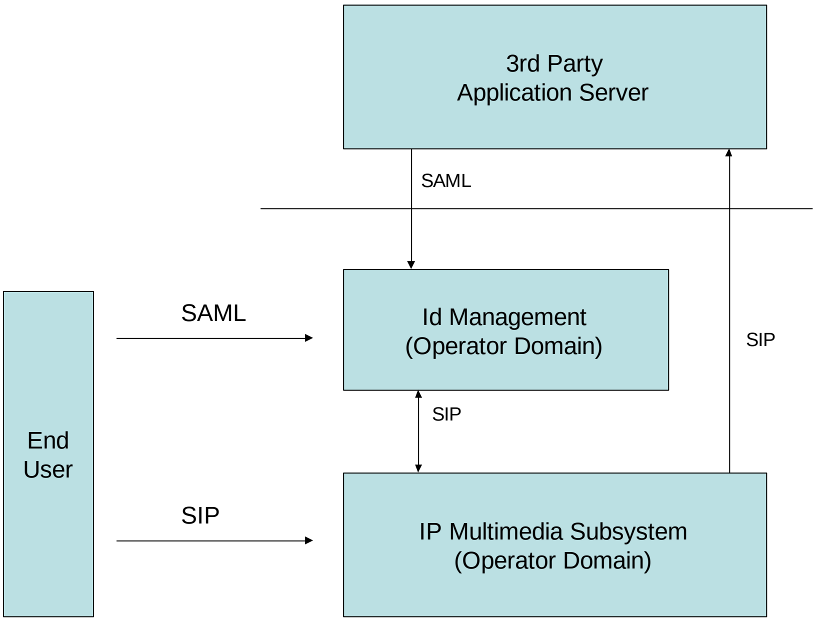

Figure 14: Domain View

Note: the SAML interface between the end-user and the Id. Management system is included to complete the picture with existing interfaces and protocols, although this interface is not used in the scenarios presented later.

- **3rd Party App. Server:** The SP is hosted outside the operator's domain and the trust relationship with the operator is, generally, weak. This is the general broader scenarios, although it can also be applied when the App. Server belongs to the operator administrative domain, and the trust relationship is higher.
- **Id Management:** It is deployed inside the operator's domain and it handles the Identity Federation with other participants in the operator's Circle of Trust, and it offers functionality such as Single Sign-On (based on SAML) and Identity Services (based on ID-WSF protocol).
- **IP Multimedia Subsystem:** Contains the operator's infrastructure to offer IMS Services, including the IMS core network elements such as HSS.

C.3 SIP/SAML Direct Variant

In this section, the Direct Variant of the SIP/SAML profile is specified. In the following, UA denotes the user agent (client), SP denotes a SIP Proxy, and Identity Provider denotes a SAML-based Identity Provider. This specification relies on a new SIP header, called the `SAML- Endpoint (SAML-EP)' header. This header contains a URI endpoint pointing to the user's SAML-based Identity Provider.

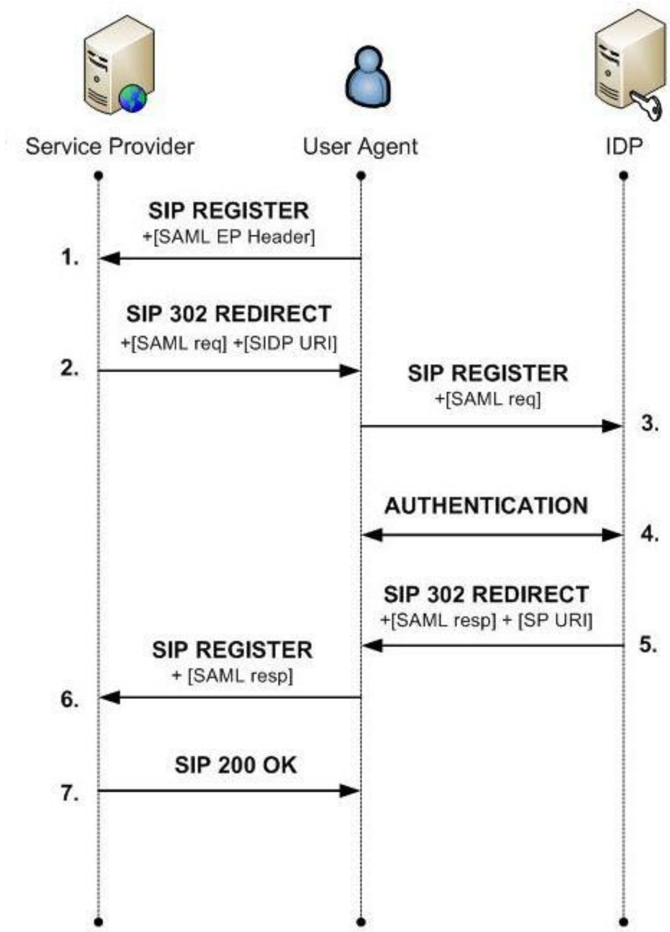

Figure 15: Direct Variant of the SIP/SAML Profile

Figure 15 shows the direct variant of the SAML/SIP profile in full i.e. where the user authenticates himself at the Identity Provider for the first time. It is assumed that all communication takes place over SIP; of course re-encapsulation over HTTP is possible (but not shown). The figure shows individual steps that occur during the protocol execution. With the exception of *authentication*, all the steps uniquely correspond to a particular message that is exchanged in the corresponding step. In the following, we say `message X' in order to refer to the message that is exchanged in step X of the protocol.

First, the End-User constructs a SIP REGISTER message and sends it to the Service Provider (message 1). This message MUST contain one or more SAML-EP headers, where the value of each SAML-EP header MUST be one or more URIs. All the indicated URIs MUST belong to some SAML-based Identity Provider that is able to consume SIP REGISTER messages conforming to the format of message 3. The population of the SAML-EP header values is the responsibility of the End-User. If multiple SAML-EP header values are present in message 1 (either in the same or in multiple SAML-EP headers), then each URI within a SAML-EP header value MUST refer to a different Identity Provider. Also, each URI within a SAML-EP header value MUST refer to an Identity Provider where the user maintains an active account. However, there is no requirement to include more than Identity Provider URI, even if the user maintains accounts at multiple Identity Providers. Moreover, the order of the URIs within SAML-EP header values SHOULD reflect the user's preferences, most preferred first. That is, if the user prefers to be authenticated by Identity Provider A in preference to Identity Provider B, then the URI referring to Identity Provider A SHOULD be included in a SAML-EP header before the URI referring to Identity Provider B.

The following two possibilities exist when message 1 is received by the Service Provider. Case 1: the Service Provider does not support the SIP/SAML profile specified in this document. In this case, the SAML-EP header(s) are ignored, and the Service Provider responds 'normally', i.e. as in standard SIP. The End-User MUST be able to correctly handle a message conforming to standard SIP (instead of message 2 in Figure 15) as a response to message 1. Case 2: the Service Provider supports the SIP/SAML profile. In this case, it MUST examine the SAML-EP headers and check whether or not an agreement exists with at least one of the indicated Identity Providers. If an agreement exists with at least one of them, then it MUST pick one of those with whom an agreement exists; the one it selects is denoted by SIDP. The Service Provider SHOULD select the Identity Provider that corresponds to the first URI within any SAML-EP header with whom an agreement exists. If no agreement consists with any of the IdPs then the Service Provider MUST act as if it does not support the SIP/SAML profile specified in this document, i.e. respond with a message conforming to 'standard' SIP.

After the SIDP has been selected, the Service Provider MUST decide with which SAML/ SIP profile it would like to proceed. This decision MAY be based on a policy or similar criteria. If the 'SIP Artifact' profile is selected, then the remainder of the processing and the protocol is as described in the next section. Otherwise, i.e. if the 'direct' profile is selected, then processing continues as follows.

Message 2 is constructed as follows. The Service Provider constructs a SIP 302 REDIRECT message where the value of the 'Contact' header is equal to the value of the SAML-EP header (from message 1) that corresponds to the SIDP. This value is denoted by SIDP URI in Figure 7. Moreover, message 2 MUST contain a SAML Request, which MUST be constructed according to [SAML].

Upon reception of message 2, the End-User SHOULD check that the SIDP URI indicated in the 'Connect' header is one of those proposed in message 1. If this is not the case, then the End-User MAY abort the protocol execution at this point. It also MAY inform the user about the inconsistency, and it MAY ask for the user's permission on whether to proceed with the given SIDP URI. It is RECOMMENDED that the End-User does not proceed with the protocol execution if the indicated SIDP URI is not one of the ones proposed in message 1, unless the user explicitly allows the protocol execution to continue.

After reception of message 2, the End-User MUST decide how to proceed in trying to obtain a SAML Response that matches the Service Provider's SAML Request in message 2. Multiple possibilities MAY exist for this, and this specification does not impose the End-User to use any particular method. However, if the End-User decides to continue with the `Direct Variant' of the SIP/SAML profile, then it MUST proceed as follows.

It constructs message 3 as a new SIP REGISTER message, which is sent to the SIDP URI. The message contains the SAML Request from message 2. Note that, since message 3 is sent to an Identity Provider (which may or may not be a SIP Proxy), its purpose it not to register at a SIP Proxy; its purpose is to trigger authentication at the Identity Provider.

In step 4 of the protocol, Identity Provider authenticates the user. This may involve multiple messages between the End-User and the Identity Provider. This specification does not impose any particular authentication mechanism. However, in order to guarantee minimal interoperability, the standard SIP user authentication mechanism (Digest Authentication, see section 22 of [RFC3261]) MUST be implemented at both the Identity Provider and the End-User. However, whether or not the Identity Provider will choose this method or some other method is dependent on policy.

After the authentication of the user towards the Identity Provider, the Identity Provider constructs message 5. This is a SIP 302 REDIRECT message where the 'Contact' header MUST contain a value that is extracted from the SAML request in 3, according to [SAML]. According to [SAML], the SAML Response contains the description of an authentication context if the user's authentication in step 4 has been successful. If this is the case, the authentication context in the SAML Response MUST describe the user's authentication context that resulted from the authentication in step 4.

Finally, the End-User constructs a new SIP REGISTER message and sends this to the Service Provider in step 6. This SIP REGISTER message MUST contain the SAML Response from message 5. Upon reception of that message, the Service Provider MUST examine the SAML Response according to [SAML]. If the Service Provider is satisfied, then the user is recorded as 'registered' in the SIP Proxy, and the remaining processing continues according to standard SIP [RFC3261].

C.4 SIP/SAML Artifact Variant

This section specifies the SIP-Artifact Variant of the SIP/SAML Profile. The main difference between the SIP-Artifact Variant and the Direct Variant is that, in the SIP-Artifact Profile, the End-User cannot see the SAML messages that are exchanged between the Service Provider and the Identity Provider. Instead, the Service Provider and the Identity Provider exchange SAML messages directly. Special identifiers that identify individual SAML messages, called `SAML Artifacts' are tunneled through the End-User.

Figure 16 shows the SIP-Artifact variant of the SAML/SIP profile in full i.e. where the user authenticates himself at the Identity Provider for the first time. The figure shows individual steps that occur during the protocol execution. With the exception of steps 4, 5, and 8 all the steps uniquely correspond to a particular message that is exchanged in the corresponding step. In the following, we say `message X' in order to refer to the message that is exchanged in step X of the protocol.

First, the End-User constructs a SIP REGISTER message and sends it to the Service Provider (message 1). This message is constructed in a manner identical to the construction of the first message in the `direct' variant, as specified in the section above. The behavior of the Service Provider after having received message 1 is identical to the behavior specified for the `direct' variant in the section above, up to the point where the Service Provider decides which variant to use. If the Service Provider decides to use the `Artifact' variant, the processing is as follows.

The Service Provider MUST construct a SAML Artifact pointing to a SAML Request message for consumption by the SIDP, according to [SAML]. Message 2 is then constructed as a SIP 302 REDIRECT message, where the `Contact' header MUST take as value the URI indicated by the SAML- Endpoint header (from message 1) that corresponds to the SIDP, modified as follows.

Moreover, message 2 MUST contain exactly one SAML-EP header, where the value is the URI at which the Service Provider will accept a SAML Artifact Resolution request from the SIDP.

Upon reception of message 2, the End-User SHOULD check that the SIDP URI indicated in the 'Connect' header is one of those proposed in message 1. If this is not the case, then the End-User MAY abort the protocol execution at this point. It also MAY inform the user about the inconsistency, and it MAY ask for the user's permission on whether to proceed with the given SIDP URI. It is RECOMMENDED that the End-User does not proceed with the protocol execution if the indicated SIDP URI is does not correspond to any of those that were proposed in message 1, unless the user explicitly allows the protocol execution to continue.

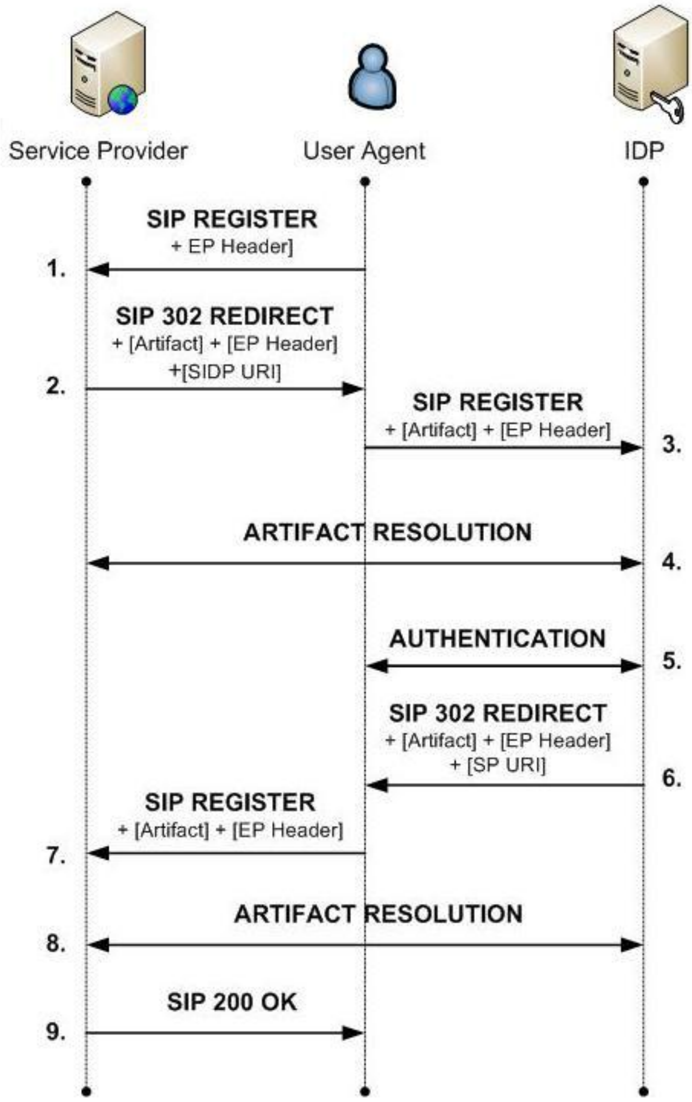

Figure 16: Artifact Variant of the SIP/SAML Profile

The End-User constructs message 3 as a new SIP REGISTER message, which is sent to the SIDP URI. Message 3 MUST contain a single SAML-EP header, with a value identical to the value of the SAML-EP header from message 2. Since message 3 is sent to an Identity Provider (which is NOT a SIP Proxy), its purpose it not to register at a SIP Proxy; its purpose is to trigger authentication at the Identity Provider.

In step 4 of the protocol, the Identity Provider resolves the SAML Artifact found in the query string of the URI from message 3, into a SAML Request message. This is done by means of the Artifact Resolution protocol specified in [SAMLART]. The SAML Endpoint that the Identity Provider uses for initiating the exchange is the one indicated in the SAML-EP header in message 3.

If the SAML Artifact has successfully been resolved into a SAML Request message, in step 5 of the protocol the Identity Provider authenticates the user. This corresponds to step 4 in the 'direct' variant specified in the previous section, and the requirements concerning this steps are identical to the requirements in the 'direct' variant.

After the authentication of the user towards the Identity Provider, the Identity Provider MUST construct a SAML Artifact pointing to a SAML Response message for consumption by the Service Provider, according to [SAML]. Message 6 is then constructed as a SIP 302 REDIRECT message, where the `Contact' header MUST take the value of an specific URI that is extracted from the SAML request in 3, according to [SAML], modified as follows.

The SAML Response to which the SAML Artifact points, MUST contain the description of an authentication context if the user's authentication in step 5 has been successful. If this is the case, the authentication context in the SAML Response MUST describe the user's authentication context that resulted from the authentication in step 5.

Moreover, message 6 MUST contain exactly one SAML-Endpoint header, where the value is the URI at which the Identity Provider will accept a SAML Artifact Resolution request from the Service Provider.

Upon reception of message 6, the End-User constructs message 7 as a new SIP REGISTER message. Message 7 MUST contain exactly one SAML-Endpoint header, where the value is identical to the value of the SAML- Endpoint header from message 6. Message 7 is then sent to the URI indicated in the 'Contact' header of message 6.

In step 8 of the protocol, the Identity Provider resolves the SAML Artifact found in the query string of the URI from message 7, into a SAML Response message. This is done by means of the Artifact Resolution protocol specified in [SAMLART]. The SAML Endpoint that the Service Provider uses for initiating the exchange is the one indicated in the SAML-Endpoint header of message 7.

C.5 SIP/SAML Interaction for Outgoing Calls

User-A tries to establish an outgoing call towards an Application Server (User-to-Content). The destination Application Server can be hosted in the same network as user A, or maybe it could be hosted in another IMS network.
In any case, the routing of the call could be done through direct interaction between the S-CSCF in the home network and the Application Server in the destination network (this could be done if the S-CSCF knows how to address the App. Server based, for instance, in a DNS lookup of the realm part of the SIP-request URI), or it can be done though the usual IMS routing mechanisms.
In the following diagram, the basic sequence flow is shown; the I-CSCF in the destination network is not shown for simplicity, but it does not play a special role (as it happens in the case of the symmetrical case where the Application Server calls the user A). In turn, the I-CSCF in the destination network can contact the Application Server through an S-CSCF or directly, if it knows how to route the SIP messages (maybe by means of the DNS resolution of the domain name of the PSI).

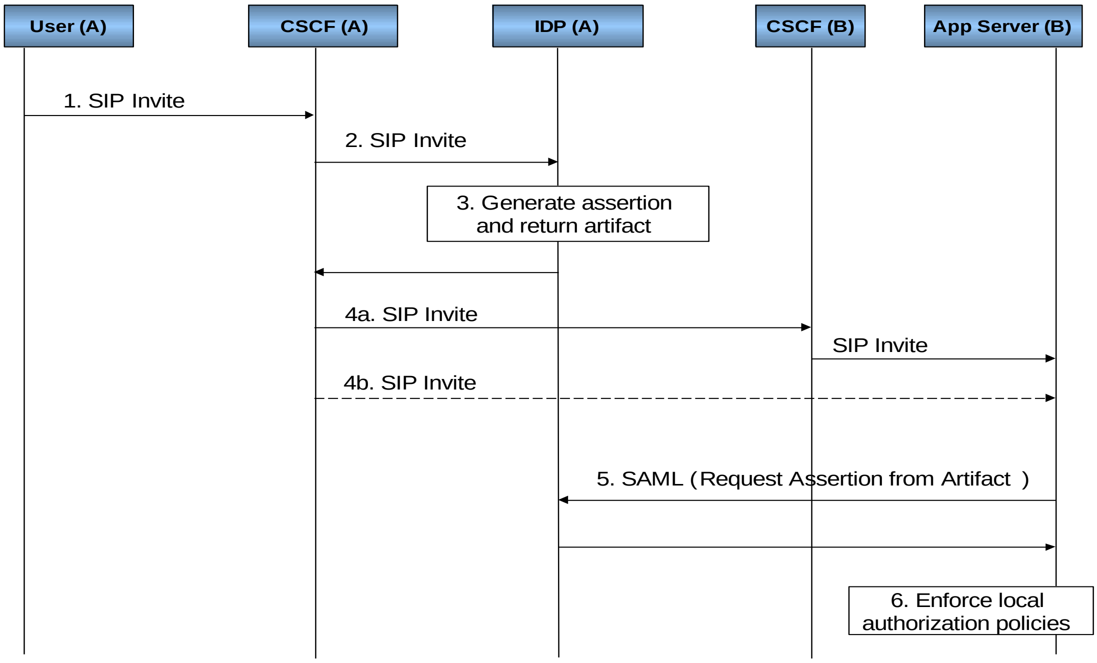

Figure 17: SIP/SAML Interaction Flow for Outgoing Call

A typical use case interaction sequence would be as follows:

1. The user agent sends a session initiation request by sending a SIP INVITE message to the call server (CSCF) in his home network. The message is targeted towards an application server in a remote network, but the initial message is actually sent to the call server in the user's home network. The message is first sent to the P-CSCF (in case the user is roaming in a visited network), and then sent towards the I-CSCF, which in turn locates the appropriate S-CSCF.

   Example:

   INVITE
   sip:serviceB@example.com
   SIP/2.0
   Via: SIP/2.0/UDP 10.20.30.40:5060
   From: UserA <sip:userA@example.com>;tag=589304
   To: ServiceB <sip:serviceB@example.com>
   Call-ID: 8204589102@example.com
   CSeq: 1 INVITE
   Contact: <sip:userA@10.20.30.40>
   Content-Type: application/sdp
   Content-Length: …

2. The S-CSCF checks that there is a trigger defined for those messages directed to that specific application server, and therefore, sends the message to the Id. Server, via the ISC interface. In this scenario, the Id. Server is acting as another application server, from the point of view of the S-CSCF.

   It must be noted that if there are several Application Servers connected with the S-CSCF through the ISC interface, it must be necessary to process the different triggers in an appropriate order because, once the public identities are converted to federated shared identities, they will become useless to the remaining Application Servers. Therefore, the translation of user identities to federated alias must be the last thing to be done before the SIP message leaves the operator's home network.

3. The Id. Sever generates a SAML assertion according to the security and identity information regarding user A. This assertion may contain authentication information, user attributes, specific access control and authorization information, etc… The assertion is referenced by a small piece of data called "artifact". Either the full assertion or the artifact will be returned to the CSCF inserted in a specific header of the SIP message (for instance, in the "Identity" header).

   It must be pointed out that this behavior does not follow the traditional Request-Response procedures defined for SAML, since the assertion are generated by the Id. Server without being requested (i.e., there is not an incoming SAML Authentication Request message to trigger the generation of the SAML assertion). If anything, it could resemble to the behavior of the Unsolicited Authentication Request mechanism.

   Note that the assertion will include the identity of the user A, but properly qualified for the targeted Application Server. This means that, if user A holds a federated identity relationship with that Application Server, then the shared federated identity (alias) will be included as the user identity towards the Application Server.

   Before returning the SIP message to the S-CSCF, the alias must be properly qualified with a domain name associated to a Public Service Identifier (PSI) associated with the Identity Server itself. This must be done like this to allow the I-CSCF to process an eventual incoming call received from the remote Application Server, as will be explained in the next use case.

   In case the identity token employed in the Identity header is an artifact, the PSI domain name of the Identity Server is not needed, since the artifact itself includes the Id. of the issuer (the Id. Server).

   Note that the artifact must be appropriately formatted when it is included in the Identity header, to conform to the "URI-style" content (i.e., special chars must be formatted with the "%xx" notation).

   Example:

INVITE
sip:serviceB@example.com
SIP/2.0
Via: SIP/2.0/UDP 10.20.30.40:5060
From: “Anonymous”
<sip:anonymous@anonymous.invalid>;tag=589304
To: “ServiceB” <sip:serviceB@example.com>
Identity:
AAQAADWNEw5VT47wcO4zX%2FiEzMmFQvGknDfws2ZtqSG
dkNSbsW1cmVR0bzU%3D
Call-ID: 8204589102@example.com
CSeq: 1 INVITE
~~Contact: <sip:UserA@10.20.30.40>~~ (Removed)
Content-Type: application/sdp
Content-Length: …

4. The CSCF receives the modified SIP message and forwards it to the destination application server. This server could be located in the same network as the Id. Server and CSCF, or it could be located in a remote IMS network. Therefore, the Application Server can be contacted directly from the CSCF (if the CSCF knows how to address it), or maybe it is necessary to contact first the I/S-CSCF’s of the remote network, in order to reach the Application Server. Both alternatives are considered as feasible.

5. When the SIP INVITE message reaches the Application Server, it extracts the identity information from the specific SIP header (“Identity”), and if the identity is found to be in the format of a SAML artifact, it must retrieve the original SAML assertion generated previously by the Id. Server. To do that, the Application Server issues a SAML Request (using for instance a SOAP request) to retrieve the full assertion. The SOAP end-point of the Id. Server must be known in advance by the Application Server and this is typically configuration data exchanged out-of-band.

   Note that the assertion could have been fully delivered in the SIP message, and in this case, the App. Server does not need to contact the Identity Server to resolve the artifact into the full assertion.

   Example:

   Request

POST /SAML/Artifact/Resolve HTTP/1.1
Host: IdentityProvider.com
Content-Type: text/xml
Content-Length: …
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope

```
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Body>
<samlp:ArtifactResolve
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_6c3a4f8b9c2d" Version="2.0"
IssueInstant="2004-01-21T19:00:49Z">
<Issuer>https://serviceB.example.com/SAML</Issuer>
<Artifact>
AAQAADWNEw5VT47wcO4zX/iEzMmFQvGknDfws2ZtqSGdkN
SbsW1cmVR0bzU=
</Artifact>
</samlp:ArtifactResolve>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Response

```
HTTP/1.1 200 OK
Date: 21 Jan 2004 07:00:49 GMT
Content-Type: text/xml
Content-Length: …
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Body>
<samlp:ArtifactResponse
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_FQvGknDfws2Z" Version="2.0"
InResponseTo="_6c3a4f8b9c2d"
IssueInstant="2004-01-21T19:00:49Z">
<Issuer>https://ids.example.com/</Issuer>
<samlp:Status>
<samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<samlp:AuthnResponse ID="d2b7c388cec36fa7c39c28fd298644a8"
IssueInstant="2004-01-21T19:00:49Z"
Version="2.0">
<Issuer>https://IdentityProvider.com/SAML</Issuer>
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameidformat:
persistent">005a06e0-004005b13a2b@ids.example.com</NameID>

(…)

</samlp:AuthnResponse>
</samlp:ArtifactResponse>
</SOAP-ENV:Body>
```

</SOAP-ENV:Envelope>

6. Once the assertion has been delivered by the Id. Server, the Application Server can inspect the user identity included in the assertion (it could be the real public identity, IMPU, of the user A, or an alias if privacy issues are a concern towards this specific Application Server). Additional access control policies can be enforced by the AS according to the information and attributes received in the SAML assertion from the Id. Server.

C.6 SIP/SAML Interaction for Incoming Calls

The Application Server tries to establish an outgoing call towards user A (Content-to-User). The Application Server can be hosted in the same network as user A, or maybe it could be hosted in another IMS network.
It is assumed that there is an existing relationship (federation) between the user and the Application Server. This federation could have happened through different channels (for instance, web-based service registration and federation).
The routing of the call could be done through direct interaction between the S-CSCF in the home network of the Application Server and the I-CSCF of the home network of user A, or it can be done though the usual IMS routing mechanisms (contacting first the local S-CSCF in the home network of the Application Server).
In the following diagram, the basic sequence flow is shown; the I-CSCF in the home network of user A receives an aliased identifier which is invalid for routing purposes, so it must be resolved to a valid IMS identifier before the call routing can take place.
The proposed flow would be as follows:

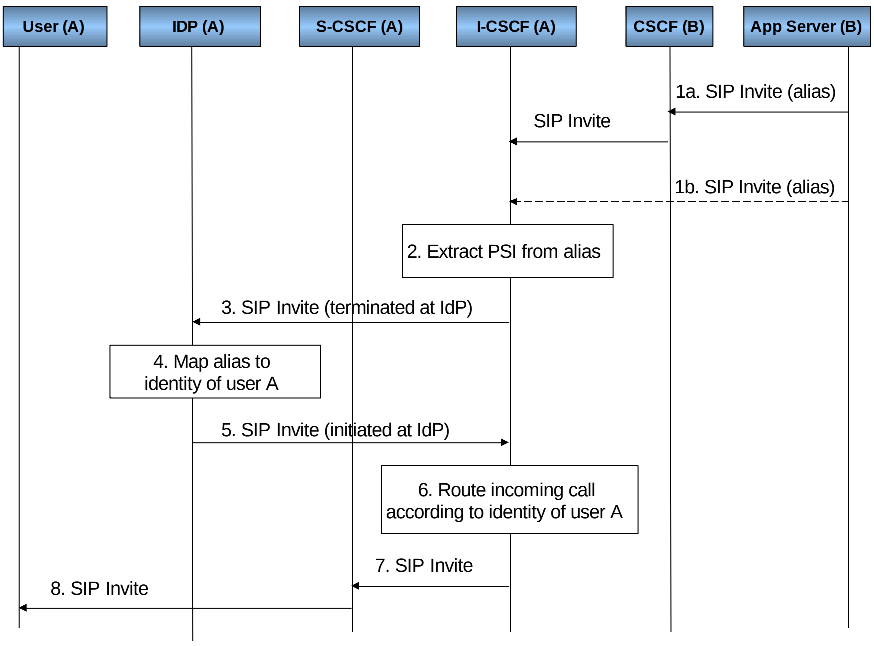

Figure 18: SIP/SAML Interaction Flow for Incoming Call

The interaction sequence would be as follows:

The Application Server sends a session initiation request by sending a SIP INVITE message targeted to the user A. This user might be known at the Application Server by its public identity (IMPU) or maybe by an alias shared with the Id. Server in its home network. In both cases, the Application Server should contact the call server of the user A home network; this can be done establishing a direct connection to the I-CSCF (if the Application Server is able to locate it), or maybe making use of the CSCF in its own network. Both are considered as feasible alternatives.

Example:

INVITE
sip:005a06e0-004005b13a2b@ids.example.com
SIP/2.0
Via: SIP/2.0/UDP 10.20.30.40:5060
From: ServiceB <sip:Service ProviderB@example.com>;tag=589304
To: UserA <sip:005a06e0-004005b13a2b@ids.example.com>
Call-ID: 8204589102@example.com
CSeq: 1 INVITE
Content-Type: application/sdp
Content-Length: …

1. In the home network of user A, the I-CSCF receives the SIP INVITE message. It must be able to route the message to the appropriate S-CSCF. In order to do that, the real IMPU of user A must be known, and therefore, if an alias was received from the Application Server, it must be first de-referenced to the real user identity. This is achieved by relaying the SIP message to the Id. Server.

2. Since there is no ISC interface defined between I-CSCF and an Application Server, a different mechanism must be defined to contact the Id. Server. The proposal is basically to define a Public Service Identifier (PSI) associated to the Id. Server, and make the I-CSCF extract the PSI from the identity received from the Application Server in the request URI of the SIP message (extracted from the domain name of the URI).

   Obviously, the I-CSCF must have been configured with this PSI and the aliased identity must have been composed by appending the PSI domain name to the federated shared alias between the Id. Server and the Application Server.

3. The SIP message is received in the Id. Server. This call must be terminated here, since there is no way to use this interface to return the SIP message to the I-CSCF, as it was done with the ISC interface.
   The aliased identity is mapped at the Id. Server to the real user identity (IMPU).

   The Id. Server, in this case, behaves as a “back-to-back user agent”, and it is involved in the SIP call flow for all the other SIP messages that compose the SIP call, not only the first “Invite”.

4. A new SIP call is initiated at the Id. Server, with a request URI including the real IMS identity of user A, and the SIP message is sent to the I-CSCF.

   Example:

   INVITE
   sip:userA@example.com
   SIP/2.0
   Via: SIP/2.0/UDP 10.20.30.40:5060
   From: IDS <sip:ids@example.com>;tag=589304
   To: UserA <sip:userA@example.com>
   Call-ID: 8204589102@example.com
   CSeq: 1 INVITE
   Content-Type: application/sdp
   Content-Length: …

5. Then, the I-CSCF locates the right S-CSCF (by querying the HSS) with user A’s public identity (IMPU).

6. Once the proper S-CSCF is located, the SIP INVITE message is forwarded to it.

7. The S-CSCF handles the incoming call as appropriate. It will eventually send the INVITE message to the user agent of user A to complete the establishment of the incoming call.

D. Technical Annex: "Liberty ID-WSF and IMS inter-working"

This annex gives more technical details on how IMS Application Servers could integrate with the Liberty ID-WSF framework considering two generic use-cases:

- An IMS Application Server is acting as a Liberty ID-WSF Web Service Consumer in order to consume resources exposed through the ID-WSF framework.
- An IMS Application Server acting as a Liberty ID-WSF Web Service Provider in order to expose IMS resources through the ID-WSF framework.

D.1 IMS Application Server as a Liberty ID-WSF WSC

This use-case is an extension of the "SIP/SAML Interaction for Outgoing Calls" case (see Technical Annex : "SIP/SAML Messaging").

User-A tries to establish an outgoing call towards an Application Server (User-to-Content). And in this use-case, the destination Application Server needs to retrieve data associated to User-A to fulfill the service. These data are exposed by an ID-WSF WSP that can be discovered through the ID-WSF Discovery Service.

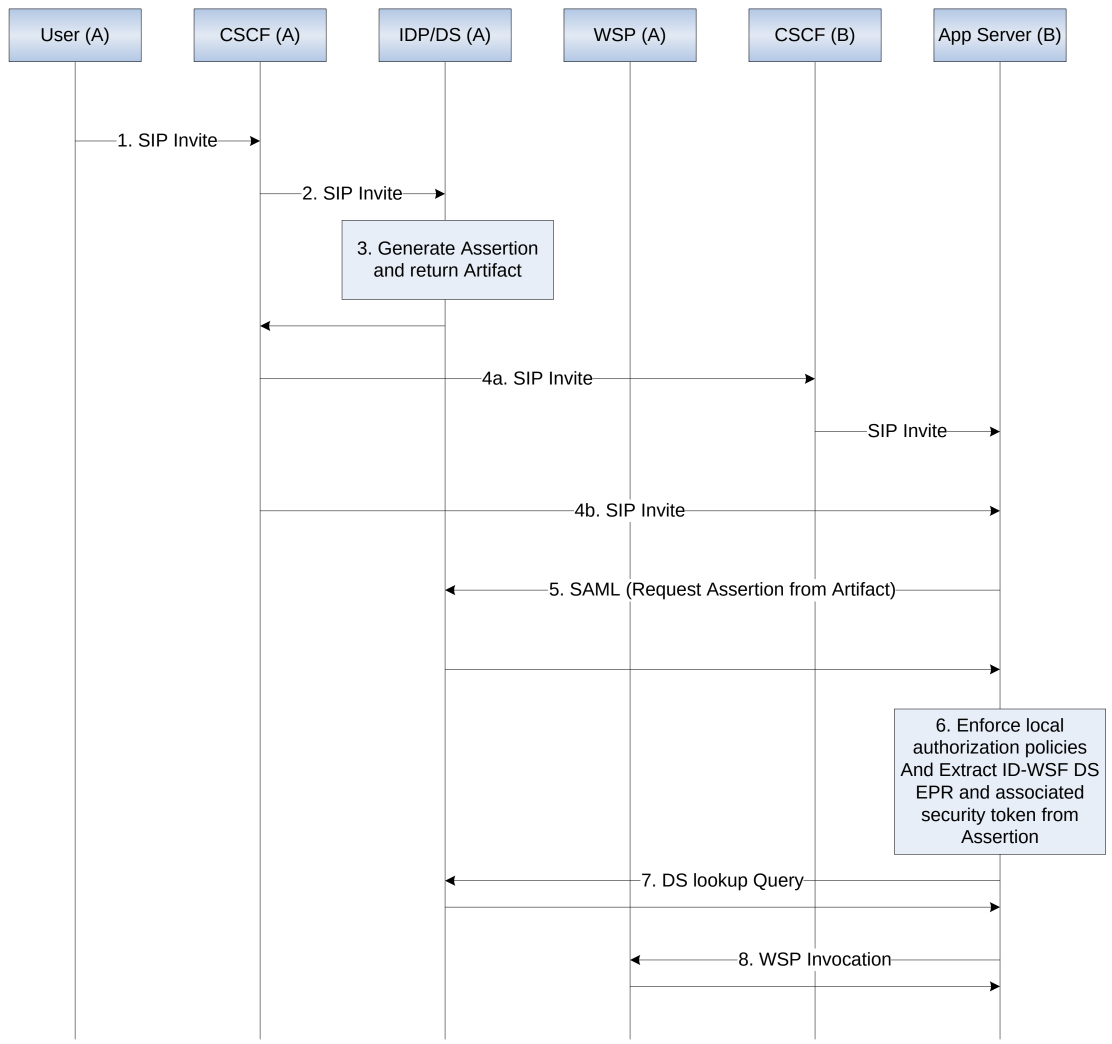

Figure 17: Application Server as a Liberty ID-WSF WSC

Steps 1 to 6 are identical to use-case "SIP/SAML Interaction for Outgoing Calls".

6. At this stage, the Application Server can extract from the SAML Assertion all the information required to contact the Discovery Service (DS EPR and associated security token).
7. The Application Server issues a lookup query to the ID-WSF Discovery Service to discover and get all the required information to contact the ID-WSF WSP exposing the requested data for the involved user.
8. The Application Server invokes the ID-WSF WSP and obtains the user data requested to fulfill the service.

D.2 IMS AS as a Liberty ID-WSF WSP

This use-case is a more typical ID-WSF use-case, except that the ID-WSF WSP exposes user data retrieved from the IMS. This entity is both an ID-WSF WSP in the Web domain and IMS Application Server in the IMS domain.

Registration in the DS

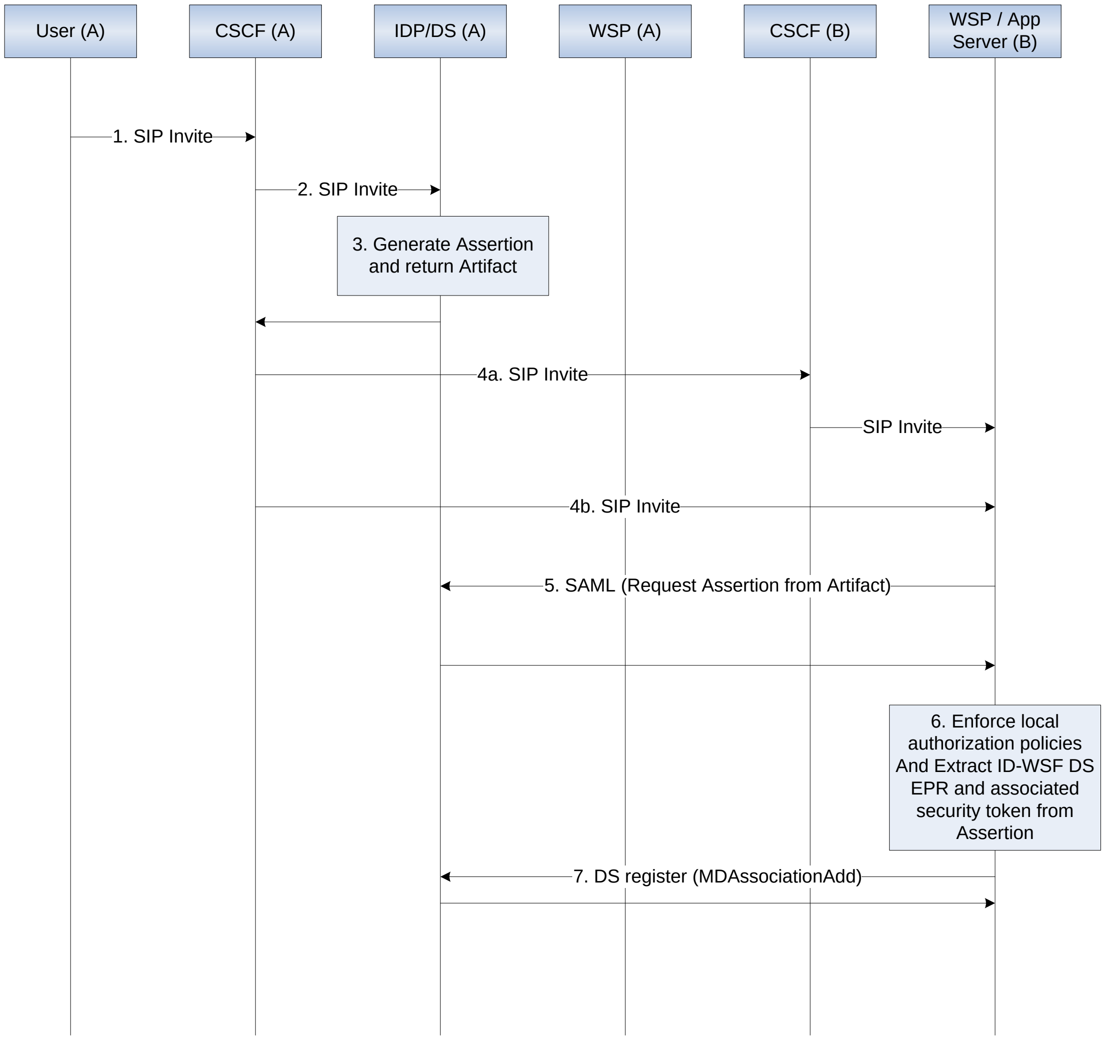

Figure 18: IMS as a Liberty ID-WSF WSP

To be discovered through the ID-WSF DS, the WSP/AS must register itself for the involved user. This is done through the "MDAssociationAdd" operation exposed by the ID-WSF DS.

Steps 1 to 6 are identical to use-case "SIP/SAML Interaction for Outgoing Calls".

6. At this stage, the Application Server can extract from the SAML Assertion all the information required to contact the Discovery Service (DS EPR and associated security token).

7. The Application Server issues an "MDAssociationAdd" request to the ID-WSF Discovery Service to register itself as an ID-WSF WSP for the involved user. The WSP / AS can now be discovered for that user.

Invocation

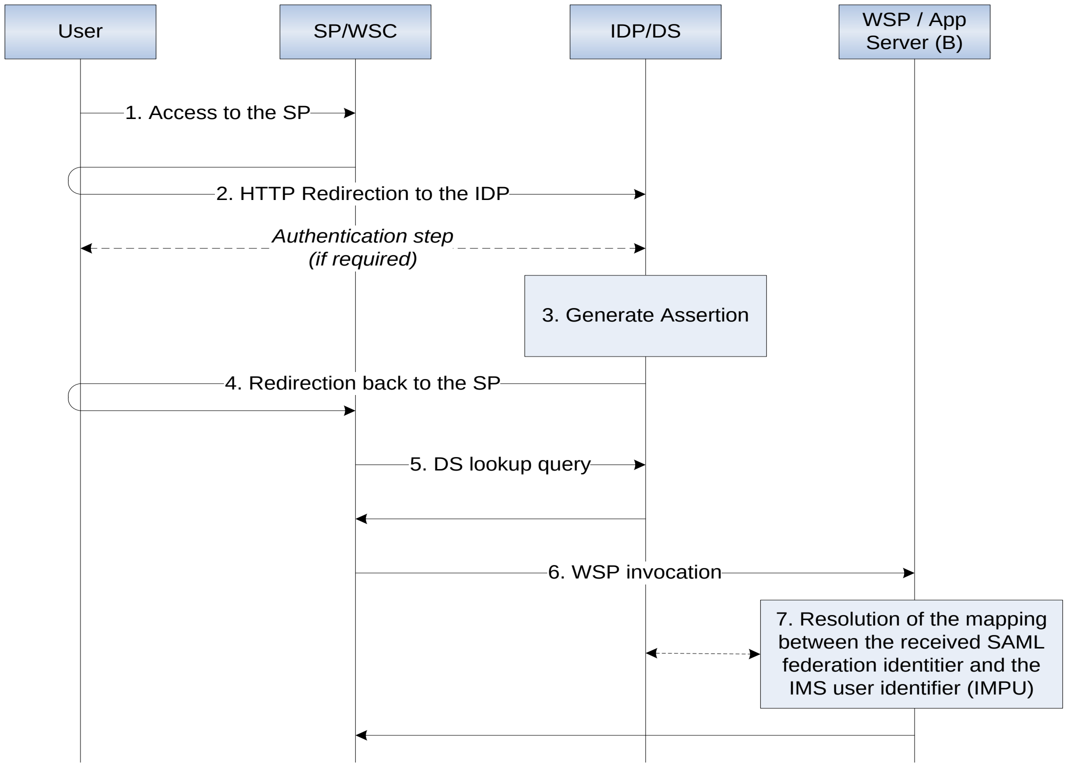

Figure 19: IMS as a Liberty ID-WSF WSP

This corresponds to standard ID-WSF flows. The only specificity occurs at step (7) with the resolution of the mapping between the received SAML federation identifier and the IMS user identifier (IMPU) in order to identify the user in the IMS world and respond with the right IMS user data.
This operation can be performed locally to the WSP/AS or can be delegated to the IdP/DS entity (that owns this mapping).