Bernd Zwattendorfer, Thomas Zefferer, Klaus Stranacher - "An Overview of Cloud Identity Management-Models",
10th International Conference on Web Information Systems and Technologies (WEBIST), 2014, pp. 82-92
http://www.webist.org/?y=2014

An Overview of Cloud Identity Management-Models

Bernd Zwattendorfer, Thomas Zefferer and Klaus Stranacher
Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{*bernd.zwattendorfer, thomas.zefferer, klaus.stranacher*}*@iaik.tugraz.at*

Keywords: Cloud, Cloud Computing, Cloud Identity Management-Model, Identity Management

Abstract: Unique identification and secure authentication are essential processes in various areas of application, e.g. in e-Government, e-Health, or e-Business. During the past years several identity management-systems and models have evolved. Many organizations and enterprises or even countries for their national eID solutions rely on identity management-systems for securing their applications. Since more and more applications are migrated into the cloud, secure identification and authentication are also vital in the cloud domain. However, cloud identity management-systems need to meet slightly different requirements than traditional identity management-systems and thus cannot be clustered into the same model types or categories. Therefore, in this paper we give an overview of different cloud identity management-models that have already emerged up to now. We further compare these models based on selected criteria, e.g. on practicability and privacy aspects.

1 INTRODUCTION

Secure and reliable identity management (IdM) plays a vital role in several security-sensitive areas of applications, e.g. in e-Government, e-Business, or e-Health. An identity management-system helps online applications to control access for users to protected resources or services. However, identity management is no new topic and several identity management-approaches and systems have already emerged over time. A comprehensive overview on identity management-systems is given in (Bauer et al., 2005).

Due to the increasing number of cloud computing adoption and the deployment of security-sensitive cloud applications, secure identity management becomes also more and more important in the cloud domain. In addition, outsourcing identity management-systems to the cloud can bring up several benefits such as higher scalability or cost savings, since no in-house infrastructure needs to be hosted and maintained. However, the field of cloud identity management is still new and not extensively investigated yet. Therefore, the aim of this paper is to overview different cloud identity management-models, discuss advantages and disadvantages of the individual models, provide a comprehensive survey, and finally compare them based on selected criteria. The criteria for the comparison have been selected by focusing on practicability and privacy, since one of the main issues of cloud computing is the loss of data protection and privacy (Pearson and Benameur, 2010), (Zissis and Lekkas, 2012), and (Sen, 2013).

The paper is structured as follows. Section 2 classifies existing traditional identity management-models and their implementations. Section 3 surveys existing cloud identity management-models and describes their benefits and drawbacks. These models are compared in Section 4 based on selected criteria. Finally, conclusions are drawn in Section 5.

2 TRADITIONAL IDENTITY MANAGEMENT-MODELS

An identity management-system usually involves four entities (Bertino and Takahashi, 2011). A *service provider* (SP) provides different online services to *users*. Before being allowed to consume such services, a user has to successfully identify and authenticate. Therefore, the user usually identifies and authenticates at a so-called *identity provider* (IdP). The identity provider is then in charge of providing the users identity data and supplementary authentication results to the service provider in a secure way. Finally, a *control party*, which is usually a law or regulation enforcing body, needs to investigate identity data transactions, e.g. for data protection reasons. Hence, main purpose of such control party is auditing. Figure

1 illustrates the communication process in an identity management-system including all four entities.

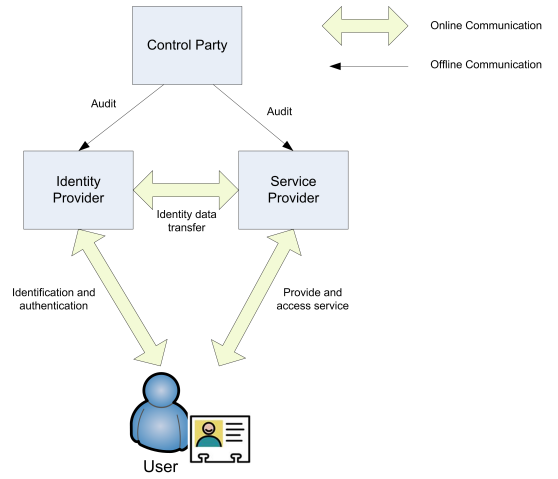

Figure 1: Entities involved in an identity management-system

Over time, several identity models involving these four entities and supporting similar but slightly different use cases have evolved. Some of these models have advantages in scalability, others in privacy or user control. In the following subsections we briefly describe the most important models based on the work of (Cao and Yang, 2010), (Dabrowski and Pacyna, 2008), (Dbrowski and Pacyna, 2008), (Jøsang et al., 2005), (Jøsang and Pope, 2005), (Jøsang et al., 2007), and (Palfrey and Gasser, 2007). For simplicity, we skip a discussion of the control party in all subsequent models because its functionality remains the same in all models.

2.1 Isolated Model

The *isolated model* is basically the simplest traditional identity model. In this model, the service provider and identity provider merge, hence identification and authentication are directly carried out at the service provider. In addition, the functionality of the identity management-system (creating, maintaining, or deleting identities) can only be used by this specific service provider. If a user wants to access services of another service provider, she needs to register at the other service providers identity management-system again. This further means that each individual service provider has to store and maintain the identity data and credentials of the user separately. While this still may not be a huge burden for service providers, the diversity of credentials for accessing various service providers may become unmanageable for users (Jøsang and Pope, 2005). This model can still be found by service providers on the Internet.

2.2 Central Model

The *central identity model* avoids diverse identity management-systems, where the user has to register separately. Instead, the identity management-system is outsourced by several service providers to a central identity provider. The identity provider takes over all identity-related functionality for the service provider, including credential issuance, identification and authentication, and the management of the identity lifecycle in general (Bertino and Takahashi, 2011). Furthermore, in this model users' identity data are stored in a central repository at the identity provider and service providers do not need to maintain identity data in their own repositories (Cao and Yang, 2010). For authentication at a service provider, the user has to identify and authenticate at the identity provider before. The identity provider then assembles a token including all necessary identity and authentication information of the user and transmits it to the service provider[1]. (Jøsang et al., 2005) further distinguish the domain model for the identifier used. In the *common identifier model* one and the same identifier is used for identification at all service providers. In contrast to that, in the *meta identifier domain model* separate identifiers are used for identification at the individual service providers. However, all separate identifiers map to a common meta identifier at the identity provider to uniquely identify the user. Typical examples implementing this approach are Kerberos (Neuman et al., 2005) or the Central Authentication Service (CAS)[2].

2.3 User-Centric Model

While in the central model all identity data of the user are stored in the domain of the identity provider, in the *user-centric model* all identity data are stored directly in the users domain, e.g. on a secure token such as a smart card. The main advantage of this model is that the user always remains the owner of her identity data and stays under their full control (Dbrowski and Pacyna, 2008). Identity data can only be transferred by an identity provider to a service provider if the user explicitly gives her consent to do so. Compared to the central model, this tremendously increases users' privacy. (Jøsang and Pope, 2005) discuss in detail this user-centric approach. Typical examples implementing this model are Windows CardSpace[3] or var-

[1] Different approaches exist; hence identity data can be either pushed to or pulled from the service provider.

[2] http://www.jasig.org/cas

[3] http://msdn.microsoft.com/en-us/library/vstudio/ms733090\%28v\=vs.90\%29.aspx

ious national eID solutions such as the Austrian citizen card (Leitold et al., 2002) or the German eID (Frommm and Hoepner, 2011).

2.4 Federated Model

In the *federated model* identity data are not stored in a central repository but are rather stored distributed across different identity and/or service providers. No single entity is fully controlling the identity information (Palfrey and Gasser, 2007). The distributed identity data of a particular user are linked usually by the help of a common identifier[4]. All identity providers and service providers, which take part in such a federation, share a common trust relationship amongst each other. The trust relationship is usually established on organizational level whereas enforcement is carried out on technical level. This federated model particularly supports identification and authentication across different domains, which paves the way for cross-domain single sign-on (Cao and Yang, 2010). Popular examples of this approach are the Security Assertion Markup Language (SAML)[5], Shibboleth[6], or WS-Federation (Kaler and McIntosh, 2009).

3 CLOUD IDENTITY MANAGEMENT-MODELS

Cloud computing is currently still one of the most emerging trends in the IT sector. Many applications are already migrated to the cloud because of its benefits such as cost savings, scalability, or less maintenance efforts (Armbrust et al., 2009). Due to the increasing number of cloud applications, secure identity management is equally important for cloud applications as for traditional web applications. Hence, new cloud identity management-models have already emerged, which particularly take the properties of cloud computing into account. (Cloud Security Alliance, 2011), (Cox, 2012), (Gopalakrishnan, 2009), (Goulding, 2010), or (Zwattendorfer et al., 2013) already describe cloud identity management-models in their publications. We take these publications as a basis to give an overview of different existing cloud identity management-models. In the following subsections we describe the individual models in more detail and explain how and where identities are stored and managed.

[4]It is not necessary that the common identifier is shared. Different identifiers mapping to the same user are also possible (Cao and Yang, 2010).

[5]http://saml.xml.org

[6]http://shibboleth.net

3.1 Identity in the Cloud-Model

The *Identity in the Cloud-Model* is similar to the *isolated identity model* described in Section 2.1. Again, identity provider and service provider merge also in this model. This means for the cloud case that the cloud service provider, which hosts the application, is also responsible for the identity management. Figure 2 illustrates this model.

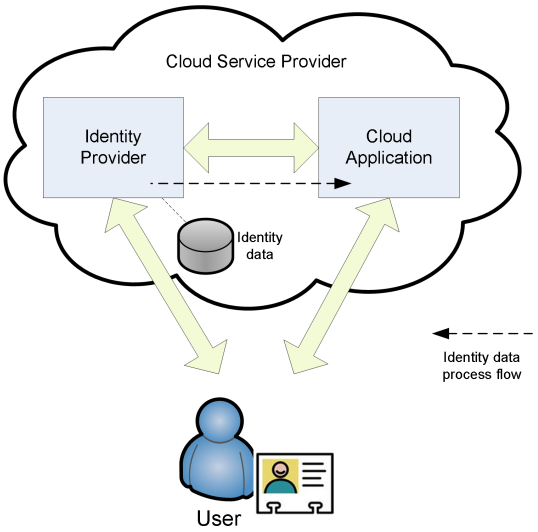

Figure 2: Identity in the Cloud-Model

Identity data of users, who are accessing the cloud application, are directly stored in the domain of the cloud service provider. Hence, the user has actually no control which data are processed in the cloud. Cloud service providers which already use this model for their Software as a Service (SaaS) applications are for instance Google or Salesforce.com. They offer their own user management to their customers for managing their own identities. The main advantage of this model is that organizations do not need to host and maintain their own identity management-system but can simply rely on an existing one, which will be maintained by the cloud service provider. Needless to say that costs can be decreased at an organization when applying this model. However, the use of this model also shifts responsibility in terms of security and privacy to the cloud service provider and the organization more or less looses control over the identity data stored and managed in the cloud.

3.2 Identity to the Cloud-Model

The *Identity to the Cloud-Model* is similar to the traditional *central identity model*. Also in this model, the identity provider takes over the tasks regarding identity management for the service provider. How-

ever, the main difference in this model is that the service provider and its applications are cloud-based. This further means that in this model the identity provider is not deployed in the cloud, which avoids unnecessary identity data disclosure to a cloud service provider. Figure 3 illustrates the *Identity to the Cloud-Model*.

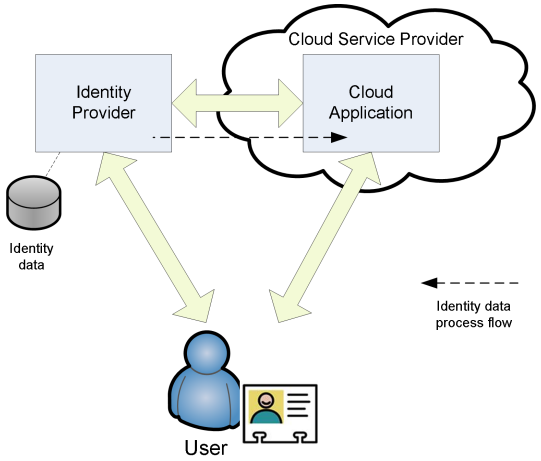

Figure 3: Identity to the Cloud-Model

In more detail, the complete user and identity management is still hosted by the organization e.g. in one of its data centers. Before gaining access to a cloud application, users have to authenticate at the identity provider first. After that, the identity provider transfers appropriate identity and authentication data to the cloud service provider through well-defined and standardized interfaces. Google or Salesforce.com, for instance, rely on SAML, OpenID[7], or OAuth[8] for these interfaces and external identity provisioning.

Appliance of this model has the advantage that an existing identity management-infrastructure of an organization can be re-used. Users are identified and authenticated at the cloud application by the use of this external identity management-system. No new user management has to be created or migrated to the cloud service provider. The organization remains under control of the identity data and provides it to the cloud service provider just on demand. However, interoperability issues may arise due to the use of external interfaces. For instance, a common agreement on the attributes transferred (e.g. format or semantic) between the identity provider and the cloud service provider must be given. In addition, the identity provider must support the interface provided by the cloud service provider.

[7] http://openid.net
[8] http://oauth.net

3.3 Identity from the Cloud-Model

The *Identity from the Cloud-Model* fully features the cloud computing paradigm. In this case, both the cloud application and the identity provider are operated in the cloud. However, in contrast to the *Identity in the Cloud-Model* of Section 3.1 both entities are operated by distinct cloud service providers. Since identities are provided as a service from the cloud, this model is also named "Identity as a Service Model" (Ates et al., 2011). Google or Facebook are for instance such providers, when using the authentication functionality for other services than their own (Google Accounts Authentication and Authorization[9] or Facebook Login[10]). Figure 4 illustrates this model.

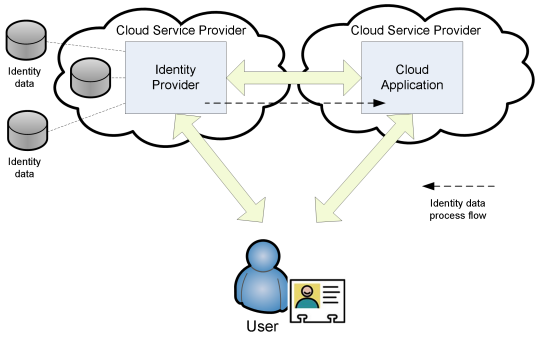

Figure 4: Identity from the Cloud-Model

By applying this model, an organization can benefit from the pure cloud computing advantages such as high scalability or elasticity. Besides that, compared to the previous cloud identity management-models the advantage of this model is the separation of cloud service providers. In this model, organizations can select their preferred identity provider in the cloud. This is particularly important because the organization needs to trust the identity provider, which is responsible for the organization's identity and user management. Organizations must be careful in cloud service provider selection, as e.g. legal implications such as data protection regulations might hinder the selection of a provider which stores identity data in a foreign country.

3.4 Cloud Identity Broker-Model

The *Cloud Identity Broker-Model* can be seen as an extension to the *Identity from the Cloud-Model*. In this *Cloud Identity Broker-Model*, the identity provider in the cloud acts now as an identity broker

[9] https://developers.google.com/accounts
[10] https://developers.facebook.com/docs/facebook-login

in the cloud. In other words, the cloud identity broker is some kind of hub between one or more service providers and one or more identity providers. Figure 5 illustrates this model.

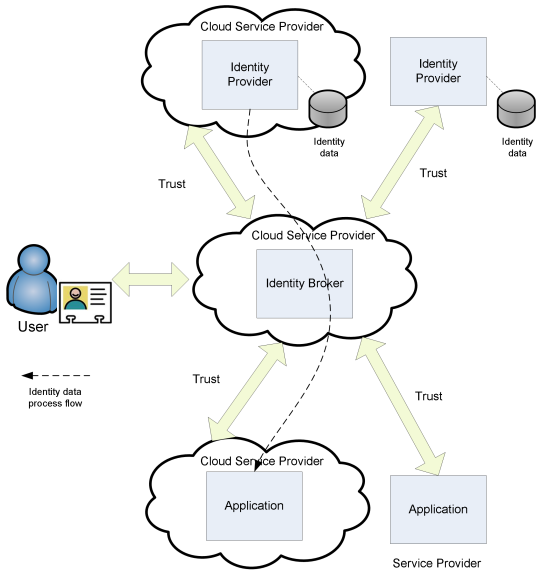

Figure 5: Cloud Identity Broker-Model

The basic idea behind this model is to decouple the service provider from integrating and connecting a vast amount of identity providers. If no broker is used, a single service provider has to implement all interfaces for communication with the individual identity providers if the service provider wants to support them. By applying the broker concept, the identity broker hides the complexity of the individual identity providers from the service provider. This further means that the service provider just needs to implement one interface, namely the one to the identity broker. All other interfaces are encapsulated by the identity broker and tailored or mapped to the service provider's interface. In addition, for the service provider only one strong trust relationship between the service provider and the identity broker is required. All other trust relationships with the individual identity providers are "brokered" by the identity broker. Deploying the broker in the cloud makes this model even more powerful. Due to the cloud advantages of nearly unlimited computing resources and scalability, a high number of active connections and identification/authentication processes at the broker can be easily absorbed by the cloud.

Nevertheless, still some disadvantages can be found in this model. One disadvantage is that both the user and the service provider are dependent on the functionality the cloud identity broker supports. If the identity broker does not support the desired identity provider the user wants to use for authentication, the service provider cannot provide its services to the user. Furthermore, if the broker does not support the communication interface to the service provider anymore, the service provider is cut off from any other identity provider. However, probably the main issue is that identity data runs through the cloud identity broker in plaintext. As already mentioned before, privacy issues concerning the cloud service provider might hinder adoption of this cloud-based identity management-service (Pearson and Benameur, 2010).

The *Cloud Identity Broker-Model* has already been implemented by some organizations. McAfee Cloud Single Sign On[11], the SkIDentity[12] implementation, or the Cloud ID Broker[13] of Fugen are just a few examples. Further details on this model can be found in (Cloud Security Alliance, 2011), (Huang et al., 2010), or (Zwattendorfer et al., 2013).

3.5 Federated Cloud Identity Broker-Model

The *Federated Cloud Identity Broker-Model* combines the traditional *federated identity model* with the newly *Cloud Identity Broker-Model*. This combined model has been introduced by (Zwattendorfer et al., 2013) and aims on eliminating the drawbacks of the central *Cloud Identity Broker-Model*. The general architecture is illustrated in Figure 6, showing the federation of two different cloud identity brokers.

Compared to the simple *Cloud Identity Broker-Model*, in this federated model users and service providers do not need to rely on one and the same identity broker. Actually, both the user and the service provider can rely on the individual broker of their choice. This eliminates the drawback for both the user and the service provider of being dependent on the same identity broker. On the one hand, users can simply select the identity broker that supports all their desired identity providers (Identity Broker 1 in Figure 6). On the other hand, service providers can select the broker that e.g. supports a specific communication interface (Identity Broker 2 in Figure 6). Hence, referring to Figure 6 the communication process flow between identity provider and service provider is brokered through the two Identity Brokers 1 and 2.

While this model eliminates some problems of the *Cloud Identity Broker-Model*, the issue of plain identity data transfer between and through cloud service

[11] http://www.mcafee.com/us/products/cloud-single-sign-on.aspx

[12] http://www.skidentity.com

[13] http://fugensolutions.com/cloud-id-broker.html

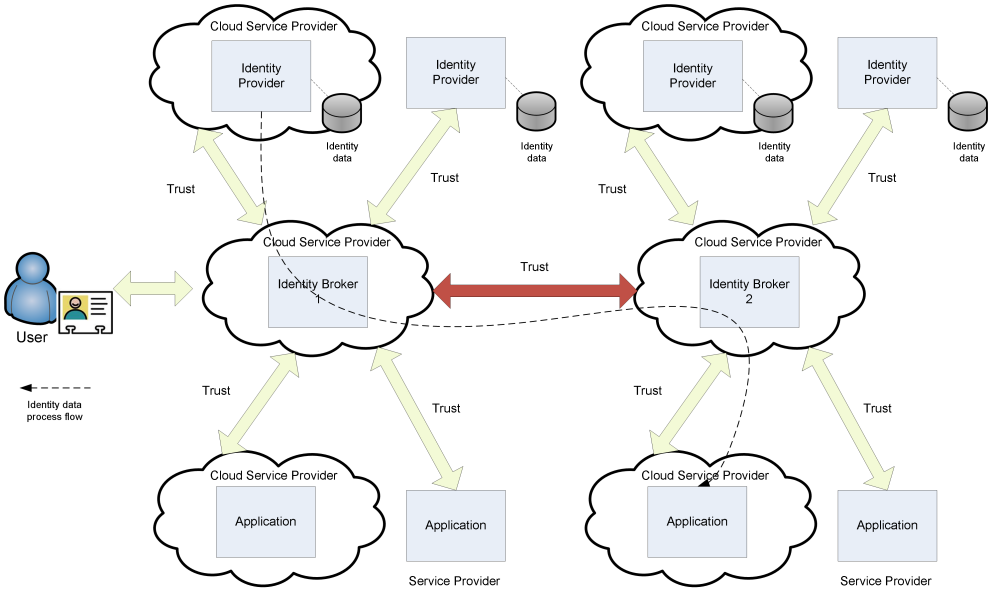

Figure 6: Federated Cloud Identity Broker-Model

providers still persists. To bypass such privacy issue, the following two models had been introduced.

3.6 BlindIdM-Model

The *BlindIdM-Model* has been introduced by (Nuñez et al., 2013) and (Nuñez and Agudo, ress)[14] and can also be seen as an extension and alteration of the *Identity from the Cloud-Model*. The basic idea is principally the same, however, this model enables identity data storage and data processing also by semi-trusted identity providers[15] in the cloud. In fact, the identity provider in the cloud can provide identity data to service providers without actually knowing the contents of these data. Hence, the identity provider provides these data in a blind manner (Nuñez et al., 2013). This particularly preserves users' privacy, as only blinded data is transferred through the cloud identity provider and the cloud provider has no possibility to inspect these data.

The identity data being transferred are actually blinded by using a proxy re-encryption scheme[16] (Green and Ateniese, 2007) (Ateniese et al., 2006). In more detail, during identity management setup and user registration the organization stores the users' identity data in encrypted format at the cloud identity provider. Thereby, the private key is kept confidential by the organization, hence the cloud provider is not able to decrypt the stored identity data. In addition, the organization generates a re-encryption key for the identity provider[17], which allows the re-encryption from the stored data encrypted for the cloud identity provider into other encrypted data, which however can be decrypted by the service provider. During an authentication process, the cloud identity provider then just re-encrypts the desired identity data of the user for the service provider. The practical applicability of the *BlindIdM-Model* has been shown by an implementation in connection with OpenID (Nuñez et al., 2012).

3.7 Privacy-Preserving Federated Cloud Identity Broker-Model

The main aim of this model is – similar to the *BlindIdM-Model* – an improved privacy-preservation for the user. Thereby, the same concept of "blinding" identity data is applied to the basic *Federated Cloud Identity Broker-Model*. Hence, this model combines the advantages of the *Federated Cloud Identity Broker-Model* with the advantages of the *BlindIdM-Model*. Furthermore, this model can again be applied when having semi-trusted cloud identity brokers. The

[14] a similar approach has been introduced by (Zwattendorfer and Slamanig, 2013a)

[15] A semi-trusted identity provider is an identity provider that works correctly but may be interested in inspecting private data. In other words, the identity provider acts *honest but curious*.

[16] By using proxy re-encryption a semi-trusted proxy can alter a ciphertext, which has been encrypted for person A, in such a way that it can be decrypted by person B. Thereby, the proxy gains no access to the plaintext of the data.

[17] For generating a re-encryption key, the organization requires its private key and the public key of the service provider.

general concept of this model has been introduced by (Zwattendorfer, 2014).

The general concept of this model is similar to the *BlindIdM-Model* because also proxy re-encryption is used for protecting identity data from the cloud service providers. However, the main differences are that the data can also be stored encrypted at non-cloud identity providers and that the data can also be encrypted by the user and not only by an organization. In addition – which is the basic concept of this federated model – there are two re-encryption steps required, since identity data needs to flow at least through two cloud identity brokers. For instance, lets assume that the user has stored some identity data, which are encrypted for Identity Broker 1, at an identity provider. To successfully run such a privacy-preserving authentication process, the user additionally has to generate two re-encryption keys (One for the direction Identity Broker 1 $\rightarrow$ Identity Broker 2 and one for the direction Identity Broker 2 $\rightarrow$ service provider) and issues them to the respective entities. Finally, after successful authentication at the identity provider, identity data are transferred through the chain identity provider $\rightarrow$ Identity Broker 1 $\rightarrow$ Identity Broker 2 $\rightarrow$ service provider by applying proxy re-encryption in the last two steps (The identity data was already encrypted for Identity Broker 1 during storage at the identity provider, hence only two instead of three re-encryption steps are required). An application of this model can be found in (Zwattendorfer and Slamanig, 2013b), where parts of the STORK[18] framework are realized using this architecture to enhance scalability by ensuring users' privacy at the same time.

4 COMPARISON OF CLOUD IDENTITY MANAGEMENT-MODELS

In this section we evaluate, discuss, and compare the various cloud identity management-models based on different criteria. Comparison criteria are defined in the following Subsection 4.1 whereas the comparison itself is elaborated in Subsection 4.2.

4.1 Comparison Criteria

The following criteria act as a basis for comparing the various cloud identity management-models. Some of the comparison criteria were selected or derived from (Cao and Yang, 2010), (Nuñez et al., 2013), and (Birrell and Schneider, 2013). The selected criteria target aspects of different areas (e.g. general architecture, trust, privacy, etc.). The diversity of the criteria was deliberately considered to give a comprehensive overview on the different cloud identity management-models.

Number of SPs supported: Is the model limited to one SP or can multiple SPs be supported?

Number of IdPs supported: Is the model limited to one IdP or can multiple IdPs be supported?

Trust domains: Is authentication supported only within a single trust domain or also across different trust domains?

Trust model: Is a direct trust model or a brokered trust model applied?

Trust in the cloud IdP/identity broker: Must the cloud identity provider/identity broker be trusted or can they be semi-trusted?

Single sign-on (SSO): Can the model support single sign-on (SSO)?

Storage location of identity data: Where are users' identity data stored?

Scalability: Is the model applicable in a large scale?

Extensibility: Is the model easily extensible, e.g. by adding new service providers?

Governance framework: Is a governance framework involving several entities required?

Cost effectiveness: Is the model cost effective?

Confidentiality: Does the identity data stay confidential at the identity provider/identity broker?

Minimal/Selective disclosure: Can the user select the amount of identity data to be disclosed to the identity provider/service provider?

User control: Does the user have full control over her identity data?

Unlinkability: Is the user unlinkable to the identity provider/identity broker? In other words, are different authentication processes of the same user linkable?

Anonymity: Can the user stay anonymous with respect to the identity provider/identity broker?

4.2 Comparison

In this section we compare the individual cloud identity management-models with respect to the prior defined criteria. Table 1 shows and summarizes this comparison. For some comparisons we use

[18]Secure Identity Across Borders Linked, `https://www.eid-stork.eu/`

qualitative arguments, for others quantitative arguments (low, medium, high), and for the rest simply boolean (e.g. yes/no for being applicable or not) arguments. The options marked in bolt indicate the respective best option (only applicable for quantitative and boolean values). The underlying principle for all comparisons (in particular for those that are related to privacy such as confidentiality, minimal/selective disclosure, etc.) is that we assume an identity provider or an identity broker deployed in the cloud acting *honest but curious* (thus being semi-trusted). In contrast to that we assume applications in the cloud and their hosting service providers as being trusted, as they anyhow require users' identity data for service provisioning.

In the following we discuss the various models based on the individual criteria.

Number of SPs supported: Since in the *Identity in the Cloud-Model* the service provider and the identity provider are the same entity, the identity provider can only serve one service provider. All other models have no such restriction and thus can provide multiple service providers with identity data.

Number of IdPs supported: Only those models that rely on a broker-based approach are able to deal with multiple connected identity providers. All others just include one identity provider. Dealing with multiple identity providers has the advantage that a user can simply select her preferred identity provider for an authentication process. Different identity providers can have different identity data stored or support different qualities in the authentication mechanisms. This allows users to select the identity provider satisfying best the needs for authentication at a service provider.

Trust domains: The broker-based models support authentication across multiple trust domains, as multiple entities are involved during an authentication process. All others support authentication in single domains only.

Trust model: Again, all models which rely on an identity broker also feature a brokered trust model, hence the trust relationships are segmented. All other models rely on a direct or pairwise trust model, as only the service provider and the identity provider communicate with each other during an authentication process. A clear statement which model has more advantages cannot be made. Both have their benefits and drawbacks, however, details on the individual models can be found in (Linn et al., 2004).

Trust in the cloud IdP/identity broker: For the two models (*BlindIdM-Model* and *Privacy-Preserving Federated Cloud Identity Broker-Model*), which rely on proxy re-encryption for securing the data during cloud transmission, it is sufficient when the identity provider/identity broker is considered semi-trusted. In all other cloud identity models the identity provider/identity broker must be trusted.

Single sign-on (SSO): In fact, all models that can handle multiple service providers are principally applicable to support single sign-on. This means, that only the *Identity in the Cloud-Model* cannot support a simplified log-in process.

Storage location of identity data: In the *Identity to the Cloud-Model* identity data are stored on a single external identity provider, which is capable of providing identity to the cloud application through a well-defined interface. In the broker-based models, identity data can be stored distributed across multiple different identity providers, being either deployed in the cloud or in a conventional data center. However, the different identity providers could also have identity data stored redundantly, i.e. the same attribute name/value-pair is stored at different providers. No identity data are actually stored at the identity broker. In the remaining cloud identity models identity data are stored directly at the cloud identity provider.

Scalability: The *Identity to the Cloud-Model* has the lowest scalability, as an external identity provider is usually not designed for dealing with high load activities. In addition, an external identity provider has not that flexibility or elasticity that an identity provider deployed in a cloud has. Hence, such cloud identity providers (*Identity in the Cloud-Model*, *Identity from the Cloud-Model*, and *BlindIdM-Model*) have higher scalability features. Although in these three models the identity provider/identity broker is deployed in the cloud, we rated the models with just medium level scalability. The reason is that with the broker-based models load can additionally be distributed to other identity providers and thus is not bundled at one single provider. Hence, the broker-based models achieve the highest scalability.

Extensibility: The *Identity in the Cloud-Model* cannot be extended because service provider and identity provider are one and the same entity. The *Identity to the Cloud-Model*, the *Identity from the Cloud-Model*, and the *BlindIdM-Model* can be extended to integrate additional service providers. Nevertheless, the broker-based models have the

Table 1: Comparison of the individual cloud identity management-models based on selected criteria

Criterion / Model	**Identity in the Cloud-Model**	**Identity to the Cloud-Model**	**Identity from the Cloud-Model**	**Cloud Identity Broker-Model**	**Federated Cloud Identity Broker-Model**	**BlindIdM-Model**	**Privacy-Preserving Federated Cloud Identity Broker-Model**
Number of SPs supported	One	**Multiple**	**Multiple**	**Multiple**	**Multiple**	**Multiple**	**Multiple**
Number of IdPs supported	One	One	One	**Multiple**	**Multiple**	One	**Multiple**
Trust domains	One	One	One	**Multiple**	**Multiple**	One	**Multiple**
Trust model	Direct	Direct	Direct	Brokered	Brokered	Direct	Brokered
Trust in the cloud IdP/identity broker	Trusted	Trusted	Trusted	Trusted	Trusted	**Semi-Trusted**	**Semi-Trusted**
Single sign-on (SSO)	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Storage location of identity data	Cloud identity provider	External identity provider	Cloud identity provider	Cloud identity provider and external identity provider	Cloud identity provider and external identity provider	Cloud identity provider	Cloud identity provider and external identity provider
Scalability	Medium	Low	Medium	**High**	**High**	Medium	**High**
Extensibility	Low	Medium	Medium	**High**	**High**	Medium	**High**
Governance framework	**No**	**No**	**No**	Yes	Yes	Yes	Yes
Cost effectiveness	Medium	Medium	Medium	**High**	**High**	Medium	**High**
Confidentiality	No	No	No	No	No	**Yes**	**Yes**
Minimum/Selective disclosure	No	**Yes**	No	**Yes**	**Yes**	No	**Yes**
User Control	No	**Yes**	No	**Yes**	**Yes**	No	**Yes**
Unlinkability	No	No	No	No	No	No	**Yes**
Anonymity	No	No	No	No	No	**Yes**	**Yes**

best extensibility as from their nature the general aim is to support multiple service providers and identity providers.

Governance framework: The non-broker-based cloud identity models do not require an extensive governance framework as only a simple pairwise (direct) trust model applies. In the broker-based concepts a thorough governance framework is required as multiple providers have to interact. For the privacy-preserving models (*BlindIdM-Model* and *Privacy-Preserving Federated Cloud Identity Broker-Model*) the governance framework gets even more complex, as encryption keys have to be managed for the individual entities.

Cost effectiveness: The broker-based models have the highest cost effectiveness, since the identity brokers are deployed in the cloud and additionally multiple identity providers can be connected and re-used. Due to the re-use of existing external identity providers, costs can be saved. The same arguments also hold for the *Identity to the Cloud-Model*, where an existing identity management-system through an external interface is re-used for identity data provisioning. However, this model cannot benefit from the advantages of an identity provider in the cloud deployment, which leads to medium cost effectiveness only. All other models also have medium cost effectiveness, as the identity provider is deployed in the cloud but no existing identity providers can be re-used.

Confidentiality: Only the *BlindIdM-Model* and the *Privacy-Preserving Federated Cloud Identity Broker-Model* support confidentiality with respect to the cloud service provider because the identity data transferred through the cloud service provider are encrypted. In comparison, in all other cloud identity models identity data are routed in plaintext through the cloud service provider that hosts the cloud identity provider/identity broker.

Minimum/Selective disclosure: For evaluating this

criterion we assume that minimum/selective disclosure is only possible at trusted identity providers. Hence, this feature is only supported where external (and trusted) identity providers are part of the model. These are the broker-based models as well as the *Identity to the Cloud-Model*. All other models rely on cloud identity providers only.

User control: Again, for evaluating this criterion we assume that full user-control is only possible at trusted identity providers. Therefore, the same results as for the comparison with respect to minimum/selective disclosure apply.

Unlinkability: The user – in fact – is only unlinkable with respect to the identity broker in the *Privacy-Preserving Federated Cloud Identity Broker-Model*. The reasons are that, on the one hand, the identity broker just sees encrypted data and, on the other hand, that the encrypted data can be randomized if certain proxy re-encryption schemes such as from (Ateniese et al., 2006) are used. The randomization feature allows to provide the identity broker with different ciphertexts during different authentication processes although the containing plaintext data remains the same. Hence, this avoids user linkage during different authentication processes of the same user. Although the *BlindIdm-Model* supports proxy re-encryption too, the randomization feature has no effect in this case because the encrypted data are directly stored at the cloud identity provider. If the user wants to update her encrypted identity data at the cloud identity provider, she must somehow be linkable. All other models also do not support unlinkability because identity data flows through the identity provider/identity broker in plaintext.

Anonymity: The only two models that support anonymity with respect to the identity broker are the *BlindIdM-Model* and the *Privacy-Preserving Federated Cloud Identity Broker-Model*. In these two models the identity data are fully hidden from the identity broker due to encryption. Even if the user is linkable, the broker cannot reveal the user's identity. In all other models anonymity with respect to the identity provider/identity broker is not possible because identity data are processed in plaintext.

5 CONCLUSIONS

Based on the comparison and discussion of the different cloud identity management-models it can be concluded that the *Privacy-Preserving Federated Cloud Identity Broker-Model* does the best with respect to the selected criteria. It supports the main basic functions like all other cloud identity models but additionally tremendously increases users' privacy. However, application of this model is also more complex than the others. Reasons are the support of authentication across several domains of multiple identity providers and service providers and the incorporation of privacy features due to the use of proxy re-encryption. Furthermore, the use of proxy re-encryption requires a thorough key management, which implies the necessity of an appropriate governance framework. In addition, the brokered trust model might be a blocking issue for further adoption of this model as liability is shifted to the intermediary components (identity brokers). However, in general the broker-based cloud identity management-models have more advantages than the simple cloud identity management-models. Nevertheless, the use of any cloud identity management-model is advantageous compared to traditional identity management-models as they provide higher scalability and better cost effectiveness due to the cloud computing features.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. (2009). Above the Clouds : A Berkeley View of Cloud Computing Cloud Computing. Technical report, RAD Lab.

Ateniese, G., Fu, K., Green, M., and Hohenberger, S. (2006). Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.*, 9(1):1–30.

Ates, M., Ravet, S., Ahmat, A. M., and Fayolle, J. (2011). An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and Other Delights. *ARES 2011*, pages 555–560.

Bauer, M., Meints, M., and Hansen, M. (2005). D3.1: Structured Overview on Prototypes and Concepts of Identity Management System. FIDIS.

Bertino, E. and Takahashi, K. (2011). *Identity Management: Concepts, Technologies, and Systems*. Artech House.

Birrell, E. and Schneider, F. (2013). Federated Identity Management Systems: A Privacy-based Characterization. *IEEE Security and Privacy*, 11(5):36–48.

Cao, Y. and Yang, L. (2010). A survey of Identity Management technology. In *IEEE ICITIS 2010*, pages 287–293. IEEE.

Cloud Security Alliance (2011). SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0. CSA.

Cox, P. (2012). How to Manage Identity in the Public Cloud. *InformationWeek reports*.

Dabrowski, M. and Pacyna, P. (2008). Generic and Complete Three-Level Identity Management Model. In *SECURWARE 2008*, pages 232–237. IEEE.

Dbrowski, M. and Pacyna, P. (2008). Overview of Identity Management. Technical report, chinacommunications.cn.

Frommm, J. and Hoepner, P. (2011). The New German eID Card. In Fumy, W. and Paeschke, M., editors, *Handbook of eID Security - Concepts, Practical Experiences, Technologies*, pages 154–166. Publicis Publishing, Erlangen.

Gopalakrishnan, A. (2009). Cloud Computing Identity Management. *SETLabs Briefings*, 7(7):45–55.

Goulding, J. T. (2010). identity and access management for the cloud : CA s strategy and vision. Technical Report May, CA Technologies.

Green, M. and Ateniese, G. (2007). Identity-Based Proxy Re-encryption. In *ACNS 2007*, volume 4521 of *LNCS*, pages 288–306. Springer.

Huang, H. Y., Wang, B., Liu, X. X., and Xu, J. M. (2010). Identity Federation Broker for Service Cloud. *ICSS 2010*, pages 115–120.

Jøsang, A., Fabre, J., Hay, B., Dalziel, J., and Pope, S. (2005). Trust requirements in identity management. *Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, pages 99–108.

Jøsang, A. and Pope, S. (2005). User centric identity management. *AusCERT 2005*.

Jøsang, A., Zomai, M. A., and Suriadi, S. (2007). Usability and privacy in identity management architectures. In *ACSW '07*, pages 143–152.

Kaler, C. and McIntosh, M. (2009). Web Services Federation Language (WS-Federation) Version 1.2. OASIS Standard.

Leitold, H., Hollosi, A., and Posch, R. (2002). Security architecture of the Austrian citizen card concept. In *ACSAC 2002*, pages 391–400.

Linn, J., Boeyen, S., Ellison, G., Karhuluoma, N., Macgregor, W., Madsen, P., Sengodan, S., Shinkar, S., and Thompson, P. (2004). Trust Models Guidelines. Technical report, OASIS.

Neuman, C., Yu, T., Hartman, S., and Raeburn, K. (2005). The Kerberos Network Authentication Service (V5). RFC 4120 (Proposed Standard).

Nuñez, D., Agudo, I., and Lopez, J. (2013). Leveraging Privacy in Identity Management as a Service through Proxy Re-Encryption. In Zimmermann, W., editor, *Proceedings of the PhD Symposium at the 2nd European Conference on Service-Oriented and Cloud Computing*, pages 42–47.

Nuñez, D. and Agudo, I. (In Press). Blindidm: A privacy-preserving approach for identity management as a service. *International Journal of Information Security*.

Nuñez, D., Agudo, I., and Lopez, J. (2012). Integrating OpenID with Proxy Re-Encryption to enhance privacy in cloud-based identity services. In *IEEE CloudCom 2012*, pages 241 – 248.

Palfrey, J. and Gasser, U. (2007). CASE STUDY: Digital Identity Interoperability and eInnovation. Berkman Publication Series,.

Pearson, S. and Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. In *CloudCom 2010*, pages 693–702. IEEE.

Sen, J. (2013). Security and Privacy Issues in Cloud Computing. In Martínez, A. R., Marin-Lopez, R., and Pereniguez-Garcia, F., editors, *Architectures and Protocols for Secure Information Technology Infrastructures*, pages 1–45. IGI Global.

Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592.

Zwattendorfer, B. (2014). Towards a Privacy-Preserving Federated Identity as a Service Model. to appear.

Zwattendorfer, B. and Slamanig, D. (2013a). On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud. In *SEC 2013*, AICT, pages 300–314. Springer.

Zwattendorfer, B. and Slamanig, D. (2013b). Privacy-Preserving Realization of the STORK Framework in the Public Cloud. In *SECRYPT 2013*, pages 419–426.

Zwattendorfer, B., Stranacher, K., and Tauber, A. (2013). Towards a Federated Identity as a Service Model. In *Egovis 2013*, pages 43–57.