Bernd Zwattendorfer, Klaus Stranacher, Arne Tauber - "Towards a Federated Identity as a Service Model",
Technology-Enabled Innovation for Democracy, Government and Governance
Lecture Notes in Computer Science Volume 8061, 2013, pp 43-57
URL: http://link.springer.com/chapter/10.1007%2F978-3-642-40160-2_5
The original publication is available at www.springerlink.com

Towards a Federated Identity as a Service Model

Bernd Zwattendorfer, Klaus Stranacher, Arne Tauber

E-Government Innovation Center (EGIZ), Graz University of Technology, Graz, Austria
{bernd.zwattendorfer, klaus.stranacher, arne.tauber}@egiz.gv.at

Abstract. Identity management plays a key role in e-Government. Giving the increasing number of cloud applications, also in the field of e-Government, identity management is also vital in the area of cloud computing. Several cloud identity models have already emerged, whereas the so-called "Identity as a Service"-model seems to be the most promising one. Cloud service providers currently implement this model by relying on a central identity broker, acting as a hub between different service and identity providers. While the identity broker model has a couple of advantages, still some disadvantages can be identified. One major drawback of the central identity broker model is that both the user and the service provider must rely on one and the same identity broker for identification and authentication. This heavily decreases flexibility and hinders freedom of choice for selecting other identity broker implementations. We bypass this issue by proposing a federated identity as a service model, where identity brokers are interconnected. This federated identity as a service model retains the benefits but eliminates the drawbacks of the central cloud identity broker model.

Keywords: Cloud Computing, Identity as a Service, Federated Identity as a Service, Identity Broker, Identity Management

1 Introduction

Electronic identity management [1] is the key enabler for reliable identification of users, which is essential in e-Government applications. The main tasks of identity management comprise secure management of identities, management of attributes corresponding to identities in a specific context, and identification and authentication processes [2]. Identification of users is a main requirement for many applications, especially for those which are processing confidential or sensitive data.

Numerous identity management initiatives and systems exist since many years. In the enterprise sector, directory services such as LDAP (Lightweight Directory Access Protocol) [3] or Kerberos [4] are still present. Within the Web, systems or standards such as the Security Assertion Markup Language (SAML) [5], the Liberty Alliance Project[1] (that evolved to the Kantara initiative[2]) or Shibboleth[3] gained increased popu-

[1] http://www.projectliberty.org
[2] http://kantarainitiative.org
[3] http://shibboleth.net

adfa, p. 1, 2011.

larity, to just name a few. Also a couple of research projects covered the topic on identity management, e.g. FIDIS[4], PRIME[5] and PrimeLife[6], or PICOS[7].

Secure identity management also plays an important role for governments. Many European countries have already national eID solutions to be used in public or private sector applications in place since years [6]. Additionally, within Europe the project STORK[8] successfully piloted secure identification and authentication across borders using various national eIDs. Those results are further taken up by its successor project STORK 2.0[9], which started in 2012. In relation to that, the USA introduced its "National Strategy for Trusted Identities in Cyberspace"[10] (NSTIC), which aims on the creation of a secure and trusted identity ecosystem in the US.

In most electronic identity management systems, identity providers are the means of choice for identification of users and authentication at the service provider. Identity providers are usually an essential entity within an identity model. We briefly introduce traditional identity models for central, user-centric, or federated approaches in Section 2.

Given the increasing number of cloud applications, also in the field of e-Government, identification of users gains also more and more importance in the field of cloud computing. Hence, different cloud identity models have already been defined to cover new requirements particularly relating to cloud computing. The main distinctive criterion between these cloud identity models is the entity, which operates the identity provider in relation to the cloud application. We overview these cloud identity models in Section 3. Thereby, the so-called "Identity as a Service"-model [7] specifies the very cloud identity model, which takes best advantage of the cloud computing paradigm. In this model, the identity provider is fully operated in the cloud. This allows for a separation between cloud service providers, which host and operate the application, and cloud service providers, which host and operate the identity provider. Therefore, this model is currently the most promising identity model for cloud-based identity management.

Based on the "Identity as a Service"-model, a couple of so-called cloud identity brokers have already emerged. The identity broker model consists of a central identity broker in the cloud, which acts as a hub between various service and identity providers. The benefit of this approach is decoupling the service provider from multiple identity providers, which in fact facilitates identity management.

Nevertheless, the cloud identity broker model has one major drawback, which has not been solved yet. Users and service providers must rely on the same central identity broker for identification and authentication, if this model is applied. Obviously, this causes strong dependencies on the availability and functionalities of the identity broker. To overcome this issue, we present a new identity model for the cloud relying on

---

4 http://www.fidis.net
5 https://www.prime-project.eu
6 http://primelife.ercim.eu
7 http://www.picos-project.eu/
8 https://www.eid-stork.eu/
9 http://www.eid-stork2.eu/
10 http://www.nist.gov/nstic

a federated approach between multiple identity brokers. This federated identity as a service model retains the benefits, but eliminates the drawbacks of the cloud identity broker model.

The remainder of this paper is structured as follows. In Section 2, we describe traditional identity models and their basic approaches. Section 3 elaborates on existing cloud identity models and classifies them. The subsequent Section 4 introduces the centralized cloud identity broker model based on the "Identity as a Service" approach of Section 3. In Section 5, we present our idea of a federated identity as a service model. Finally, we draw conclusions including future work.

2 Traditional Identity Models

Identification and authentication are by far no new issues, thus several different identity management systems have evolved [8]. In most identity management systems, user identification and authentication at a service provider is carried out via a so-called identity provider. Such an identity provider is responsible for user authentication and transferring user's identity and authentication data to the requesting service provider. Not all systems follow the same methodological approach. For instance, some systems store identity data centrally, whereas other systems follow a federated approach. In this section we briefly describe three types of traditional identity models (central, user-centric, and federated approach) based on the work of Palfrey and Gasser [9]. Distinction criteria are the storage location of identity data (i.e. central database, user domain, or distributed storage). Each of these three models has its specific characteristics. One may have advantages on privacy and user control, another one on scalability. This classification of identity models can also be found in [10]. However, also other classification approaches such as by Alpár, Hoepman, and Siljee [11] exist.

2.1 Central Approach

In the central identity model identity data are stored in a central database at the service provider or the identity provider. Before being allowed to use a service, users usually have to register. This registration has to be done at an affiliated identity provider. Once registered, the identity data are managed and stored in central repositories in the identity provider's domain. When accessing a certain service or application at a service provider, the user must have been successfully authenticated at the identity provider before. After that, the identity provider forwards the identity data to the service provider. In this approach, the user has no control anymore on which data are stored or actually transmitted to the identity information requesting service provider.

2.2 User-centric Approach

In the user-centric model, the user herself always remains the owner of her identity data. Identity data are managed and stored within the user's domain (e.g. on a smart card) and are transferred to a service provider only if the user explicitly gives her

consent. Using this approach, a direct communication channel between the user and the service provider can be achieved and end-to-end security without involving third parties can be guaranteed.

2.3 Federated Approach

In this model, user or identity data are distributed across various identity providers, which have a trust relationship amongst each other. Such trust relationships are usually established on organizational level, whereas enforcement is carried out on technical level. Commonly, the data repositories of the individual identity providers are linked and data can be easily exchanged. In most cases, data exchange takes place based on an agreement of a common identifier for a certain user.

3 Cloud Identity Models

Identification and authentication are not less important in the area of cloud computing. Many e-Government applications are being migrated into the cloud [12] because of cost benefits and higher scalability. Hence, also new cloud identity models, which are tailored to the needs of cloud computing, have emerged. For example, Gopalakrishnan [13] or Cox [14] classify such cloud identity models in their publications. Classification criteria are mainly how and where identities are managed.

Gopalakrishnan concludes that three different identity management patterns in the cloud can be distinguished. Within the first identity management pattern (Trusted IDM Pattern), the identity management system is running within the trusted domain of the cloud provider, which is also hosting the application to be secured by the identity management system. According to her remarks, this pattern is intended for smaller and less scalable cloud models, such as private clouds. In contrast to that, the second identity management pattern (External IDM Pattern) is intended for public clouds, which have high scalability. In this pattern, the identity management system is external to the cloud provider's domain. Identity data and attributes are provisioned through a well-defined protocol, such as SAML [5]. The last and most flexible proposed identity management pattern is the so-called Interoperable IDM pattern. In this pattern, a central identity management system is capable of various authentication technologies and is serving multiple identity consuming service providers.

Cox focuses on public clouds in his identity model classification. In his opinion, identity management in private clouds is obvious, as the identities are managed by the private cloud's organization on their own and no trust relationship to external providers is required. He actually defines four different models and particularly pays attention for provisioning and de-provisioning of users or identities, respectively. In the first model, the cloud service provider generates and manages the identities for the enterprise. There is no external connection to e.g. an enterprise data source. The second model of Cox deals with synchronization. Thereby, the identity management system of an enterprise is synchronized with the user management of the cloud service provider. In the third model, identities are federated. This means that identities

are still managed by the enterprise but are consumed by the cloud service provider. Similar to the Interoperable IDM pattern of Gopalakrishnan, Cox proposes a unified model implementing features of the three other described models as a fourth identity model for the cloud.

Also Goulding [15] classifies such cloud identity models in his whitepaper. The models are based on three use cases. The first model serves the use case of extending the enterprise identity management system up to the cloud. The second model deals with the use case of securing cloud services with an enterprise identity management system. In the third model, identity services are delivered to various applications down from the cloud.

In addition to those classifications, also the Cloud Security Alliance (CSA) [16] discusses three identity architectures for the cloud. In the so-called "hub-and-spoke"-model identities are managed by a central broker or proxy, which serves multiple identity and service providers. In the "free-form"-model, the service provider itself is responsible for managing several and disparate identity providers. The third model described by the CSA constitutes a hybrid model, which synthesizes advantages of the hub-and-spoke model and the free-form model.

In the following, we take the different identity models described before as a basis and classify three cloud identity models, which have already been deployed in several cloud computing environments. In addition, we list advantages and disadvantages of the individual model.

3.1 Identity in the Cloud

The "Identity in the Cloud"-model constitutes the simplest cloud identity model. In this model, the cloud service provider, which hosts the cloud application, also acts as identity provider. This means that the cloud service provider has its own user management, which is used for identification and authentication at its cloud applications. Hence, identity data are stored *in the cloud*. Fig. 1. illustrates the "Identity in the Cloud"- model.

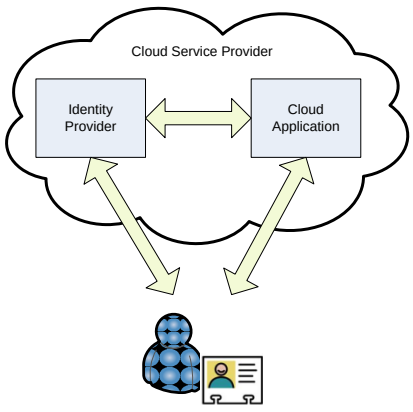

Fig. 1. Identity in the Cloud

This model can be seen as a special case of the traditional central identity model described in section 2.1, where the identity provider and service provider define the same entity for this cloud case. This model has been also discussed by Gopalakrishnan [13] or Cox [14]. Typical practical and already deployed examples of this model are the cloud service providers Google or Salesforce.com. Both cloud service providers host, maintain, and offer their own user management for their Software as a Service (SaaS)[11] applications.

The advantage of this cloud identity model is that organizations can just rely on the existing user management of the cloud service provider. This saves costs and maintenance efforts as no separate user management is required and accounts are created and maintained directly at the cloud service provider, which also hosts the organization's applications. However, this transfer of responsibility to the cloud service provider means also less control for the organization on identity and user data. Additionally, transfer of identity data to the cloud service provider or synchronization (e.g. as discussed by Cox [14]) cannot be easily achieved, because the cloud service provider might rely on different data models in its storage systems.

3.2 Identity to the Cloud

The "Identity to the Cloud"-model actually puts the traditional central identity model of section 2.1 into the cloud domain. In the traditional case, the user management is outsourced by the service provider to an external identity provider. The only difference in the cloud identity model is that the service provider is cloud-based and not only simply web-based. In addition, we assume that the identity provider is not cloud-based equally as in the traditional model. We will consider the scenario of a fully cloud-based identity provider in the next Section 3.3. However, Fig. 2 illustrates the "Identity to the Cloud"-model.

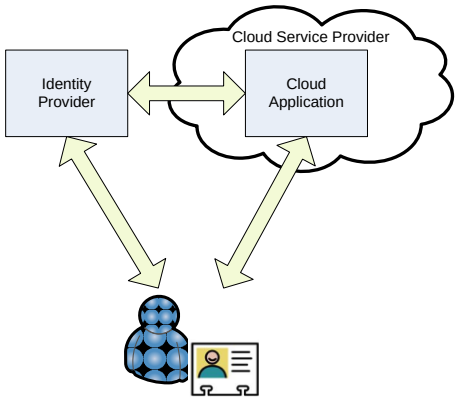

Fig. 2. Identity to the Cloud

[11] Software as a Service (SaaS) constitutes a cloud computing service model, where software is provided as a service by a cloud service provider to customers.

The identity provider is responsible for the complete user management, such as provisioning or de-provisioning of identities, user authentication, etc. The cloud service provider is responsible for the cloud application only and just consumes identity data or information respectively from the identity provider. In other words, identity data is transferred *to the cloud*. Transfer of identity data between the identity and the cloud service provider is usually carried out based on well-defined interfaces and standardized protocols. Such protocols dealing with the secure exchange of identity and authentication data are e.g. SAML [5], OpenID[12], or OAuth[13].

Many existing cloud service providers, in particular public cloud providers such as Google or Salesforce.com, rely on such interfaces or protocols for external identity provisioning. For instance, both mentioned cloud service providers rely on SAML and OpenID for their identity provisioning or so-called Single Sign-On (SSO) interfaces. In contrast to Salesforce.com, Google additionally allows external authentications via OAuth. The use of such interfaces does not only allow the implementation of the traditional central identity model, but moreover enables the application of the federated identity model described in section 2.3.

When applying this model, advantageous is the possibility to re-use existing identity management systems (e.g. an internal identity management system of an organization or enterprise) for external identification and authentication at cloud providers and cloud services. In contrast to the previous model (Identity in the Cloud), no new user management at the cloud service provider or any migration to the cloud service provider is required. While the application or service is operated in the cloud, the user management stays under full control of the individual organization. In contrast to that, an issue might be interoperability (e.g. technical or semantic interoperability). Many cloud service providers, which offer SSO interfaces for external identification or identity federation, rely on standardized protocols. Although standardized protocols should actually guarantee technical interoperability, the implementations of such protocols may have a different behavior, as shown in [17]. In addition, the respective cloud service provider might not support the desired identity protocol for external authentication, which could cause additional implementation efforts and costs at the organization's or enterprise's site. Semantic interoperability constitutes another issue, as user attributes of the external identity provider might not be understood by the cloud service provider. Hence, a thorough attribute mapping between the identity provider and the cloud service provider is required.

3.3 Identity from the Cloud

Within the third introduced cloud identity model identities are provided from an identity provider, which fully resides in the cloud. In fact, identities are provided as a service *from the cloud*. Therefore, the proposed model can also be seen as an "Identity as a Service"-model [7]. Fig. 3 illustrates the so-called "Identity from the Cloud"-model.

---

[12] http://openid.net
[13] http://oauth.net

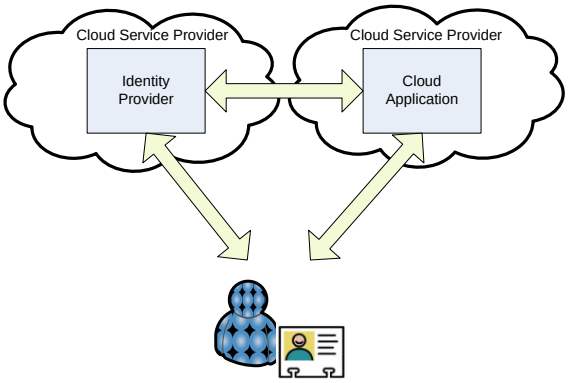

Fig. 3. Identity from the Cloud

In this model, both the identity provider and the application are operated in the cloud. Contrary to the "Identity in the Cloud"-model of Section 3.1, the identity provider need not necessarily be operated by the same cloud service provider that also hosts the application. Needless to say that still just one cloud service provider can operate both, the identity provider and the application. However, the precondition is that the user management of the identity provider is separated from the application's cloud service provider.

Basically, this cloud identity model is independent of the underlying cloud deployment or operational model. In fact, this "Identity as a Service"-model can be operated in a public, private, or community cloud. Due to the interconnection of different cloud deployment models (the cloud model used for operating the identity provider might be different than the cloud model for hosting the application), this cloud identity model can also be seen as hybrid cloud model. However, although within the illustrating Fig. 3 only cloud applications are shown acting as identity consuming services, this "Identity as a Service"-model can also be applied to traditional web-based applications of service providers.

Besides cost advantages and less maintenance efforts due to the outsourcing of identity management tasks into the cloud, the main advantage of this model is the separation of the cloud service providers. I.e., the cloud service provider for the application is usually different to the cloud service provider acting as identity provider. This allows organizations or enterprises an individual selection, which service provider they are going to trust to host and maintain their user management. A requirement for selecting a particular cloud service provider to act as identity provider might be, for instance, specific data protection regulations, such as enforcement that sensitive data is only allowed to be stored in selected or specific countries. Disadvantages of this model are, however, the need to move identity data into the cloud and thus trust a third party (the cloud service provider) for the user management. Furthermore, although complexity is decreased due to the take up of management tasks through the cloud service provider, organizations or enterprises need to think about how identity data can be easily transferred to this cloud service provider.

4 The Cloud Identity Broker Model

The “Identity as a Service”-model seems to be a promising concept for identity management in the cloud. In the previous section, we provided a more general view on this model, just illustrating the basic idea that identities are provided from the cloud. However, according to the Cloud Security Alliance [16] or Huang et al. [18] this “Identity as a Service”-model can be more seen as an identity broker model. This means that the identity provider in the cloud, which provides identities as a service, acts as central identity broker between various other identity providers and several service providers. In other words, the cloud identity provider plays some kind of hub between multiple service and identity providers [16]. Fig. 4 gives a more detailed view on the “Identity as a Service” model with central identity broker functionality.

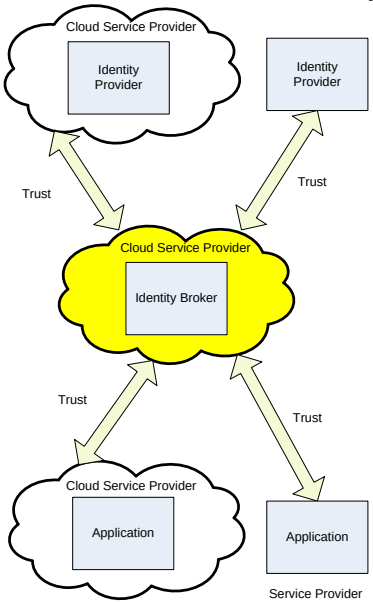

Fig. 4. Identity as a Service using a central Identity Broker

The main idea of this model is to decouple the service provider from multiple identity providers. Hence, instead of having multiple dependencies to various identity providers, only one strong dependency to the identity broker is given. This has further advantages, both on technical and organizational level. On technical level, the service provider only needs to implement the communication protocol to the identity broker and thus can ignore specific protocols of the individual identity providers. To lower the implementation efforts for service providers, the identity broker can offer standardized and well-established interfaces and protocols for secure data exchange (e.g. SAML, OpenID, etc.), where service providers can easily connect to. On organizational level, the strength of this model is aggregating multiple different trust relationships between service and identity providers to just one, namely between the service

provider and the identity broker. The identity broker now takes over these various trust relationships with the individual identity providers. In other words, the trust relationship between the service provider and the identity provider is brokered through the cloud identity broker. Having just one trust relationship simplifies the contractual model for the service provider. Needless to say that this centralized model has one general drawback. If the identity broker breaks down, users are cut off service provisioning. Nevertheless, this risk is not specific to this model and can be found in several other identity models, where identification and authentication are outsourced to an external entity.

The identity broker model is not new and has already been implemented and deployed by several organizations. For instance, the Cloud SSO[14] product of Intel constitutes a ready implementation. Intel Cloud SSO offers strong user authentication and connectivity to different identity stores and more than 100 external Software as a Service (SaaS) applications. For achieving that, Intel Cloud SSO relies on existing federation interfaces provided by the different SaaS vendors. Another implementation of the identity broker model constitutes the results of the SkIDentity project[15]. SkIDentity especially focuses on eIDs, providing secure access to cloud services by supporting various types of eIDs. Hence, the SkIDentity implementation might also be interesting for e-Government adoption. In contrast to Intel Cloud SSO, for identity provisioning SkIDentity requires a special connector module to be installed at the cloud service provider. Other products implementing the identity broker model are e.g. RadiantOne's Cloud Federation Service[16], McAfee's Cloud Identity Manager[17], VMWare's Horizon[18], or Fugen's Cloud ID Broker[19].

Although we have identified several benefits of this model, still some drawbacks can be found. One major drawback is that users and service providers must rely on the same central service, the identity broker. This means that both the service provider and the user must have a trust relationship with the same authenticating authority. In terms of trust, this model is similar to the traditional central identity model (see Section 2.1), which uses a pairwise trust model as described in [19]. Brokered trust only comes into play between the service providers and the different identity providers.

In addition, another disadvantage is that both the service provider and the user are more or less dependent on the functionality and features of the identity broker. For instance, on the one hand service providers are dependent on the interfaces the identity broker supports. If the identity broker suddenly quits the support of a particular interface, the service provider is cut off of any identity service and requires much effort for implementing another supported interface. On the other hand, users are dependent on the type and number of identity providers the identity broker supports. If a user wants to authenticate at a specific identity provider, which has no affiliation

---

[14] http://www.intelcloudsso.com
[15] http://www.skidentity.com
[16] http://www.radiantlogic.com/products/radiantone-cfs
[17] http://www.mcafee.com/uk/products/cloud-identity-manager.aspx
[18] http://www.vmware.com/products/desktop_virtualization/horizon-application-manager/overview.html
[19] http://fugensolutions.com/cloud-id-broker.html

with the identity broker, or if a user wants to use a particular authentication mechanism, which is not supported by the identity broker, accessing the service provider becomes impossible. In other words, the user has actually no real free choice which identity provider to use and is dependent on the support of the identity broker.

To bypass these disadvantages, we propose a new identity model for the cloud. This new model relies on a federated approach between multiple identity brokers. We will discuss this federated identity broker model or federated identity as a service model in more detail in the next section.

5 Federated Identity as a Service Model

A federated identity as a service (or federated identity broker model) solves the issue on being dependent on just one and the same identity broker for both, the service provider and the user. In this federated model, users and service providers do not need to rely on the same identity broker as authenticating authority. Both can actually contract their individual identity broker of choice, which offers greater flexibility. In addition, the individual identity broker can easier respond on individual requirements, either from the user or the service provider. Such requirements might be some local or domestic regulations specific to a country. This means for example, a user can rely on her desired identity broker, which acts compliant to such local or national regulations. Although there is no direct trust relationship between the user and the affiliated identity broker of the service provider, due to identity broker federation the user is still able to authenticate at the service provider. Fig. 5 illustrates this federated identity as a service model.

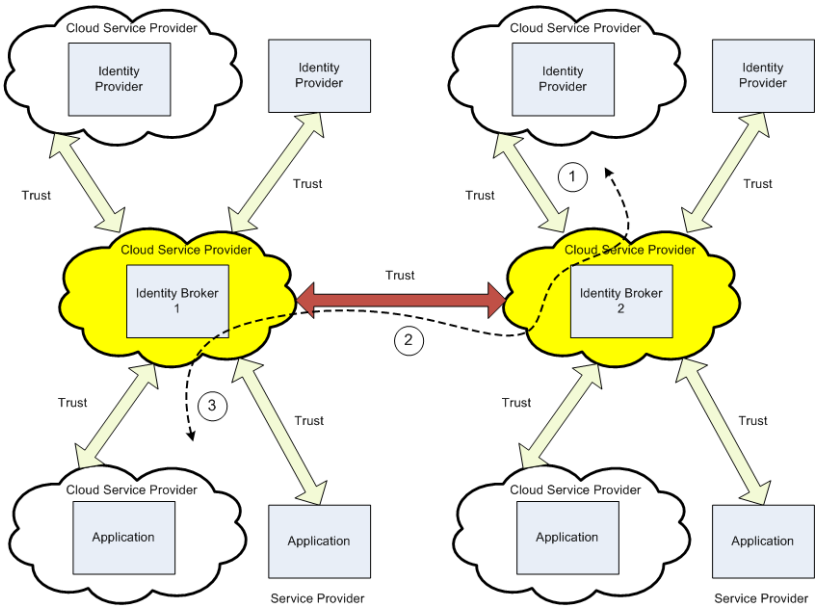

Fig. 5. Federated Identity as a Service Model

In this federated model it is possible that the service provider has a contractual relationship with identity broker 1, whereas the user has a contractual relationship with identity broker 2. In addition, both identity brokers have some kind of trust and contractual relationship amongst each other. Hence, this model fully features the brokered trust model according to [19] across multiple identity brokers.

Having a closer look at the information and process flow, in a first step the user contacts a service provider by stating that she wants to consume a protected resource. For accessing this protected resource, proper identification and authentication is required. The service provider has a contractual and trust relationship with identity broker 1. However, the user only has a contractual and trust relationship with identity broker 2, which supports – in contrast to identity broker 1 - the identity provider the user actually wants to use for authentication. To use this intended identity provider, in a next step the user is forwarded to her affiliated identity broker 2. After that, identity broker 2 initiates the identification and authentication process with the desired identity provider. The user provides appropriate credentials for successful authentication at the desired identity provider. If authentication was successful, identification and authentication data will be transmitted to identity broker 2. Subsequently, identity broker 2 forwards the user's identity and authentication data to identity broker 1, which in turn transmits these data to the service provider. Based on the received data, the service provider either grants or denies access to the protected resource.

In this model, there are three communication channels (cf. Fig. 5) where identity data are transferred, namely between

1. Identity Provider and Identity Broker 2
2. Identity Broker 2 and Identity Broker 1
3. Identity Broker 1 and Service Provider

The communication channels 1 (between identity provider and identity broker 2) and 3 (between identity broker 1 and service provider) can be covered by existing identity protocols, such as SAML, OAuth, etc. However, for communication channel 2 (between identity broker 2 and identity broker 1) it must be investigated whether existing protocols might be sufficient or whether new protocols need to be developed.

In the following, we list some requirements that must be fulfilled to set up and build such a federated identity as a service model. Thereby, we distinguish the requirements based on five different aspects (functional, technological, organizational, legal, and business aspects).

5.1 Functional Requirements

For such a system, the support of basic identity management functionality such as registration, collection and proofing of attributes, credential management, or claims issuance and transformation by the different identity brokers are required. In addition, the vision is to not only support natural persons, but also legal persons such as companies or governments as users. This support might also enable person to person transactions (e.g. two natural persons are exchanging identity data via this network), without involving a service provider in between.

In particular, the framework should be designed user-centric (information control remains with the individual) and should be claims-based. User-centricity means that in every transaction the user always has maximum control over her personal data. The use of claims instead of attributes particularly preserves privacy. By using claims, only the minimum set of personal data required may be disclosed. In addition, single sign-on (SSO) should be supported to allow seamless authentication between various service providers without re-authentication or any further interactions. Finally, the network should be simple to use and especially transparent and auditable to allow for compliance with legal regulations.

5.2 Technological Requirements

As a main technological requirement, the proposed framework should be secure and should automatically preserve users' privacy. In addition, the brokered trust pattern should be modeled accordingly at technological level. This implies the implementation of a proper trust protocol.

Furthermore, the technological framework should build upon existing infrastructures and rely on open standards wherever possible. Application programing interfaces (APIs) should be provided to adopt further applications and business models. Finally, the technical implementation of such a framework should be location independent and agnostic of the user's client used for accessing the network.

5.3 Organizational Requirements

The use of open standards constitutes also an important organizational requirement because it facilitates interoperability between network entities. Moreover, if possible, existing standards should be relied on instead of developing new ones.

A reliable trust framework and meta model needs to be taken up or defined to ensure interoperability between different entities, such as identity brokers. Especially, on semantic level, regulations or guidelines should be defined. This particularly includes a common understanding on identity attributes or claims, which are transferred. Additionally, a common understanding on used authentication mechanisms, e.g. authentication assurance levels as defined in STORK [20], is required. Furthermore, data verification processes need to be defined.

5.4 Legal Requirements

Especially for national identity management systems, compliance with data protection laws or regulations defines an essential requirement. For instance, when supporting national eID solutions, the identity brokers must act compliant to any specific national law or regulation. This requirement might involve not only one but several laws and regulations. However, data protection will be one of the most important legal requirements to suffice. In addition, legal requirements might also include the support of special contracts, certifications, or terms of use according to national laws.

5.5 Business Requirements

Entering and the use of this identity management network in the cloud will probably be not free of charge. Therefore, appropriate accounting and pricing models need to be developed. Moreover, incentives must be generated to involve businesses to participate in such a network and to cooperate. During business model generation, focus should also lie on the re-use of existing infrastructure and API provisioning for further business generation.

6 Conclusions

Identity management and the processes of identification and authentication are essential when protected applications or resources need to be accessed. Identity management is of particular importance in e-Government. While identity management does not define a new topic, identity management in the cloud brings up new challenges. Traditional identity models have already been transferred to the cloud, hence different cloud identity models have emerged. Depending on the cloud identity model, identity data are either provided in the cloud, to the cloud, or from the cloud. The most promising cloud identity model is the "Identity from the Cloud"-model, which can also be called "Identity as a Service"-model. As the name already indicates, identities are provided from a cloud service provider as a service. Current implementations of this model rely on the so-called identity broker model, where a central identity broker acts as a hub between several identity and service providers. While this model has a couple of advantages, also one major drawback can be identified. Both the user and the service provider must rely on the same identity broker during an identification and authentication process, which causes strong dependency on the central identity broker. To bypass this issue, we proposed a federated identity broker model (federated identity as a service model), which guarantees freedom of choice on the desired identity broker for the user and the service provider. Furthermore, we listed requirements (functional, technological, organizational, legal, and business requirements) that must be taken into account when setting up and implementing such a federated identity broker approach.

Future work will include further research on how these requirements can be fulfilled for setting up such a federated identity broker model. In more detail, this will include research on the required trust framework and the transport protocol required for secure message and data exchange between identity brokers.

References

1. Bertino, E., Takahashi, K.: Identity Management: Concepts, Technologies, and Systems, Artech House Inc, 2010
2. ISO/IEC JTC 1/SC 27/WG 5: A framework for IdM
3. Sermersheim, J.: Lightweight Directory Access Protocol (LDAP): The Protocol. RFC 4511. Internet Engineering Task Force (IETF), 2006

4. Neuman, C., Yu, T., Hartman, S. and Raeburn, K.: The Kerberos Network Authentication Service (V5). RFC 4120. Internet Engineering Task Force (IETF), 2005
5. Lockhart, H., Campbell, B: Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft 02, 2008
6. Siddhartha A.: National e-ID card schemes: A European overview. Inf. Secur. Tech. Rep. 13, 2, pp. 46-53, 2008
7. Emig, C., Brandt, F., Kreuzer, S., Abeck, S.: Identity as a Service – Towards a Service-Oriented Identity Management Architecture. Dependable and Adaptable Networks and Services (pp. 1–8), 2007
8. Bauer, M., Meints, M., and Hansen, M.: D3.1: Structured Overview on Prototypes and Concepts of Identity Management System, FIDIS, 2005
9. Palfrey, J., Gasser, U.: Digital Identity Interoperability and eInnovation, Case Study. Berkman Publication Series, 2007
10. Jøsang, A., Pope, S.: User centric identity management. In AusCERT Asia Pacific Information Technology (pp. 1-13), 2005
11. Alpár, G., Hoepman, J.-H., and Siljee, J.: The Identity Crisis - Security, Privacy and Usability Issues in Identity Management. CoRR. 2011
12. Kurdi, R.; Taleb-Bendiab, A.; Randles, M.; Taylor, M.: E-Government Information Systems and Cloud Computing (Readiness and Analysis), Developments in E-systems Engineering (DeSE), 2011 , pp.404-409, 2011
13. Gopalakrishnan, A.: Cloud Computing Identity Management. SETLabs Briefings, vol. 7, no. 7, pp. 45-55, 2009.
14. Cox, P.: How to Manage Identity in the Public Cloud. InformationWeek reports, no. March, 2012
15. Goulding, J.: Identity and Access Management for the Cloud: CA's strategy and vision. Whitepaper, CA Cloud Business Unit, Mai 2010
16. Cloud Security Alliance: SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0, 2011
17. Zwattendorfer, B., Tauber, A.: Secure Cloud Authentication using eIDs. In: Proceedings of IEEE CCIS2012 (pp. 515-519), 2012
18. Huang, H. Y., Wang, B., Liu, X. X., and Xu, J. M.: Identity Federation Broker for Service Cloud. 2010 International Conference on Service Sciences (pp. 115–120), 2010
19. Boyen, S., Ellison, G., Karhuluoma,, G., MacGregor, W., Madsen, P., Sengodan, S. Shinkar, S. and Thompson,, P.: Trust Models Guidelines. Draft. OASIS, 2004
20. Hulsebosch, B., Lenzini, G. and Eertink, H.: D2.3 - Quality authenticator scheme. STORK Deliverable, 2009