Multi-level Authentication Based Single Sign-On for IMS Services

M. Maachaoui[1,2], A. Abou El Kalam[2], C. Fraboul[1], and A. Ait Ouahman[2]

[1] Université de Toulouse, IRIT-ENSEEIHT. Toulouse, France
[2] Université Cadi-Ayyad, ENSA. Marrakesh, Morocco
{mohamed.maachaoui,anas.abouelkalam,
christian.fraboul}@enseeiht.fr, ouahman@ucam.ac.ma

Abstract. The IP multimedia Subsystem (IMS) is the evolution of the 3G mobile networks towards new generation networks (NGN) that are only IP based. This architectural framework is seen as a key element for achieving network convergence defining a new horizontal integrated service offering, based on a common signaling protocol (SIP) for all multimedia services such as Voice over IP, Video call, or instant messaging. However the present deployment of IMS is specified according to a specific model, the so called walled-garden. In this model the applications are only provided to the users within the same operator so that the users will not have to look for applications outside the IMS garden. It is a very restrictive access mode for the users because they remain dependent on services offered by the provider and can consequently not choose freely applications they want to subscribe for. The goal of this paper is to include Single Sign-On (SSO) features in the standing IMS architectures to allow the user accessing all the applications, even the external ones transparently, simulating a walled-garden environment. We also introduce the notion of security level that will be affected to the SPs, and implementing it in what we can call "a Multi-level authentication model".

Keywords: IMS, SIP, Service provider, Single Sign-On (SSO), Multi-level-SSO, SAML, Authentication.

1 Introduction

The IP Multimedia Subsystem (IMS) standard defines a generic architecture for offering voice, video and data communication services to mobile and fixed users. It is an international recognized standard, first specified by the Third Generation Partnership Project [1] (3GPP) and then supported by others standards organisms including ETSI/TISPAN [2]. The IMS standard supports multiple access technologies such as GSM, WCDMA, CDMA2000, Wireline broadband access and WLAN. IMS is based on the Internet Protocol (IP) and uses primarily the Session Initiation Protocol (SIP) [3] for transparent delivery of multimedia and communication applications. IMS breaks the traditional isolated, dedicated, per-service architecture, and introduces the application-oriented horizontal solution. Hence, the benefit of IMS

B. De Decker and D.W. Chadwick (Eds.): CMS 2012, LNCS 7394, pp. 174–187, 2012.

is to provide common mechanisms for billing, authentication, security, QoS, etc. Therefore, in the IMS service model, common functions are reutilized rather than being (re-) implemented in multiple copies. Moreover, IMS creates a service environment where any service can access any aspect of the session. This allows Service Providers (SP) to create far richer services than in an environment where all the services are independent of one another. In Next Generation Network (NGN), IMS has become the core of control and fused multi-access modes. Based on IMS, ubiquitous services will be implemented easily. Therefore, IMS is supposed to become the most suitable solution for fixed and mobile multimedia providers. However the framework has been specified according to a specific model, the so called walled-garden model. Nowadays, two service provisioning models are facing each other. The one cited above and the new "open-garden" [4] model. In a walled garden model, the applications are only provided to the users within the same operator so that the users will not have to look for applications outside the IMS garden. These applications are hosted by the IMS network operator, which keeps then total control over the users. However it is a restrictive access mode for the users because they remain dependent on services offered by the provider and can consequently not choose freely applications they want to subscribe for. They are indeed restrained to what is offered by their telecom operator. The second approach is known as "open garden" and it allows the users to access all kind of applications hosted by external service providers. The benefits of using a third party service provider are basically related to the user's satisfaction since all the IMS subscribers will have full access to all kind of applications that are available through the internet. In addition, External services 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 full customer's profile. Consequently, third-party services can be available only when a secured way is provided for their access.

In IMS, users are authenticated through the IMS authentication and Key Agreement (AKA) [5] technique. Once the authentication has succeeded, the client will gain full access to all the applications offered by the IMS core network but this is only true in a walled garden context. Whereas in the second model, the user will need to authenticate again across all the applications servers which will leads to an increase in the number of authentications performed during a session. Therefore, a Single Sign-On (SSO) mechanism should be deployed to allow the user accessing all their applications even the external ones transparently, simulating a walled-garden model.

SSO is a useful technology that allows users to skip bothersome authentication processes during accesses to multiple services. Most SSO systems treat all the SPs as the same security level. For banks and other SPs with higher requirements of security, SSO can't provide a good solution. Actually, SSO is a good way to provide usability, but since the user is only authenticated once, and therefore with one particular authentication method, this can cause security degradation. One way to improve the basic SSO is to introduce the notion of security level that will be affected to the SPs, and implementing it in what we can call "a Multi-level authentication model". In this paper we propose ways to include this SSO features in the standing IMS architectures. We proceed in four steps. Firstly, we review the IMS structural design, then the different possible SSO approaches and mechanisms, after what we expose an SSO enabled IMS architecture and propose evolutions to a multi-level SSO architecture for more security. Finally we present an example of authentication mechanism using the ML-SSO.

2 IMS Architecture and Service Provisioning Models

2.1 IMS Architecture

IMS is a whole new way to deliver multimedia (voice, video, data, etc.) regardless of the device (mobile phone, landline phone, cable, Internet, etc.) or the access medium (cellular, WiFi, Broadband, fixed-line, etc.). It was originally designed by the 3GPP to evolve UMTS networks in order to deliver IP multimedia to mobile users. IMS specification began in 3GPP Release 5 as part of the core network evolution from circuit-switching to packet-switching and was refined by subsequent Releases 6 and 7. IMS aims to make network management easier. Therefore, it separates control and bearer functions. This means that IMS service delivery network is on top of a packet switched infrastructure, which leads to easier deployment, development and integration of new services in the market. The overall architecture of IMS is shown in Figure 1.

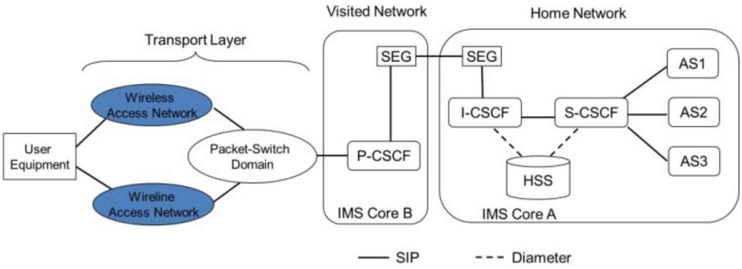

Fig. 1. IP Multimedia Subsystem Architecture

The main components of this architecture are CSCF (Call Session Control Function) and HSS (Home Subscriber Server). HSS (Home Subscriber Server) contains subscriber databases, e.g., user identity and registration information. HSS entity interacts with other network entities via the Diameter protocol [6]. CSCF (Call Session Control Function), which is a SIP server, is an essential node in IMS. CSCF processes SIP signaling in IMS. There are three types of CSCF, (1) a Proxy-CSCF (P-CSCF), (2) a Serving-CSCF (S-CSCF) and, (3) an Interrogating-CSCF (I-CSCF).

IMS-AKA is the 3GPP standard for authentication and secure sessions between User Equipment (UE) terminals and IMS systems. The IMS AKA security mechanism has two main functions:

- Authentication of a UE by the home S-CSCF and the home S-CSCF by the UE.
- Protection of all traffic between a UE and the P-CSCF on the Gm interface on dual IPsec channels [7].

IMS-AKA is a challenge-response based authentication mechanism, which uses symmetric cryptography and provides mutual authentication between the IMS Services Identity Module (ISIM) of the UE and the home network. For identification, the ISIM uses the IP Multimedia Private Identity (IMPI), which has the form of a Network Access Identifier (NAI). The HSS of the home network and ISIM share a long-term key associated with the IMPI. On successful authentication of the UE, the S-CSCF registers the IM Public Identity (IMPU) of the UE, and the user is allowed to receive any service for which he has proper authorization [8].

2.2 IMS Service Provisioning

Operators and service providers are keen to deploy IMS as it is expected to increase the Average Revenue Per User (ARPU) significantly. However, the rate of IMS deployment has slowed down due to a number of reasons, a key one being the IMS operator “walled garden” framework which assumes a unique operator over access network, IMS core network and Application Servers. Ultimately, the goal is to create a self-sustaining universe in which subscribers are allowed in to enjoy all the services and content the operator offers, in a fully secure environment and with an assured user experience and quality of service. Unfortunately, this model restricts the end users to the services their IMS operator offers. Moreover, internal 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). Therefore, the walled garden model fails to create mass user demand, which is the main driving force in revenue generating business world. Another limitation is the multiple authentications/ authorizations. In today's IMS architecture, a user or UE has to complete at least two authentication steps before he receives services from the IMS core. The user will be authenticated first by the access network. Next, using IMS-AKA, the IMS core will authenticate the UE. If the services are administered by the same operator, no further authentication is required. However, to receive third-party services, the user will have to re-authenticate and re-authorize to each service provider.

In a competitive market, users like to enjoy the freedom of using services from any content provider according to their needs and preferences. To attract operators and service providers, IMS needs to demonstrate that it is indeed a multi–service architecture which can be used as the common service framework even for non-SIP services, and certainly at least for Web Services. Actually, IMS was from the beginning designed to permit end-to-end SIP signaling between IMS and non-IMS endpoints, and if the non-IMS endpoint does not support SIP, the IMS service architecture permits an easy integration of protocol gateways. 3GPP always intended to keep IMS open to non-IMS networks, and more especially the Internet. Creating new walled gardens is not a strategy that will be sustainable for operators in the years to come. Given the proliferation of internet and internet services, the eventual success of IMS would be proportional to the traffic generated between IMS and the Internet. An IMS with very low traffic to and from the Internet would be an IMS which has failed to deliver any added value to end-users and the users may prefer to bypass IMS to directly access services on the Internet. One proof that IMS is open to integration with non-IMS networks especially internet is the dependency between the two standards organization, the 3GPP and the IETF.

Therefore, an opening of the IMS operators to third party service providers tends to be an obligation to ensure the success of the IMS network. 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 full customer's profile. To address these challenges we propose an extension of the existing IMS model to access IMS applications that are located outside the IMS domain and maintained by other service operators. This extended model will create a trust link between IMS domain and external services, and will reduce the burden of both end users and SPs through a Multi-Level Single Sign-On (MLSSO) feature, accomplished through identity federation.

3 Single Sign-On Standard

The establishment of SSO enables centralized authentication so that users can access all the resources that they are authorized to access, by being identified once on the network. For this, the SSO mechanism will have to propagate the authentication information to the various services of the network or other networks, thus avoiding the user to multiple identifications. The difficulty of the exercise lies in the level of trust between entities on the one hand and on the other, the establishment of a common procedure to spread the authentication information to all the entities we intend to unite. Thereby concentrating the security effort on the authentication server (s), SSO architecture allows implementing a coherent security policy. Using a common authentication service should also facilitate the development of authentication methods or the inclusion of multiple levels of authentication.

3.1 SSO Approaches

Centralized Approach

The basic principle of the centralized approach is to have a global and centralized database for all users. This also allows a centralized management of security policy to provide services. This approach is mainly for services that are all dependent of the same establishment, for example within a company. Each service has complete confidence in the authentication validated by the AC (Authentication Centre).

Federated Approach

The basic principle of the federated approach is to create an identity federation that groups a set of institutions. Normally each institution has an identity provider and service provider. The users' database is distributed and there is the spread of identity between the members in the federation. The federated approach thus allows a user, in a transparent manner to browse the sites and services within a given federation. Each service provider manages a portion of a user's data, but share the information for that user with partner services. This approach was developed to meet a need for decentralized management of users, where each service partner wishes to retain control over its own security policy, such as a set of independent dealer sites in terms of business and organization.

Cooperative Approach
In the cooperative approach, each user depends on a partner entity. When he tries to reach a network service, the user is authenticated by the partner on whom he depends. As in the federal approach, all network services independently manage their own security policy. The identity provider handles authentication and provides user attributes and the service provider manages access control. With this approach, the security credentials of the user are not exchanged. The main representative of this approach is Shibboleth [9].

3.2 SAML

The Security Assertion Markup Language (SAML) [10] is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an Identity Provider (a producer of assertions) and a service provider (a consumer of assertions). SAML assumes the user has enrolled with at least one identity provider. This Identity Provider (IdP) is expected to provide local authentication services to the user. A service provider relies on the identity provider to identify the user. At the user's request, the identity provider passes a SAML assertion to the service provider. On the basis of this assertion, the service provider makes an access control decision. SAML consists of building-block components that, when put together, allow a number of use cases to be supported. The components primarily permit transfer of identity, authentication, attribute, and authorization information between autonomous organizations that have an established trust relationship. The core SAML specification defines the structure and content of both assertions and protocol messages used to transfer this information.

4 Proposed Architecture

4.1 Chosen SSO Approach

We can immediately eliminate the centralized SSO approach in our case for many reasons. Indeed we need a system able to work through multiple domains, the IMS operator’s domain and the domains of the service providers. Moreover centralized SSO allows authenticating to different services with only one identity, which can cause severe privacy issues. Finally, centralized systems do not allow the transmission of authorization attributes or user information. So we have to focus our attention on the two other approaches, which both allow to access services on multiple domains and protect user's identity. In the solution presented we can find some characteristics of both federative and cooperative, approaches:

- The users dispose of multiple identities and accounts, one in each domain, with distributed profile information. Indeed It is interesting for the different service providers to keep information on each user, information that in general are specific to the application, for example the remaining credit of the user that will be used during the authorization phase and should not be the business of one particular IdP. From this perspective, the solution could be seen as federative.
- These different identities are federated with the IMS identity. The IMS identity of the user is federated with his corresponding identity at each service provider. This allow the user to access every service provider as soon as he is authenticated with his IMS identity, but does not allow a user to authenticate to one specific service provider to access another service provider without re-authentication. From this perspective, the solution could be seen as both federative and cooperative.
- The authentication is only performed with a single IdP (in the operator domain or a third party identity provider relying on the operator authentication). From this perspective, the solution could be seen as cooperative.

The result is that the proposed solution is a hybrid solution lying between cooperation and federation.

4.2 Adding SSO Features into IMS Network

Adding SSO components in the IMS architecture should not modify its native behavior and goal. Moreover the existing identity federation standards, such as the Liberty Alliance Federation Framework [11] or Shibboleth [9] are limited to web services. That is the reason why we have to adapt the existing federation mechanisms to the IMS/SIP world. As explained above SAML v2.0 is currently the most used protocol to exchange identity, authentication, attributes and authorization information between security domains. Thus, we have mainly to introduce in the IMS architecture two specific SAML entities, the IdP and the different SPs. The IdP will authenticate the user thanks to his IMS identity, issue SAML identity assertions, whereas the SP will receive and validate the assertions. The IdP can be merged with some IMS entity, but it requires to modify the current IMS Core implementations. It is possible to avoid this by adding IdP and SP as new SIP entities with enhanced SAML capabilities. Each SP will possess SIP proxy SAML connected to its different Application Servers (AS). Figure 2 basically presents the different entities in the SSO enabled IMS architecture for accessing third party services. Between the IMS Core and the SP network stands a SIP proxy acting as a SAML IdP which will be able to forward SIP messages to the SP network with SAML identity assertions. This IdP is connected to an Identity Store database allowing to create the identity assertions, particularly by recording the identity federations. Between the IdP and the AS, stands in the SP network a SIP proxy acting as a SAML SP which will request and verify the SAML identity

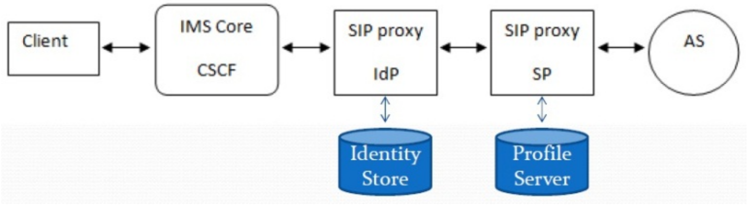

Fig. 2. Basic SSO architecture for IMS

assertions as well as performing user authorization thanks to the connection to a Profile Server containing the mapping between pseudonyms and local identities, and the users information specific to the service. If each service provider necessarily possesses one SAML SP entity, the positioning of the IdP may be multiple. There are mainly two possibilities, the IdP can either be located inside the IMS home network of the user or outside this network as a third party identity provider.

With a third party identity provider the IdP is not located in the IMS operator domain. It implies that the IdP has to use an authentication mechanism to identify the issuer of the SIP request. The main problem here is that there exist no standard protocols that the IdP can use to authenticate the user. However since the user is already authenticated by the IMS network with the IMS-AKA procedure, we can reuse this authentication context to allow a direct authentication of the UE with the IdP. Indeed, the 3GPP GBA model [12], part of the Generic Authentication Architecture defines a bootstrapping procedure based on AKA to authenticate a user to an application. In this way we re-using the IMS-AKA authentication mechanism and then have a low implementation cost, as well as a totally transparent SSO mechanism to the user. The second way to provide SSO is to place the IdP inside the IMS home network. At the registration procedure, the UE is authenticated through IMS-AKA. After P-CSCF and UE established an IPSec connection for integrity protection and confidentiality, identity enforcement is delegated to the P-CSCF. In IMS two headers P-Preferred-Identity and P-Asserted-Identity are used [13]. The P-Preferred-Identity header field is used from a user agent to a trusted proxy to carry the identity the user sending the SIP message wishes to be used for the P-Asserted-Header field value that the trusted element will insert. The P-Asserted-Identity header field is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication. When the client makes a SIP request, he adds a P-Preferred-Identity header containing his SIP URI. After receiving the SIP message, the P-CSCF validates the URI in the P-Preferred-Identity header and replaces it by a P-asserted-identity header before forwarding the message. Since in this architecture the IdP is located inside the IMS trusted network, the SIP requests that will be received by the IdP will contain the P-Asserted-Identity header with the IMPU of the client. There is no need for the IdP to use an authentication mechanism again, which avoid a new authentication step, which would be resource and time consuming. This SSO architecture is then essentially based on IMS-AKA. However this can only work if the IdP is located inside the IMS operator network. If it is not the case another authentication mechanism should be used, as seen previously.

Therefore the easiest way to provide SSO is to place the IdP inside the IMS home network. Figure 3 presents in more details the SSO enabled architecture with IdP inside the IMS home network. It introduces specific entities names; we keep the same terminology as in [14]. Indeed the IdP is merged with the S-CSCF. In the service provider network, the SIP server acts as the SAML SP. It is connected to the AS through the ISC interface and to the profile server named PfS, which contains the profile information of the users and allows making authorization. Moreover added to the HSS, an USD (User Subscription Database) keeps the user profile information regarding his subscription to third party service providers. Despite the major benefits brought by the SSO it is important to point out some drawbacks. SSO may also affect the security, because it gives access to a multitude of resources once the user is authenticated. For this reason it is preferable to couple the SSO solutions, with a strong authentication system, such as the use of certificates or even use multiple authentications mechanisms according to the criticality of the application to be accessed. Moreover, since the user is only authenticated once and therefore with one particular authentication method, this can cause security degradation. Since IMS allows establishing SIP sessions to access web services, which can be very sensitive like bank applications namely, E-Payment, Electronic Bill Payment, and E-Auction, this security degradation can be a threat. A way to improve the basic SSO solution is to allow multiple authentication mechanisms, each of these associated to a number of applications according to a LoA (Level of Assurance).

4.3 Multi-level-SSO

The multi-level architecture extends the one presented in section 4.2. The entities are still the same, except that new features have to be added to some entities, mainly the IdP. Indeed, the IdP needs now to be aware of the distinctive LoA and needs to be able to authenticate the user via different authentication strategies. In Section 5 we provide an example with two LoA using IMS-AKA for level 1 and Authenticated Diffie-Hellman using digital signature for level 2. But it should be noted that our model is independent of the authentication mechanism used.

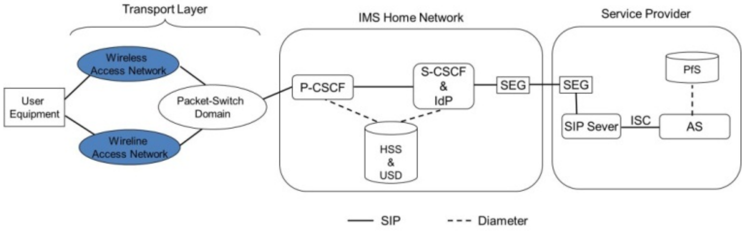

Fig. 3. SSO enabled IMS architecture with IdP inside the IMS home network

IdP Enhancements

The IdP is the most impacted entity by adding multi authentication levels. The way how it will behave is similar to the SHARE proposed in [15]. The IdP maintains a mapping of the SP with their respective level, recorded during the federation establishment, as well as the current level of the user. It also has to include information about the LoA of the user in the SAML assertion. Moreover it has to adopt a correct behavior when a client tries to access different levels of application servers and terminates sessions with these application servers, which is explained in the two following sections.

Multi-level Single Sign-On

As the IdP lies between the client and the SP in the SIP path, it will check the current authentication level of the user after receiving a SIP invite message and before forwarding it to the SP. If the level of the SP is greater than the current level of the user, the IdP will ask the user to authenticate using the authentication strategy of the level of the SP invited, by sending a SIP 401 Unauthorized response specifying the type of the expected authentication. Then, the user will resend his SIP invite message with the good credentials. After the check of the credentials by the IdP, the SIP message will be forwarded normally with the URI of the assertion. The message flow associated to this behavior is depicted in Figure 4a. The SP may also want to know the authentication context linked to a specified assertion. SAML allows adding into assertions the corresponding LoA. OASIS is in the process of defining schemas to exchange LoA information within SAML assertions [16].

Multi-level Single Sign-Out

Most of the SSO systems focus more on the safety certification in login rather than effective management of logout, which can be critical for SP with high security requirements such as banks. One main question is whether the log out from one application should or respectively not also imply a log out from the other applications with the same LoA. These two single sign-out techniques are called overall and respectively loose single sign-out. In the IMS context the session of a client with an SP will be assimilated to a SIP session. With loose single sign-out, if a user terminates a SIP session of level x, nothing particular is made except that the IdP will decrease the current level of authentication of the user to level x-1. With overall single sign-out, if a user terminates a SIP session of level x, the IdP will initiate the termination of all the other SIP sessions of level greater or equal than x. One possible way of doing this is that the IdP sends a BYE request to the user on the behalf of the SP, and a BYE request to the SP on the behalf of the user. However this requires the IdP to keep track of current sessions of each user, which could be very resource consuming. Furthermore the IdP will decrease the current authentication level of the user to x-1. To ensure maximum security, overall single sign-out seems to be the best solution, despite the fact it is more resource consuming. However hardly terminate SIP sessions seems also not to be very suitable. That is the reason why loose single sign-out may be preferred. The message flow and the behavior of the IdP with loose single sign-out

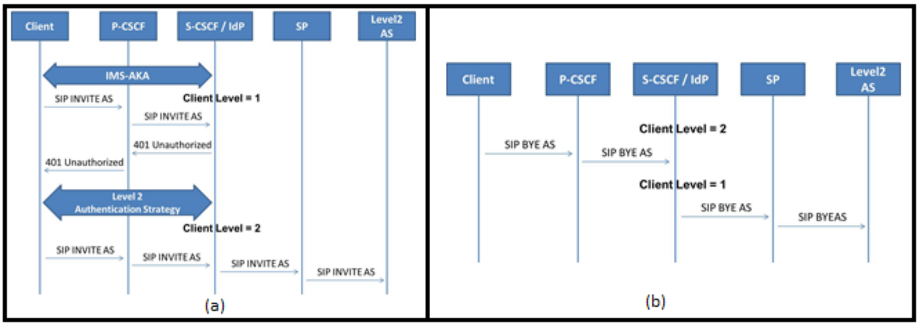

Fig. 4. (a) Client wanting to access a level 2 application server message flow. (b) Loose single sign-out.

is depicted in Figure 4b. A client who has a SIP session established with a level 2 application server requests a termination of session by sending a SIP BYE message. The IdP which stands in the path intercepts this message and sees a session termination with a level 2 AS, that is the reason why it decreases the current authentication level of the client before forwarding the message to the service provider.

Establishing Federation

As a same user can have different identities in different domains, the heart of the SSO solution is to establish and use a federation of different identities related to one particular user. There must be an agreement between providers on a set of identifiers and/or identity attributes by which the SP will refer to the user. This agreement should address a number of questions, such as the existence of local identities of the same user in each domain, the way to establish federation, dynamically or based on pre-established federated identities, the persistence of the federated identifiers, or the exchange of user's attributes. Since the introduction of SAML v2.0, it is possible, by exchanging SAML messages to dynamically establish an identity federation, as well as preserve user's anonymity by using federation alias. A SAML assertion includes a unique identifier called nameID. It can directly identify a user or it can be a pseudonym. Using a pseudonym can be useful to protect user's privacy and anonymity. SAML v2 specification defines two aliases: the transient identifier and the persistent identifier. The transient identifier is a temporary alias changing after each session. Then it does not allow the principal to be linked to a local account at the service provider. This alias method seems well adapted to the cooperated approach, but does not well suit our wish to maintain local accounts at each service provider. The persistent identifier is more adapted to our needs since it does not change over time and then allows to link user accounts preserving anonymity. With the architecture proposed, it is possible to use either an out of bound federation or a dynamic federation using persistent identifiers to create alias and perform the mapping of IMPU with IMLI (IM Local Identity) the identity known by the service providers [17][18].

SIP SAML Profile and Binding

We decided to use SAML as the base of the identity federation and propagation in the IMS SSO architecture. This requires the IMS environment to be able to carry the SAML protocol through adequate binding and profiles. Indeed, the mapping of SAML request-response message exchanges onto standard messaging or communication protocols, called SAML bindings, need to be specified and described in sufficient detail to ensure that independently implemented SAML-conforming software can interoperate when using standard messaging or communication protocols. Oasis defines for example the SAML SOAP binding describing how SAML request and response message exchanges should be mapped into SOAP message exchanges [19] [20].

5 Authentication Mechanisms and LoA

Multi-level SSO requires multiple authentication mechanisms. As soon as the client accesses the IMS Network, the user is authenticated to the IdP thanks to IMS-AKA. Thus IMS-AKA will be the authentication mechanism corresponding to the lowest level of assurance.

However IMS-AKA with UICC is already a strong two factor authentication mechanism based on “something you know”, the PIN code, and “something you have” the UICC. According to the NIST electronic authentication guideline [21], which categorizes authentication mechanisms on 4 levels, UICC based IMS-AKA can be considered to be level 3. Moreover, all the other implemented authentication mechanisms in SIP environment are less secure than the IMS-AKA one. To keep the delegation of the identity assertion to the P-CSCF, with the P-Asserted-Identity header, after having performed the authentication, a new level of authentication needs also to employ an authentication and key agreement mechanism allowing to renew the IPSec keys of the tunnel established between the client and the P-CSCF during IMS-AKA. To be more secured than IMS-AKA, the new authentication mechanism can use asymmetric cryptography instead of employing long term shared secret keys. Some propositions have been formulated using certificates [22], or not [23], trying to address the problem that yet no real certificate authentication in SIP exists as demonstrated in [24]. We formulate another tentative to include such authentication and key agreement mechanism based on the well-known Diffie-Hellman key exchange protocol. Figure 5 shows the establishment of the new IPSec tunnel between the client and the P-CSCF as well as the authentication of the client by the IdP, using the Diffie-Hellman key exchange combined with digital signatures. Finally, the two LoA defined are summarized in the Table 1.

Table 1. Example of authentication strategies mechanism with two levels

Level	1	2
Authentication (and key agreement) mechanism	IMS-AKA	Authenticated Diffie-Hellman using digital signature for IMS

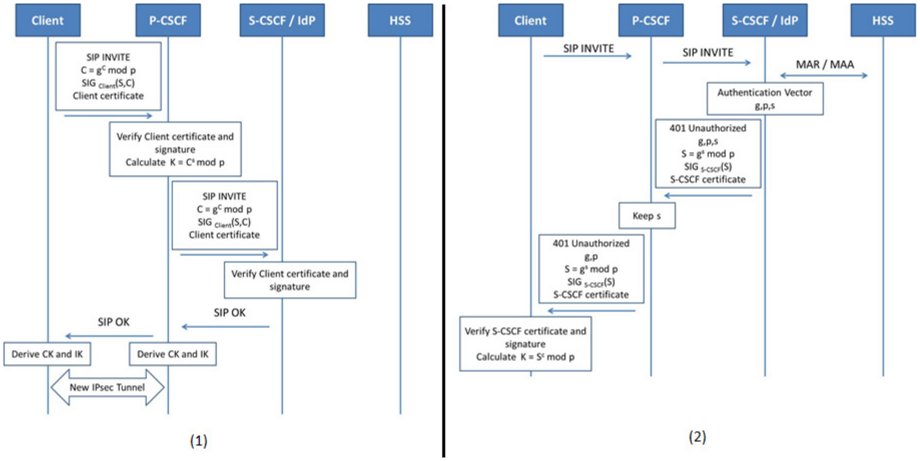

Fig. 5. Authenticated Diffie-Hellman using digital signature for IMS

6 Conclusion

In this paper we have tried to respond to an issue raised initially by the proliferation of web applications. Indeed that phenomenon has led to a more complex management of user identity information with multiple authentication processes that prove to be painful for both users and for network administrators. We therefore investigated Single sign-on technology which allows a user to access all the applications he is authorized to by authenticating only once. However, since our goal was to integrate this technology, not in a web environment but in IMS architecture opened to third-party services providers. This joint study of IMS and SSO led us to know how to integrate these two technologies, what choices and what changes have to be made for a user belonging to an IMS network to benefit effectively thanks to SSO, from services delivered by third party providers. Finally, to meet a greater security need for critical applications, we presented a solution based on multi-level SSO that integrates an additional more secured authentication mechanism. In future work, we would like to implement our model by extending the available open source implementations of IMS and identity federation and then evaluate his performance.

References

1. The 3rd Generation Partnership Project (3GPP), `http://www.3gpp.org/`
2. ETSI/TISPAN, `http://www.etsi.org/tispan/`
3. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Spark, R., Handley, M., Schooler, E.: Session Initiation Protocol. RFC 3261 (June 2002)
4. Al-Begain, K., Balakrishna, C., Galindo, L.A.: IMS: a development and deployment perspective
5. 3GPP TS 33.105: Cryptographic algorithm requirements. s.l.: ETSI, 2009-02. vol. 8

6. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J.: DiameterBase Protocol, RFC3588 (September 2003)
7. Kent, S., Atkinson, R.: Security architecture for the internet protocol. IETF, RFC2401 (November 1998)
8. Camarillo, G., Garcia-Martin, M.A.: The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the Cellular Worlds, 3rd edn. John Wiley & Sons Ltd. (2008)
9. M. A. C. for Education (MACE), Shibboleth (Internet2), `http://shibboleth.internet2.edu/`
10. Security Assertion Markup Language (SAML) V2.0 Technical Overview
11. Liberty Alliance Project: Liberty ID-WSF Authentication, Single Sign-On, and Identity Mapping Services Specification, Version: v2.0
12. 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, Generic Authentication Architecture (GAA), Generic Bootstrapping Architecture (GBA), (Release 11) 3GPP TS 33.220 V11.1.0 (2011-12) 2
13. Jennings, C., Peterson, J., Watson, M.: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks. RFC 3325 (November 2002)
14. Islam, S., Grégoire, J.-C.: Multi-domain authentication for IMS services. Computer Networks 55(12), 2689–2704 (2011)
15. Ying, N., Yao, Z., Hua, Z.: The Study of Multi-Level Authentication–Based Single Sign-on System. In: Proceedings of IC-BNMT 2009 (2009)
16. OASIS SAML V2.0 Identity Assurance Profiles,Version 1.0 Committee Draft 01 (September 22, 2009)
17. Grégoire, J.-C., Islam, S.: An SSO-enabled architecture for beyond the IMS domain services. In: Proceedings of the 6th NGNM in MANWEEK, pp. 37–49 (2009)
18. Islam, S., Grégoire, J.-C.: User-centric service provisioning for IMS. In: Proceedings of the 6th International Conference on Mobile Technology, Applications, and Systems (2009)
19. Kantara Initiative Telecommunications ID Work Group, `http://kantarainitiative.org/confluence/download/attachments/41648511/WP-BridgingIMS_AndInternetIdentity_V1.0.pdf`
20. Tschofenig, H., Peterson, J., Polk, J., Sicker, D., Hodges, J.: SIP SAML Profile and Binding, status: IETF Draft Standard (October 2010)
21. NIST, Electronic Authentication Guideline (April 2006)
22. Luo, M., Wen, Y.-Y., Zhao, H.: A Certificate-Based Authenticated Key Agreement Protocol for SIP-Based VoIP Networks. In: 2008 IFIP International Conference on Network and Parallel Computing (2008)
23. Wang, F.J., Zhang, Y.Q.: A new provably secure authentication and key agreement mechanism for SIP using certificateless public key cryptography. In: 2007 International Conference on Computational Intelligence and Security, Harbin, pp. 809–814 (2007), doi:10.1109/CIS.2007.113
24. Dotson, S.: Certificate Authentication in SIP, status: IETF Draft Standard (November 2007)