Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing

Rosa Sánchez, *Student Member*, IEEE, Florina Almenares, *Member*, IEEE, Patricia Arias, *Student Member*, IEEE, Daniel Díaz-Sánchez, *Member*, IEEE, and Andrés Marín, *Member*, IEEE

Abstract — *Consumer cloud computing paradigm has emerged as the natural evolution and integration of advances in several areas including distributed computing, service oriented architecture and consumer electronics. In this complex ecosystem, security and identity management challenges have cropped up, given their dynamism and heterogeneity. As a direct consequence, dynamic federated identity management with privacy improvements has arisen as an indispensable mechanism to enable the global scalability and usability that are required for the successful implantation of Cloud technologies. With these requirements in mind, we present an IdM architecture based on privacy and reputation extensions compliance with the SAMLv2/ID-FF standards*[1].

Index Terms — Identity Management, Dynamic Trust Management, Privacy, Consumer Cloud Computing.

I. INTRODUCTION

Cloud computing has emerged as the natural evolution and integration of advances in several areas including distributed computing, service oriented architecture, and web services. Likewise, its integration with home networks is emerging, called *consumer cloud computing*. This computing platform is a networked collection of servers, storage systems, and devices in order to combine software, data, and computing power scattered in multiple locations across the network [1], offering resources as services that are more flexible, scalable, affordable and attractive to customers and technology investors. Cloud computing is being proposed for different applications related to consumer electronics (CE), such as virtualization of consumer storage, CloudTV platforms that provide access to a number of Web applications such as social networking, user generated video games, etc. In this complex ecosystem, security and identity management challenges have cropped up, given their dynamism, distribution of information and heterogeneity of clouds: private, community, public, and hybrid. For example, users in a private cloud should be able to access applications hosted in a community cloud as long as a trust relationship exists between cloud domains, which expose different forms of their identities. This is due to cloud scenarios are multi-provider and multi-service, and applications may combine data from multiple cloud-based sources, which hold different terms of service, privacy policies, and location. Thus, because of the distributed and open nature of cloud environments, it is necessary to dynamically propagate trust in order to manage digital identity related to access control, reputation, anonymity and privacy in attribute sharing across domains in a secure and seamless manner. This last issue is very relevant, because the control over how user data is being stored, used, shared, etc., is lost. In this sense, federated Identity Management (IdM) has emerged as an indispensable mechanism to enable the global scalability that is required for the successful implantation of cloud technologies [2]. Specifically, we refer to federated identities based on the user-centric profiles, in order to protect consumers from cloud computing services.

In the context of consumer electronics, federations of clouds have the potential to alter how CE device applications are developed, deployed or used while simultaneously removing constraints on device functionality; taking into account home private clouds, public clouds, etc. For instance, consider a consumer cloud scenario, in which cloud federation allows Alice to build different layers in her car navigation map to get recommendations for the best routes (CSP_1); as well as consult relevant information on sites close to her position, in a Cloud Tourist Information Provider (CSP_2), by means of the cooperation between her mobile and the car navigator. In addition, Alice can connect to her Social Network (CSP_3) to see if some friends have been on that site and share information with them without compromising her privacy.

Nevertheless, federated IdM systems lack mechanisms to achieve agile and dynamic federation, which is one of the most significant architectural issues and requires further investigation. We previously identified this requirement in [3] to allow agile decision making without requiring static pre-configuration, and to make dynamic federation possible. Likewise, standards for federated IdM include privacy considerations, but they do not cover all aspects related to anonymity, pseudonyms or tracking. In addition, current IdM specifications support partial anonymity, define poor privacy policies or they are complex to implement or out of the scope. A similar situation can be found in the case of audit mechanisms.

In this article, we propose a dynamic privacy-enhanced federated identity management solution for cooperation, on-demand resources provisioning and delegation in cloud computing scenarios, preserving the user's privacy. Our

[1] This work was supported in part by the State of Madrid (Spain) under the contract number S2009/TIC-1650 (e-Madrid), and the Spanish Ministry of Science and Innovation under the project CONSEQUENCE (TEC2010-20572-C02-01).

Rosa Sánchez Guerrero is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: rsguerr@it.uc3m.es).

Florina Almenares is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: florina@it.uc3m.es).

Patricia Arias Cabarcos is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: ariasp@it.uc3m.es).

Andrés Marín López is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: amarin@it.uc3m.es).

Daniel Díaz-Sánchez is with the Telematic Eng. Department, Carlos III University, 28911, Leganés, Madrid, SPAIN (e-mail: dds@it.uc3m.es).

Manuscript received 01/15/12
Current version published 03/21/12
Electronic version published 03/21/12.

proposal extends SAMLv2 [4], defining an enhanced privacy module, a new reputation protocol, and considering the Enhanced Client Profile (ECP) proposed in [5], in order to provide an efficient identity management and access control, as well as dynamic, autonomic, and user-centric establishment of cloud federations.

This article is organized as follows: in section II, we give an overview about related work. Section III provides a brief background on identity management in consumer cloud computing identifying the challenges to be tackled. Then, section IV describes the proposed architecture and details the core components. Sections V and VI explain the contributions about the dynamic federation establishment and enhanced privacy, respectively. Section VIII gives details about the implementation issues. Finally, Section IX summarizes the presented work and some future lines.

II. RELATED WORK

This section covers the related work about IdM in consumer cloud computing, focused on identity management, dynamic federation and privacy issues. The proposals mentioned are specially centered in cloud computing, because cloud computing in consumer electronics is still an evolving paradigm.

So, our proposal considers aspects as multiple factor authentication, user control, portability and personalization while respecting user's privacy. Besides, introducing trust management based on reputation within identity management is an innovative aspect. We also address the dynamic management of trust relationships including unknown entities and trust evolution. These issues are very relevant because they are not fulfilled by existing solutions yet.

A. Identity management and authentication

Despite some current works propose to share media, cloud services and personalized content by means of a user-centric approach using different authentication and authorization mechanisms, none of the previous works deals with dynamic federated identity management along with privacy tools in the proposed consumer cloud computing scenarios.

The approach in [6] presents an authentication framework for consumer electronic devices, in order to share personal cloud services allowing users to temporarily transfer their services and content rights within trusted environments. The core idea that "the home network experience must become mobile and the key to achieving this is to authenticate people, rather than devices" is close to our work. The authors focus on using zero-knowledge proof techniques, which enable to preserve user's privacy in the process of providing his identity. However, this approach only deals with privacy concerning services and dynamism in the management of trust relationships is not taken into account. Zero-knowledge proof mechanisms are also proposed in [7] for authentication of an entity in a virtual machine on an active bundle with the subscriber identifier. In this work an entity-centric IdM model called IdM Wallet, based on the use of active bundles schemes to protect personal information from untrusted hosts is proposed. The proposal uses mobile agents' paradigm and introduces some architectural components that try to address trust and privacy issues, like the Trust Evaluation Agent and Audit Services Agents.

B. Dynamic federation between cloud providers

Regarding dynamic trust establishment, nowadays there is still scarce work on this field, despite it has been identified as a crucial necessity to achieve usability and scalability. The proposal in [8] defines a three-phase cross-cloud federation model based on SAML and agent technologies, but it does not specify how to carry out trust establishment between unknown cloud providers. Furthermore, approaches related to trust management in distributed environments can be found for peer to-peer systems [9] that form the basis for emerging next-generation computer applications. The proposal in [10] uses reputation based on global scope and local scope according to the familiarity-based personal relationships on a community to assign trust values.

C. Privacy

Privacy management is an important issue for consumer cloud computing and needs to be addressed in order to offer a solution compliant with legislation and enhance user trust when accessing to this kind of environments through their CE devices. Regarding legislation, it differs according to country block and national legislation. However, the broad privacy principles identified in [11] would apply to most countries. Pearson suggests a variety of guidelines and techniques on designing privacy-aware IdM architectures for cloud services such as minimizing customer personal information sent to and stored in the cloud, protecting sensitive customer information, maximizing user control, allowing user choice, specifying and limiting the purpose of data usage and providing the customer with privacy feedback. Such recommendations are addressed in this paper. Also, in [7] the principles are followed to manage identities disclosure. Moreover, the Fair Information Principles [12] are applicable to consumer cloud scenarios and contribute to mitigate threats such as frauds, unauthorized access to personal data, identity misuse, etc.

Another important aspect to consider is the cross-site sharing and tracking of data collection for personalization or targeted advertising. These techniques can bring out negative feelings and distrust when usage data collected (i.e. viewing habits for digital content, user's visited cloud service, etc.) at a trusted cloud provider is used, without the user's consent. In fact, the right of users to opt out of Web tracking has been identified by the Federal Trade Commission [13]. Besides, newly two W3C working draft documents [14][15] have been published that aim at defining technical mechanisms and the necessary terminology for users to specify their preferences for cross-site tracking, as well as for sites to make it clear whether they meet these in a unified and standard manner.

In general, research work on privacy in consumer cloud is still in its early stages. In this sense, there are several remarkable works which address guidelines, recommendations, and requirements, but a solution is not present. In [16] the authors present the main privacy issues and point out the need to develop reliable digital identity infrastructures to support tackling privacy and security

concerns in cloud environments. On the other hand, an example of how cloud computing technologies can contribute to preserve user's privacy in consumer electronics can be found in [17]. This approach defines a mechanism in which the cloud platform is used to perform electronic medical record exchange while maintaining user's privacy. To this end, this work is focused on unlinkability techniques between the patient and the electronic medical record, although issues such as how to control the doctor uses the restore mechanism of patient's health data only in cases of emergency without accessing to certain information of certain user in other circumstances are not clarified.

III. CURRENT IDENTITY MANAGEMENT TECHNOLOGIES

Standards like Secure Assertion Markup Language (SAML) version 2, X.509 [18] and OAuth [19] that were first solidified for federation are now coming to tackle cloud security challenges posed by identity management within the OASIS IDCloud (Identity in the Cloud) Technical Committee. Even, SAML is being used commercially by some companies to provide security solutions to hybrid cloud computing environments.

SAMLv2 defines an XML-based framework to allow the exchange of security assertions (about authentication, authorization decision, and attributes) between entities. This specification is based on ID-FF (Identity Federation Framework) from Liberty Alliance [20]. The aim is to establish open standards to easily conduct online transactions while protecting the privacy and security of identity information. These standards enable identity federation and management through features such as account linkage, and profiles, especially for the simple session management such as Single Sign-On (SSO) and Single LogOut (SLO).

In such federation scenarios take part the following main roles: *Service Providers* (SPs) that are entities consuming identity data issued by a trusted third party (TTP), *Identity Providers* (IdPs) that are entities asserting information about a subject, and *Users* that are the subjects of the assertions. The establishment of trust relationships between SPs and IdPs allows the creation of federations, typically governed by formal contracts, without input from consumers, creating circles-of-trust (i.e. a trust domain).

The federation establishment requires metadata's providers exchange; such metadata contains identifiers, public key certificates, service attributes, etc., that are needed for the location and secure communication between providers' services. This decoupling between providers enables that IdPs can support many SPs in a distributed fashion, and also focus on managing identities, access control policies, security token issuing, etc. In addition, enhanced users (ECPs) could be introduced in order to take part of a federation. In this sense, the user acts as an intermediary between providers. ECP also helps to empower the user's role respect to the privacy, because user makes decisions over data control.

Regarding SAML privacy support [21], this enables mechanisms that provide a degree of "partial anonymity" through the use of pseudonymous *permanent* and *transient* identifiers. *Transient* identifiers ensure that a user anonymously **accesses a service during the SSO process**; its main advantage is that correlation between identifiers is avoided. On the other hand, the *persistent* identifiers provide a persistent federation and remain active until they are explicitly deleted. The permanent federation implies an account linkage process, which relates two accounts associated to a user in different CSPs. In addition, the specification gives some non-normative considerations about confidentiality of transactions (i.e. assertions), and anonymity being "within a set" together with unobservability and pseudonymity.

X.509 is the underlying well-known key management infrastructure through digital certificates for authentication, recommended by OASIS, and widely deployed as security standard currently. So, SAML and ID-FF inherit and complement the static vision of trust from PKI, because trust relationships are also governed by formal contracts between Certification Authorities (CAs), Registration Authorities (RAs), and end users. Such relationships are managed by the creation of trusted anchor lists, similar to the circles-of-trust (CoT) in federated environments.

Finally, the OAuth 2.0 Authorization Protocol is an open protocol that has been built to use any underlying authentication system. Generally, user-password credentials are used. So OAuth allows users sharing verifiable assertions (i.e. security tokens) about themselves instead of releasing any personal information. So, this protocol aims at simplifying access to protected data while protecting the owner's account credentials. It also includes SSO scenarios between SPs, and delegation. OAuth can be used together with SAML or can be seen as a primary federation mechanism that involves token management between the actors involved in a transaction. In this last case, the federation establishment is out of the scope of the specification, but agreements are required between providers managing (i.e. issuing, validation, updating, etc.) the access token.

IV. TRUST-AWARE IDM ARCHITECTURE

Our IdM infrastructure incorporates the functionality to allow Identity Providers (IdPs), Service Providers (SPs), and enhanced clients to share common knowledge. The ECP has been defined in order to provide the required user-centric approach for cloud computing applications in consumer electronics devices. This is a software element for non-HTTP uses cases. The ECP enables to minimize direct interactions between SPs and IdPs, and provide full control to users over their identities, thereby improving mainly privacy.

The proposed architecture for the elements of the dynamic IdM system is represented in Fig. 1. Such image shows the logic blocks, in a layered model, as well as the relationship between them. At the top of the architecture, we have either the *Cloud* or the *Apps* layers. The first one contains cloud services offered by cloud providers (SPs or IdPs). The second one is located on the the ECPs, containing client applications. Next, in the underlying level we can see the *IdM layer*, which offers the basic functionality of each role defined in the SAMLv2 specification. In addition, such basic functionality is extended by adding the *Privacy Engine*

module. Finally, we find the *Trust layer,* focusing on the reputation manager in order to allow secure interaction between unknown parties. This last layer combines reputation information with other related data, for instance, historical interactions. So the user can request access, through the ECP installed on his mobile, to services provided by SPs and IdPs that are initially unknown in a dynamic and secure way.

A. IdM Layer

Regarding the logic modules that make up the *IdM Layer*, they contribute to manage sessions, user profiles, as well as issue and processing of requests and responses of authentication and authorization. In this sense, our system supports multiple authentication mechanisms (e.g. username/passwords, digital certificates, or delegated credentials) and flexible user profile management, which enables to facilitate for instance, service personalization in a robust and flexible manner.

On the other hand, this layer has cryptographic modules based on an underlying PKI for secure communications and exchange of needed metadata in the SAML dialogue between the SP and the IdP about the user. Also note that, we can think of metadata lists being equivalent to trust, since a provider considers trustworthy the entities whose metadata is stored in its repository.

The core modules of the IdM layer, which are common both to providers and ECPs, are detailed as follow:

- ***Dynamic Trust List (DTL)/CoT Management*** is in charge of maintaining an enhanced circle of trust, which contains more complete information than traditional certificate lists, such as trust level, previous interaction results, reputation scores, keys, etc. It must be noted that, this trust information is automatically updated through modules in the *Trust* layer.
- ***AuthN and AuthZ Service Management*** functionality depends on its location. So, it receives and processes the `<AuthnRequest>` messages from either the SP or the ECP, regarding to the ECP or IdP, respectively. In the CSP, it issues such authentication and authorization request. The modules in each entity interact to verify the user requesting a service is really who he claims. For this purpose, it supports multiple authentication mechanisms including PKI, username/password, etc.
  In regard to the authorization process, the security assertions and the attributes exchanged convey authentication decisions, profiles and attributes to cloud services providers allowing them to decide what services or resources the user can access. For that, this module issues (IdP) or verifies (SP), and manages SAML authentication assertions and attribute statements. The aim is to facilitate authentication and user management to users and cloud services improving user experience while reducing complexity and management costs.
- ***Privacy Engine*** is responsible for managing user identifiers (e.g. pseudonymous) and monitoring how user data is being accessed without compromising user's identity. To achieve this, the fields that are logged by monitoring tools and verified by audit tools show the auditor what information about the user is being accessed without divulging the actual information. In this way, this module provides multiple and partial identities, which allows users to access cloud services and share digital content without necessarily revealing their name and true identity to everyone. The use of different pseudonyms enables to support differing ranges of identification and authentication strengths. The technical details about the main functionalities of this module can be found in section VI.

These modules are supported by basic libraries such as IdM and cryptographic, which implement SAMLv2/ID-FF functionalities and cryptographic algorithms and protocols, respectively. In the user's side, these libraries implement the minimal functionality, taking into account limited devices. Thus, ECP incorporates "lite" library versions.

Regarding the provider's side, we can also find other two additional modules whose functionality is specific to service provision:

- ***Session Management (SM)*** is responsible for managing user identifiers, as well as the session data of those users accessing CSPs or IdPs services. The CSP together with IdP determine when user's session is active. The CSP creates session identifiers for every user once user has already been authenticated and registered in the service. Such session identifiers are linked to users' profile. SM also may check several user profiles and select the most appropriate content for a specific service (e.g. video on demand). Thus, the SM communicates with other modules handling authentication and attribute exchange, and with the *User Management* module to request the user's profile, related to the cloud services, and matches it with the cloud profile policy and any other enforced IdP policies. Finally, this module may also request information about the device profile in order to support multi-device SSO [22].
- ***User Management (UM)*** is in charge of dealing with credential storage, management users' profiles according to their preferences and policy enforcement. Regarding credential management, the user can store his credentials (e.g. username/passwords, digital certificates, etc.) that are required by cloud applications that can be accessed from the *Personal Cloud (PC)*: TV services, social networks, payment services, etc. The *Personal Cloud* term refers to a user-centric private cloud, which offers a unified perspective on the user's activities, across all the cloud applications, and all her collaborations. Furthermore, the Personal Cloud is characterized by being fully configured and production-ready software available to authorized users. On the other hand, the UM module interacts with the ECP in order to determinate which IdP is appropriate according to the service requested and user's preferences. Thus, our system will act on behalf of the user and perform authentication in the different cloud consumer applications providing a seamless, personalized and improved user experience.

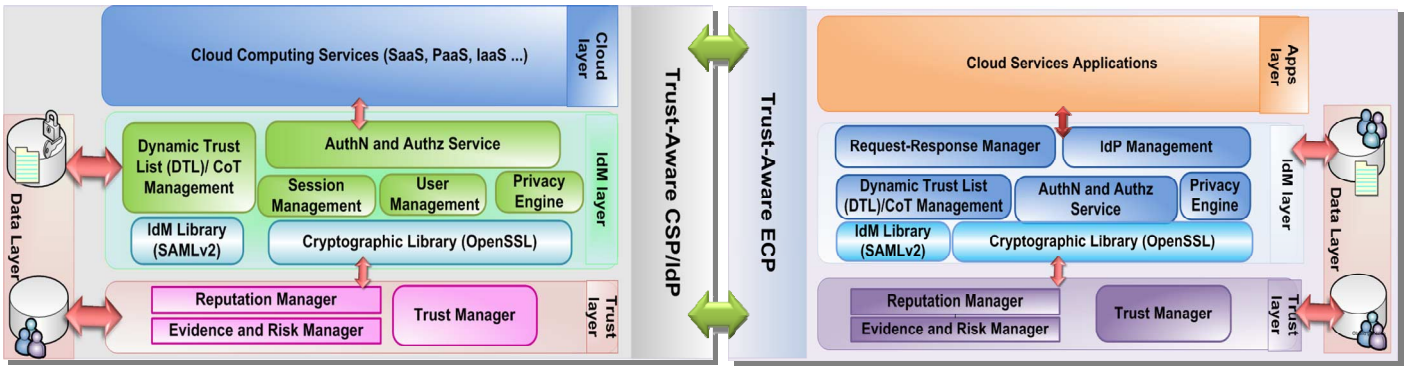

Fig. 1. Enhanced- Privacy and Trust-Aware IdM architecture for Consumer Cloud Computing. This shows the building blocks in the different roles in an identity management system for cloud scenarios, such as providers (CSP, IdP) and users (ECP).

Besides, the ECP incorporates other two additional modules whose functionalities are:

- ***IdP Management*** is coordinated with the *DTL/CoT Management* and the trust layer to configure trust relationships with the IdPs in a dynamic and secure manner. In addition, it is responsible for determining the most adequate identity provider depending on the requested service, the user's preferences related to privacy and security (e.g. type of credential) and the context. For instance, in some contexts the user may not want to reveal any personal information, whereas in other contexts he may wish for partial or full disclosure of identity. To achieve these tasks, this module collaborates with the *Request-Response Manager* and the *Privacy Engine.*
- ***Request-Response Manager*** receives authentication, authorization or attribute requests from the applications. It is the interface between *Authn and Authz Service* and applications. These requests can be originated by authentication request statements from the SP. After carrying out the processing and verification of requests, this module issues or redirects responses to the applications for being resent to the SP. Note that, the *Request-Response Manager* is able to use a reverse SOAP (PAOS) binding [23] to manage the requests and responses of authentication such as is specified.

B. Trust Layer

The *Trust Layer* consists of three components: the *Reputation Manager* (RM), the *Evidence and Risk Manager* (ERM), and the *Trust Manager* (TM). The RM is responsible for distributing, collecting and managing requests and responses of reputation to federate. The protocol is explained in the next section. The RM is connected to the ERM module to analyze the risk factors associated with each transaction and keep a history of past interactions. The ERM calculates the trust value associated to each entity, and includes the trust evolution, as this will change over time. The TM orchestrates the communications and operations of the described modules, and manages the trust data repository. It is in charge of managing dynamically trust information, negotiating the trust relationship establishment, and providing trust data to other layers. The trust information contains data related to the entities' behavior and external trust information from trusted third parties, thus taking advantage of the common knowledge in the federation. Finally, the TM is also enriched with more complex functionality, such as context and policy management in order to make richer decisions depending on the actions defined by policies and context in each specific situation.

V. DYNAMIC FEDERATION ESTABLISHMENT

According to Jøsang [24], reputation can be considered as a collective measure of trustworthiness based on the referrals or ratings from members in a community. Thus, this information can be combined with other trust related data, such as the history of past interactions, to take richer trust decisions. However, the application of this dimension of trust to identity management scenarios has not been fully addressed yet. This is gaining attention in the context of dynamic federation together with risk evaluation [25].

Adding reputation support to SAML implies modifications to both Assertions and Protocols [26]. We have defined a new assertion, which conforms to the extension mechanisms explained in [4], so compatibility is assured. Such assertion is a custom statement type, called `<ReputationStatement>`, which is conveyed in a response message.

The structure of such reputation assertion has an initial part (i.e. header), whose content is the same defined in the standard. This common section includes the assertion identifier (ID), the names of the issuer and the subject, and information about the instant in which the assertion was issued. The `<Subject>` tag, in our case, indicates the identifier of the entity for which reputation data has been requested. Apart from this information, the statement contains a body section, which contains all the related data to the reputation metric. These include the following attributes: `ReputationInstant`, to ensure data freshness; `ReputationScore` that corresponds to the reputation value; a `DistributionFunction`, for the reputation to be aggregatable; and `Context`, to illustrate for what situation the reputation was made.

This `<ReputationStatement>` is exchanged using the SAML "Assertion Query and Request Protocol". So query/response formats are compliant with the rules defined

for extending the schema. The communication flow has the following steps:

1. Alice accesses a service offered by a CSP_2. The CSP_2 needs to authenticate Alice, so it performs IdP discovery in order to determine who should be asked for user authentication. This checks local configuration data to see if the discovered IdP is known (i.e. metadata stored).
2. As CSP_2 determines IdP_1 is unknown, the RM executes the logic to gather reputation information about it. This sends a `<ReputationRequest>` acting as a *Reputation Requester*.
3. The IdP_2 and CSP_1 returns a `<ReputationResponse>` containing a `<ReputationStatement>` in case of success, or an error message in case of failure. These entities would be a *Reputation Responder*. As IdP_1 is trusted in accordance with the reputation information received, then the CSP_2 downloads IdP_1 metadata and initiates SSO as usually.
4. The CSP_2 requests Alice's authentication to IdP_1.
5. IdP_1 authenticates Alice and sends the successful authentication response to the CSP_2.
6. Finally, the CSP_2 grants service access to Alice.

We aim to demonstrate that collecting external information allows seamless trust establishment and facilitates this kind of interactions, otherwise impossible or insecure. We have worked with a simple SAML-based SSO scenario: a user, two CSPs, and two IdPs. In this situation, CSP_2 and IdP_1 are unknown, so CSP_2 requests information about IdP_1 to trusted providers such as IdP_2 and CSP_1. This same situation using SAML without the proposed extension, CSP_2 and IdP_1 will not interact, or they will require manual intervention from administrators to configure both ones. In most identity management implementations, the user must introduce the URI where the metadata document of her IdP or CSP is located. Nevertheless, many providers do not support metadata-based configuration; therefore, it is required an administrator to introduce the CSP's certificates, and construct complex cryptographic structures (i.e. certificate chains) that are required to enable interaction. After that, the metadata document is stored and all the certificates contained in it are considered trustworthy, so they will be used to validate SAML messages. The main limitation regarding trust issues is that no trust model is defined since the CSP will interact with any provider introduced by the user. In addition, usability features are very poor because the user should not have to know and remember the metadata location of her IdPs.

VI. PRIVACY MANAGEMENT

As far as privacy management carried out by our system is concerned, the proposed IdM architecture provides a user's privacy protection framework for sharing users identity attributes among different entities and can be used to keep data under control of users, as well as user confidence while preserve privacy in an appropriate way to generate trust in the cloud applications. Such privacy is preserved thanks to the ECP and the *Privacy Engine*, which has been incorporated in each entity. As explained in section IV, the enhanced client allows to give users more control over their personal information, identities, as well as control over authentication and attribute exchange processes eliminating the direct communication between the SP and the IdP. The *Privacy Engine* component carries out an appropriate management of user identifiers according to user's preferences and context, as well as to monitor how user data is being accessed by CSPs or IdPs without compromising user's identity. As shown in Fig. 2, this module has different functionalities depending on the entity in which it is located.

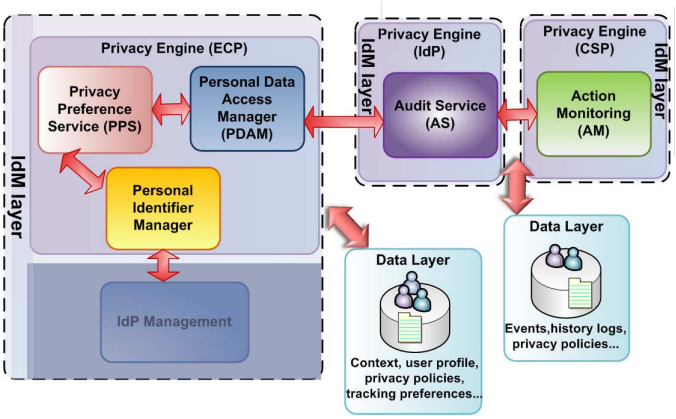

Fig. 2: Privacy Components. The Privacy Engine has different functionalities depending on the different roles of the entity where it is placed; for instance, management of user identifiers and privacy preferences or audit and monitoring functions.

The module incorporated in the **ECP** has the following components:

- ***Privacy Preferences Service*** (PPS) provides an interface for configuring user preferences about the handling of personal data and specifying options for the use and release of sensitive information. The set of variables that define the customizing privacy preferences include for instance, the user identifier, information type, the requestor, the requested operation (i.e. query, create, modify), as well as a set of pre-defined policies by the IdP. On the other hand, this module also includes the tracking preference expression (DNT) feature that allows user to express their personal preferences regarding cross-site tracking to each cloud service or application. Whereas the *Do-Not-Track* approaches that recently have been incorporated in some commercial browsers, only enable or disable tracking characteristic and this is applied to all services accessed by user without including any preference set for configuration; we believe that, it is necessary to maintain a trade-off between degree of tracking and user's privacy to obtain an adequate personalization degree in the different cloud services. Nowadays, we can find a lot of services, for example, personalized catch up TV services or location prediction applications, which require access to certain attributes related to habits, preferences and user needs to properly adapt to user behavior, to predict future patterns in his preferences and to offer a really customized user experience.

Therefore, the improvement of our proposal over current solutions comes from offering the user the option of selecting and detailing which attributes may be traced

depending on the user's trust placed in the service, the sensitivity of a specific attribute, desired personalization degree, etc.

- ***Personal Data Access Manager*** (PDAM) allows user to check the accuracy of his personal information and visualize how his data is being used by both the CSP and the IdP. For the latter purpose, this module receives notifications from the *Audit Service* located in the IdP; thereby allowing the user to obtain automatically updated information in a seamless and dynamic manner.
- ***Personal Identifier Manager*** is responsible for managing different kind of identifiers such as pseudonyms (*transient* or *permanent* identifiers), social networks identifiers, etc., in a flexible and personalized manner in order to enable user to choose between multiple identities when interacting with cloud services through his *Personal Cloud*. For this, the module interacts with the *IdP Management* component to obtain and associate user identifier in each IdP. Note that this SAML-compliant module uses different pseudonyms for each CSP in order to avoid different CSPs belonging to the same cloud federation to infer user behavior.

In regard to the *Privacy Engine* in the **providers**, its main tasks are related to the functions of auditing (i.e. IdP AS) and monitoring (i.e. CSP AM) of how each CSP accesses user data without compromising user's identity. So auditing and fraud detection at CSPs could be tackled. The IdP *Privacy Engine* module includes an ***Audit Service*** focused on data sharing, which captures any transaction or event where user data is requested, shared, modified, created or deleted from a cloud service provider, including information such as the sender, receiver, target identity, as well as identifying the user attributes accessed and the purpose for which they were accessed. It must be noted that, the actual values of the attributes involved in each event are not logged in order to ensure that events are recorded in a consistent manner amongst all the CSPs using the ***Action Monitoring*** module. The AM use an XML-based event structure defined by us to log events to the *Audit Service*, which includes the following elements:

- ***UserID*** specifies an opaque identifier or pseudonym. It refers to the principal whose personal information is accessed.
- ***CSPName*** specifies the entity name, which is accessing to user data. It identifies the cloud service provider and is a unique identifier of each CSP (`EntityID`) contained in its metadata.
- ***AttributeName*** is a compound field that contains the attribute names accessed by the CSP. In this case, attribute names must be consistent across the federation.
- ***Scope*** indicates the scope in which user data is being used, as well as how many CSPs are sharing or exchanging a specific user's attribute.
- ***Purpose*** specifies the purpose usage for attribute requested by a CSP.
- ***AccessTime*** indicates the instant time in which an attribute was accessed by a provider. It is a timestamp of the event.
- ***UserDelegatedID*** specifies an opaque identifier or pseudonym. This field is optional, because it is only logged in delegation cases and refers to principal in whose behalf on user data is being accessed.

VII. Implementation Issues

We have deployed our own identity management infrastructure according to the test scenario depicted in Fig.3. To this end, we have used the C library called Lasso [27] and the IdP developed from it, Authentic [28]. We have integrated Authentic with OpenLDAP [29] to manage users' accounts. In regard to CSPs, we have also used ZXID and have developed our own Lasso-based CSPs, in order to test different profiles. Note that, some interoperability issues have been addressed; therefore, we have modified the source code of the Authentic to make the IdP-compliant with SAMLv2/ID-FF. The ECP has been deployed in mobile and embedded devices. This has also been integrated with deployed providers.

Both providers and ECP have been extended adding the reputation protocol functionalities. So entities can act as both roles of reputation requester or responder in each time. In addition, they are being extended by implementing the SAML-based privacy engine. In the ECP, the interfaces for the PPS and the PDAM to configure user's privacy preferences and check personal data have been developed as an integrated application in Java for limited devices. We are also testing the interaction of these modules with the AS and the AM. In this sense, we are considering to create the RSS feeds from system log files in order to present this information in a user-friendly way, as well as facilitating its management, distribution and publishing.

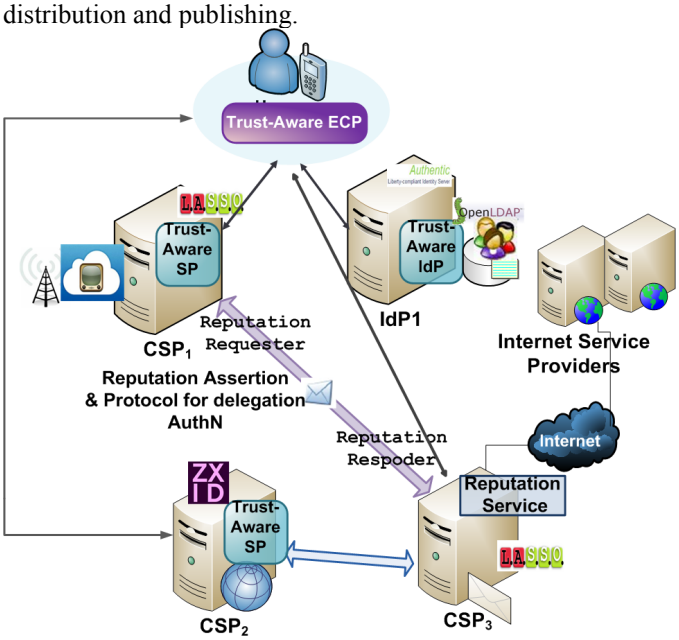

Fig. 3. Test architecture scenario. It can be seen the different interactions between the entities (the ECP, the IdP and CSPs) through the exchange of SAML authentication, authorization and reputation statements. Note that, the ECP is situated in the middle of transactions between the IdP and the CSPs. In addition, CSP_1 (the Cloud TV provider) requests reputation information to CSP_3 in order to establish a dynamic federation that allows to delegate the authentication service to well-known Internet service providers. Thus, the user can use multiple identifiers, since he/she may have several accounts associated with different providers apart from the IdP.

Furthermore, we have simulated a discovery service in order to test dynamic federation for delegating the authentication service to third parties known as Internet service providers where the user has an associated account. Thus, we have simulated an external trusted service (CSP_3) whose DTL contains trusted historical and reputation information on well-known services. This reputation service has been to be developed, since currently there is no online service providing such information. On the other hand, we have tested guarantee of user's privacy by providing explicit user consent to allow third parties access to certain parts of user profile.

IX. Conclusion and Future Work

Cloud Computing is becoming part of everyday life for users, in a way that is mainly transparent to them. Moreover, with the prevalence of mobile devices, cloud technology is being proposed for different applications related to consumer electronics, such as virtualization of consumer storage or CloudTV platforms, which allow bringing Cloud Computing paradigm to home entertainment. Thus, to alter how CE device applications are developed, deployed, used or shared while simultaneously removing constraints on device functionality, dynamic federation of clouds with privacy improvements is a powerful approach.

In this article, we have designed and proposed a privacy-enhanced and trust-aware IdM architecture compliance with SAMLv2/ID-FF standards. The aim is to provide an efficient identity management and access control, as well as dynamic, autonomic, and user-centric system for better scalability in cloud computing services. With the inclusion of reputation information and the introduction of the Trust-Aware ECP, mobile users may participate in the cloud federation in a more active way. Likewise, the presented reputation extensions allow the cloud providers to make richer trust decisions when interacting with unknown entities. Furthermore, trust evolution and risk management are also included. The addition of these features is of special importance since monitoring cloud providers and users' behavior allow to reward or penalize the current behavior, thus modeling the fact that trust changes over time. On the other hand, risk management enables to analyze the risk factors associated with each transaction.

In regard to privacy, our system empowers users to access cloud services and share digital content without necessarily revealing their true identity to everyone, thanks to the use of multiple identities, for instance depending on the context. Besides, it provides a framework that enables to keep to a trace-off between user's privacy and degree of tracking to obtain an adequate personalization degree in the different services. Finally, this module enables users to have enhanced awareness over their online identity use by introducing monitoring tools and an audit service focused on data sharing through the *Personal Cloud*.

As future work, we want to validate the optimal values of the parameters of the reputation model and evaluate the performance of the system experimentally through simulations using OMNeT++ [30]. Moreover, we aim to validate the proposed architecture on real cloud health care scenarios in order to demonstrate how the privacy is handled by the system entities.

References

[1] A. Beloglazov, R. Buyya, Y. C. Lee, and A. Zomaya, "A taxonomy and survey of energy-efficient data centers and cloud computing systems," Univ. of Melbourne, Technical Report CLOUDS-TR-2010-3, 2010.

[2] Open Cloud Manifesto Group: "Open Cloud Manifesto", 2009.

[3] P. Arias, F. Almenárez, A. Marín, and D. Díaz., "Enabling SAML for Dynamic Identity Federation Management", Wireless and Mobile Networking Conference (WMNC'09), 2009.

[4] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, and T. Scavo (Eds.), "Security Assertion Markup Language (SAML) V2.0 Technical Overview", Mar.2008.

[5] F. Almenárez, P. Arias, D. Díaz-Sánchez, A. Marín, and R. Sánchez, "fedTV: Personal Networks Federation for IdM in Mobile DTV", *IEEE Transactions on Consumer Electronics*, vol.57, no.2, May 2011.

[6] S.Grzonkowski and P.Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", *IEEE Transactions on Consumer Electronics*, vol.57, no.3, May 2011.

[7] P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien and L. Ben Othmane, "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing", in Proc. of the 29th IEEE International Symposium on Reliable Distributed Systems (SRDS), pp. 177-183, 2010.

[8] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication", 2nd International Conference on Advances in Future Internet (AFIN), 2010.

[9] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities", *IEEE Transactions on Knowledge and Data Eng.*, vol. 16, no. 7, pp. 843-857, 2004.

[10] H. Hexmoor, "Trust-based protocols for regulating online, friend-of-a-friend communities", *Journal of Experimental & Theoretical Artificial Intelligence,* pp. 1-21, 2009.

[11] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", in Proc. of the Software Engineering Challenges of Cloud Computing (CLOUD'09), ICSE Workshop, 2009.

[12] Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace", A Federal Trade Commission Report to Congress. Washington DC, May 2000.

[13] Federal Trade Commission (FTC), "Protecting Consumer Privacy in an Era of Rapid Change", Preliminary FTC Staff Report, Dec. 2011.

[14] W3C Working Draft, "Tracking Protection Working Group: "Tracking Preference Expression (DNT)", Nov. 2011.

[15] W3C Working Draft, "Tracking Protection Working Group: Tracking Compliance and Scope", Nov. 2011.

[16] A. Cavoukian, "Privacy in the clouds", Identity in the Information Society, Dec. 2008.

[17] Z. Li, E. Chang, K Huang, and F. Lai, "A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform", in Proc. of the 15th IEEE International Symposium on Consumer Electronics, 2011.

[18] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Network Working Group, IETF Request for Comments: 5280, May 2008.

[19] E. Hammer-Lahav (Ed.), D. Recordon, and D. Hardt, "The OAuth 2.0 Authorization Protocol", IETF Network Working Group, draf-ietf-oauth-v2-22, Sep. 2011.

[20] Liberty Alliance, "Identity Federation Framework (ID-FF) 1.2. Specifications", 2004.

[21] F. Hirsch, R. Philpott, E. Maler, "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, March, 2005.

[22] P. Arias, F. Almenares, R. Sánchez, A. Marín and D. Díaz-Sánchez, "Multi-device Single Sign-On for Cloud Service Continuity", in Proc. of 30th IEEE International Conference on Consumer Electronics (ICCE 2012), Las Vegas, Nevada, U.S.A, Jan. 2012.

[23] S. Cantor, F. Hirsch, J. Kemp, R. Philpott, and E. Maler (Eds.), "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, Mar. 2005.

[24] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision", *Decision Support System*, vol. 43, no. 2, pp. 681-644, Elsevier (ed.), 2007.

[25] ETSI, "Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems", PN-fed Draft ETSI GS INS-004 V 0.0.5, Group Specification. Jan. 2010.
[26] S. Cantor, J. Kemp, R. Philpott, and E. Maler (Eds.), "Assertions and Protocols for the (OASIS) Security Assertion Markup Language (SAML) V2.0", OASIS Standard, Mar. 2005.
[27] Entr'ouvert, "Lasso, Free Liberty Alliance Implementation", Jan. 2012.
[28] Entr'ouvert, "Authentic: Liberty-compliant Identity Server", Jan. 2012.
[29] OpenLDAP Foundation, "OpenLDAP (Lightweight Directory Access Protocol.) Software", Jan. 2012.
[30] A. Varga. "OMNet++", Chapter in the book "*Modeling and Tools for Network Simulation*", K. Wehrle, M. Günes, and J. Gross (Eds.), Springer Verlag, 2010.

BIOGRAPHIES

Sánchez Guerrero, Rosa received a Telecom. Eng. degree from Univ. Carlos III de Madrid in 2009 and she obtained the MSc degree in Telematics in 2011. Currently, she works as researcher at the Department of Telematics Eng. in the Univ. Carlos III of Madrid, working within the Pervasive Computing research group. Her research topics include the problem of identity management, security and privacy in healthcare.

Almenárez Mendoza, Florina (M'07) received her Ph.D. degree from the University Carlos III of Madrid (Spain) in 2006 and is currently an associate professor at UC3M. She received an award-winning as Magna CumLaude in her Computer Engineering degree. Her research interests include trust management, identity federation, security in ubiquitous computing, and SIM-based applications. She leads the research activities of the PerLab group in advanced trust models, security architectures for open and dynamic spaces, and identity management.

Arias Cabarcos, Patricia received her Telecom. Eng. degree from Univ. Carlos III of Madrid in 2008 and she obtained the MSc degree in Telematics in 2009. Currently, she is pursuing a PhD at the Department of Telematics Engineering in the Univ. Carlos III of Madrid, working within the Pervasive Computing research group. Her research focuses on the problem of identity management in open and dynamic environments, with special attention to risk analysis and the underlying trust models.

Díaz-Sánchez, Daniel (M'07) received a Telecom. Eng. degree from Univ. Carlos III de Madrid in 2002. He graduated as Master Telematic Engineering (2004) and obtained his PhD (2008) from Univ. Carlos III of Madrid. He works as researcher and teacher at Universidad Carlos III. His research topic is distributed authentication, authorization and content protection activities.

Marín López, Andrés (M'07) received a Telecom. Eng. degree and PhD from the Technical Univ. of Madrid in 1992 and 1996 respectively. He lectures in Computer Networks and Ubiquitous Computing in the Univ. Carlos III de Madrid, as an associate professor. His research interests include ubiquitous computing: limited devices, trust, security services, and security in NGN.