Privacy-ABCs to Leverage Identity Management as a Service

Ahmad Sabouri[1] and Ronny Bjones[2]

[1] Goethe University Frankfurt,
Deutsche Telekom Chair of Mobile Business & Multilateral Security,
Grueneburgplatz 1, 60323 Frankfurt, Germany
Ahmad.Sabouri@m-chair.de
[2] Microsoft Corporate, Belgium
Ronny.Bjones@microsoft.com

Abstract. Along with the rapid growth in adoption of cloud services, there have been developments towards a new emerging concept, called Identity Management as a Service. As the internal IT systems were not designed for externals, the IT solutions from the cloud can solve the challenges of connecting the enterprises to the outer world and consequently, bring all the benefits of the cloud-based services to them.

However, the other side of the coin of moving towards outsourcing identity infrastructure is a set of privacy and security challenges that cannot be neglected. In this paper, we propose an architectural model based on Privacy Preserving Attribute-based Credentials, and show how we can benefit from the advantages of Privacy-ABCs to help the concept of Identity Management as a Service, and address the privacy concerns that it raises.

Keywords: Identity Management as a Service, IdMaaS, Privacy Preserving Attribute-based Credentials.

1 Introduction

The US National Institute of Standards and Technology (NIST) defines Cloud Computing to be a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. In another perspective, cloud services give organizations the opportunity to outsource the parts of their IT infrastructures that they do not have adequate skills, and therefore focus more on their own expertise to increase their productivity and lower their costs.

Researchers have conduced various studies, like [2], to investigate the economics of the cloud and justify how migrating to cloud platforms will reduce the infrastructure and the labour cost while increasing the security and reliability. A more comprehensive list of the drivers and the blockers to uptake cloud services has been surveyed in [3]. Their results show that the drivers extend well

B. Preneel and D. Ikonomou (Eds.): APF 2014, LNCS 8450, pp. 143–153, 2014.

beyond cost savings; In addition to the lower cost of ownership, over 50% of their respondents have recognized better working practices for the employees, improved efficiency, easier external interactions, and access to specialized and affordable applications to be *significant* or *very important* drivers. On the other hand, according to [3], it seems that each industry has its own bug-bears: governments organizations are more concerned about privacy and data protection, financial services worry about regulation and compliance, commercial organization consider storage of personal identifiable data to be a barrier, while telcos see intellectual properties as the most important blocker on their way.

In spite of all the barriers, a considerable number of services are offered as cloud services and enterprises and governments are rapidly adopting them. For example, Office 365 [4] and Google Apps [5] are making a good progress in the market. Therefore, we are in the stage where the cloud paradigm is building its concrete shape. The statistics by [6] shows that Software-as-a-Service is in use in 63% of organizations and it had a growth of 15% from 2012 to 2013. Therefore, cloud-based services can be considered as a mainstream way of delivering certain aspects of the IT requirements of many organizations.

As explained by [7], cloud computing is an amalgamation of various technologies to meet the demands of an interdependent maze of software and services. This necessitates several Identity Management Systems (IdMs), based on various technologies, to interoperate and function as one consolidated body. Hence Identity Management in the cloud is sufficiently more complex problem than the traditional IdM and consequently more expensive to implement. That is why cloud IdMs need to be built by specialized organizations to deal with the compliance, security and privacy complexities. Still hiding those complexities from its users to allow easy adoptance of cloud IdMs. This justifies the move towards outsourcing the IdM infrastructure to cloud services similar to other application services. Nowadays, a majority of enterprises are using Identity Management Systems and many of the deployed IdMs are onpremise, but increasingly they are being supplemented by the use of on-demand IdM service (IdMaaS) [8].

In this paper we present an architectural model based of Privacy Preserving Attribute-based Credentials (Privacy-ABCs) to leverage Identity Management as a Service and address some of the privacy concerns that has been identified for different deployment models of IdMaaS. The rest of this paper is organized as follows. Section 2 provides a brief overview of Identity Management in the cloud environment. Section 3 introduces Privacy-ABCs and shows their significant potential in addressing IdMaaS privacy requirements. Then we propose and analyze our model for IdMaaS based on Privacy-ABCs in Section 4. Later we close the discussion and conclude in Section 5.

2 Identity Management in the Cloud Environment

There has been an interesting survey reported in [8] based on over three hundred interviews with senior IT managers in medium size to large organizations in a range of business sectors across Europe. It shows a growth of 45% in the

number of deployed IdMs in any from (on-premise, hybrid or on-demand). The report claims that the majority of businesses are opening up at least some of their application to external users and almost 58% transact directly with the users from other businesses or customers. In addition to that, their findings show that social media is emerging as key source of identity, particularly for the consumers, which has basically led to the emergence of the concept "Bring Your Own Identity". These two trends along with the rising use of cloud services and increasingly complex mix of identity sources are mentioned as the main drivers behind the growing use of Identity Management Systems.

Cloud Security Alliance [9] considers Cloud Identity as a Service (IDaaS) to be a broad term that covers the management of any part of the Identity, Entitlement, and Authorization/Access Management in the cloud environment. Based on this, [10] introduces IdMaaS as outsourcing the identity management service by companies and organizations from their internal infrastructures and deploy it on the cloud providers in order to benefit from the innovative offer by the cloud for externalizing the workload.

According to [8], IdMaaS is the provision of IdM capabilities on-demand over the Internet, which include the capabilities of an on-premise IdM Systems as well as the additional benefits specific to IdMaaS. Looking closely at the listed benefits, one could see that there is a high degree of overlap with the aforementioned drivers: IdMaaS eases provisioning of external users as it is designed for remote access, certain IdMaaS systems have pre-configured links to many social media sites supporting the concept of "Bring You Own Identity", IdMaaS enables easy federation of applications from different cloud service providers for all types of users, IdMaaS is easily scalable and can be expanded or contracted based on the need, and IdMaaS improves productivity of employees as it provides easy access to wide range of resources for all employees, including those working remotely. More interestingly, their findings show that the potential of IdMaaS is widely recognised even by those with pure on-premise IdM deployments, which gives hope to see further transitions towards IdMaaS in future.

Considering the case where internal policies of an enterprise do not allow some sensitive information to reside outside of the enterprise premises or the case where legacy system might cause interoperability problems, a Hybrid Model can be employed to bring agility to the enterprise to benefit from the full capabilities of IdMaaS while minimizing the cost of the on-premise IdM to the scale of that sensitive data or the legacy systems.

Whether IdM is deployed in the public cloud or in a private data center operated by a partner or on-premise; the great news is that this is all transparent to the user. Today there are still differences in the technologies deployed in the cloud or on-premise but this will all fade away turning the question where to run the IdM services into a pure compliance and deployment task. Services will be moved between the different deployment environments by means of a mouse click.

Besides all the benefits and motivations mentioned about IdMaaS, Identity Management in the cloud comes with a set of challenges with regard to its security and privacy. These problems has been studied and investigated to some

extend in various research works including [11] [12] [13] [14] [15]. Although security has been identified as the most important concern in using cloud services, in this work we focus more on the problem of Privacy. In this regard, [16] proposes an Identity Management System called SPICE for cloud environments whose main goal is to preserve users' privacy. The authors claim a set of properties for Identity Management Systems in the cloud environments, which we take as the basis for our analysis. Using a different set of cryptographic tools, [17] proposes another approach to the verification of digital identity for cloud platforms. This work utilizes zero-knowledge proofs to enable the user to prove the knowledge of a set of attributes without revealing their value. In our work, we do not employ any specific cryptographic solution and base our model on the abstract definitions of Privacy-ABCs' features. Therefore, any concrete implementation of Privacy-ABCs would fit in this model.

As it is shown in Figure 1, having Identity Management of an enterprise outsourced to the cloud, we suggest to consider a four-corner model where User, Enterprise, IdMaaS Provider and Cloud Service Provider (CSP) are the involved entities. This reflects the basic difference with the traditional three-corner model where IdMaaS and Enterprise were represented by a single entity called Identity Service Provider (IdSP). There are several privacy concerns in the new model that must be addressed. But before moving to this discussion, it is important to understand that the trust relationships have changed compared to the case of on-premise deployment of services (e.g. applications) and IdM Systems. In a full on-demand deployment of IdMaaS, IdM capabilities and cloud services are being operated by external entities and not the enterprise itself. Therefore, additional measures are needed to deal with the emerging privacy issues. More specifically, these privacy issues are the followings:

1. *IdMaaS must not learn about the services that the users are authenticating to:* Due to the fact that IdMaaS Provider is not the same entity as the enterprise, tracking the services accessed by the enterprise's users might introduce threats to the enterprise's business.
2. *CSPs must not be able to link a user to her identity:* The CSPs are not operating in the domain of the enterprise and therefore minimal disclosure implies that they should be provided only with the necessary information. In this regard, the CSP only needs to ensure that the user is authorized by the enterprise to access the licensed service.
3. *CSPs must not be able to profile a user based on her different accesses:* Similar to the case of IdMaaS Provider, building profile of the users by an external entity is not desired for the enterprise and can be considered as the threat.
4. *Enterprise should be able to audit the use of resources and services while the CSPs are blinded to these information:* To avoid misuse and fraud cases, the enterprises demand for mechanisms to monitor the access to the resources. However, the minimal disclosure principle requires these mechanisms to limit monitoring capabilities only to the enterprise and avoid leaking extra information to the external parties operating the resources and services on the cloud.

Fig. 1. The four corner model of IdMaaS setup

3 Privacy Preserving Attribute-Based Credentials

Strong authentication and authorization techniques used nowadays are double edged swords: while they can protect service providers by offering a satisfactory level of resilience against unauthorized accesses, most of these technologies have the drawback of threatening the clients' privacy. Privacy Preserving Attribute-based Credentials (Privacy-ABCs) are elegant techniques to cope with these problems. They can offer strong authentication and a high level of security to the service providers, while users' privacy is preserved [18]. Existing privacy preserving authentication mechanisms are based on advanced cryptographic primitives [19] [20] [21] [22] [23]. In these schemes, users obtain certified credentials for their attributes from trusted issuers and later derive, without further assistance from any issuer, unlinkable tokens that reveal only the required attribute information yet remain verifiable under the issuer's public key [24].

[24] refers to the unification of concepts and features of the different privacy preserving authentication mechanisms such as Microsoft's U-Prove [25] and IBM's Identity Mixer [26], as privacy preserving attribute-based credentials or Privacy ABCs. Their definitions abstract away from the concrete cryptographic realizations but are designed in a way that instantiation with different cryptographic protocols is feasible.

A detailed description of all these concepts and features has been defined in Chapter 2 "Features and Concepts of Privacy-ABC" of [27]. Here we briefly quote the described entities and their interactions from [27] and [24].

As it is shown in Figure 2, Users, Issuers, Verifiers, Revocation Authorities and Inspectors are the five different involved roles in the ecosystem. The Users obtain "Credentials" containing certified "Attributes" from the Issuers. They can present the tokens derived from these credentials to the "Verifiers" to prove their eligibility for accessing a resource as long as their credentials are not marked as revoked in the corresponding "Revocation Authority". Furthermore, there is a possibility for the Users to encode their attribute values in such a way that can only be read by a specific Inspector.

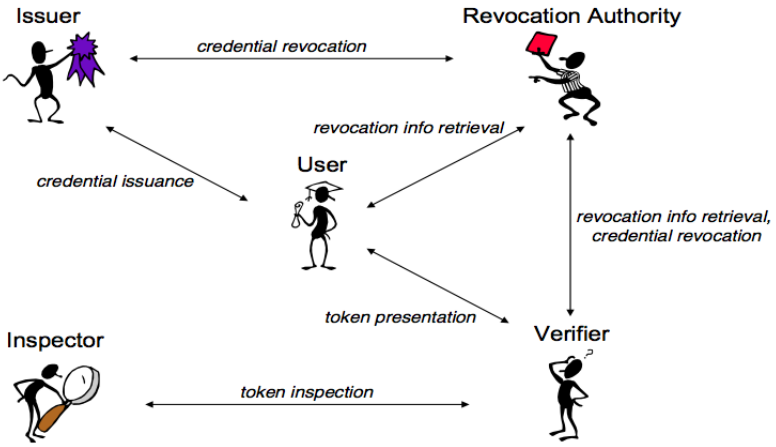

Fig. 2. Entities and interactions diagram [27]

As [24] says, "a secure realization of a Privacy-ABC system guarantees that (1) users can only generate a valid presentation token if they were indeed issued the corresponding credentials that have not been revoked, (2) that attributes encoded in the presentation token for an inspector can indeed be retrieved by that inspector, and (3) that the presentation tokens do not reveal any further information about the users other than the attributes contained in them."

4 Modeling IdMaaS Using Privacy-ABCs

In this section we propose an architectural model that represents the mapping between the Privacy-ABCs roles to the four-courner model explained earlier and demonstrated in Figure 1 in order to address the privacy concerns of IdMaaS. In a quick look, the proposed model for a full on-demand IdMaaS results in the setting shown in Figure 3.

In this setting, IdMaaS Provider will take the role of Issuer since identity information is residing on the cloud and they are available to the IdMaaS. Therefore it can issue credentials to the users based on the attributes and relationships that have been defined for the users in the user store (e.g. Directory). Theoretically, whoever is the Issuers can play as Revocation Authority as well. Even though it is possible to introduce a fifth party to perform as the revocation authority, a proper revocation scheme can give the opportunity to assign this role to the IdMaaS without any major risk. It is worth noting, that the request for revoking a credential always initiates by the Enterprise. On the other side of the story, the Cloud Service Providers (CSPs) are the entities that require to authenticate users before offering their services according to the predefined policies. Therefore, CSPs are acting as Verifier in this setting. Furthermore, another important required feature is Accountability and Auditing. The Enterprise needs to be able

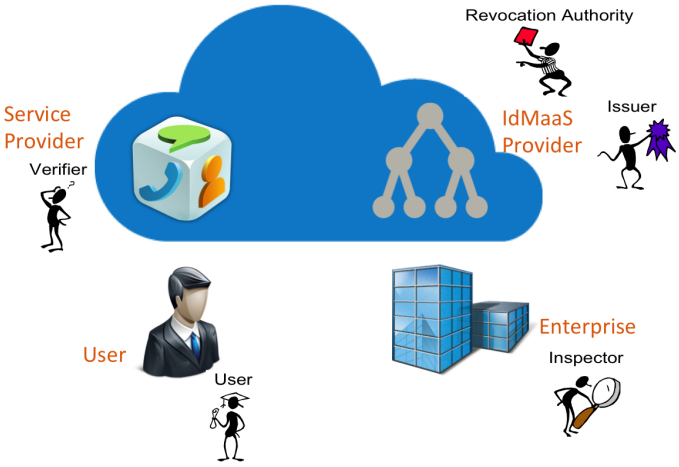

Fig. 3. Mapping of Privacy-ABCs' roles to on-demand IdMaaS four corner model

to monitor access to the resources and services in certain cases, in such a way that the Cloud Service Provider would not be able to profile the users. This is possible via the Inspection feature of Privacy-ABCs. The Enterprise becomes the Inspector and every access to the services on the cloud must be accompanied with a token, which is inspectable by the Enterprise when needed. Table 1 summarizes the role mappings.

Table 1. Mapping of the roles for full on-demand IdMaaS

Privacy-ABCs Role	Entity in the Cloud Setting
User	User
Issuer	IdMaaS Provider
Verifier	Cloud Service Provider
Revocation Authority	IdMaaS Provider
Inspector	Enterprise

The four-corner model needs to be adjusted a bit to reflect the Hybrid deployment of IdMaaS. Furthermore, the role assignment will also experience a change when Enterprise puts limited trust on IdMaaS Provider, which consequently requires on-premise hosting of attribute values. In this case, the IdMaaS Provider cannot issue credentials on its own for the users due to lack of access to the attributes. As a result, the Enterprise should be equipped with certain modules to play the role of Issuer and can be proxied by the IdMaaS to be reachable in the cloud environment. Figure 4 depicts the four-corner model for a Hybrid deployment and Table 2 summarizes the role mappings.

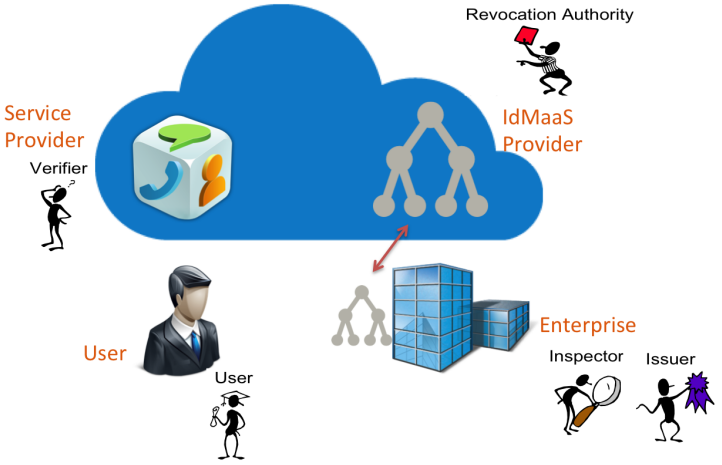

Fig. 4. Mapping of Privacy-ABCs' roles to Hybrid IdMaaS four corner model

Table 2. Mapping of the roles for Hybrid IdMaaS

Privacy-ABCs Role	Entity in the Cloud Setting
User	User
Issuer	Enterprise
Verifier	Cloud Service Provider
Revocation Authority	IdMaaS Provider
Inspector	Enterprise

4.1 Does the Model Fulfil the Privacy/Security Properties?

In [16], the authors list the following desirable security/privacy properties for authentication in the cloud. We consider this list as the basis for our analysis of the interactions between Users, IdMaaS Provider, Cloud Service Providers (CSPs) and the Enterprise.

– Unlinkability: In cloud computing, a user may access multiple services associated with the same or different CSPs. Unlinkability ensures that no CSPs, even if they collude, can link different transactions, whether they are of the same service or different services, of the same user. In addition to this definition by [16], another type of unlinkablity is needed, which concerns the IdMaaS learning about the services that a user accesses. This type of unlinkability is also known as untraceability in the literature and it is required in our model because the IdMaaS Provider is considered as an external entity for the Enterprise. The Enterprise might not be content if IdMaaS Provider profiles its employees or users.

One of the key properties of Privacy-ABCs is that the Presentation sessions are not linkable. Therefore none of the verifiers can profile a user or link different transactions of the same user even if they collude. In addition to that, the IdMaaS is not involved in the presentation process at all; therefore it will not learn about the presentation sessions and the services a user gets access to.

- Delegatable Authentication: In case that the service offered by a CSP, is a combination of services by some other CSPs, the authentication should be delegatable such that the CSP behind the scene can authenticate a user without a direct communication with either the user or the IdMaaS Provider, and without fully trusting the CSP in front.

  In our model, the CSP in front can easily act as an intermediate proxy between the user and the CSP behind the scene and help them to exchange the Presentation protocol messages. The secondary CSP can perform the authentication using only the public information available about the IdMaaS.
- Anonymity: The users should be able to anonymously authenticate themselves, as authorized users to the CSP, without letting the CSP know about their real identity or exact attributes.

  Another key feature of the Privacy-ABCs is minimal disclosure. If there presentation token does not include identifiable information, the anonymity of the user is preserved.
- Accountability: The users may abuse their anonymity. If needed, a trusted party can revoke the anonymity so the users can be held accountable for their malicious actions. As we mentioned in the previous section, the Inspection feature of Privacy-ABCs enables the Enterprises to securely log and audit the access to the resources. Using this feature, the CSPs can force the users to include encrypted identifiable information in the authentication token. Since nobody else than the actual user can create such a token, the user will be responsible in case of a misuse.
- User Centric Access Control: Users should be able to control what information they want to reveal about themselves over the cloud or to a CSP, and to control who can access that information, and how this information would be used in order to minimize the risk of identity theft and fraud.

  Users of Privacy-ABCs are in control of their credentials. Before any presentation takes place, users get notified about the information that the access policy requires them to disclose. They can fully control what kind of information they are giving out. Furthermore, since the user is actively involved in the presentation phase, nobody else (not even the IdMaaS Provider or the Enterprise) can impersonate the user.
- Single Registration: The users need to register themselves only once for getting the credentials without the need of contacting the IdMaaS every time authentication is needed. Once the users obtained their credentials, they can perform authentication until their credentials are revoked. However, for some concrete realization of Privacy-ABCs like U-Prove, the credential consists of a bunch of unlinkable U-Prove tokens. When the user runs out of tokens, she has to somehow reload the credential with more tokens.

5 Conclusion

The trend is to move towards cloud services and replace on-premise infrastructures that are managed by non-specialists with cloud services that are offered by professionals. Identity Management is the underlying layer of every IT platform and can be also counted as the backbone of the cloud environment. Along with the growth in use of cloud services, there have been efforts to also offer Identity Management as a cloud service to bring agility to enterprises and facilitate their better integration with the cloud-based applications. In this paper we suggested an architectural model based on Privacy Preserving Attribute-based Credentials for the concept Identity Management as a Service. Our analysis shows that Privacy-ABCs can deal with the privacy concerns that have been identified for Identity Management in the cloud while providing a high level of assurance for authentications.

Acknowledgements. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust).

References

1. The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
2. Harms, R., Yamartino, M.: The economics of the Cloud, http://www.microsoft.com/en-us/news/presskits/cloud/docs/the-economics-of-the-cloud.pdf
3. The adoption of cloud-based services, http://www.ca.com/es/~/media/files/industryanalystreports/the-adoption- of-cloud-based-services-increasing-confidence-through-effective-security.pdf
4. Office 365, http://www.office365.com/
5. Google Apps, http://www.google.com/apps
6. The future of cloud computing, 3rd annual survey (2013), http://www.northbridge.com/2013-cloud-computing-survey
7. Gopalakrishnan, A.: Cloud computing identity management. SETLabs briefings 7(7), 45–54 (2009)
8. Digital identities and the open business, http://www.ca.com/cn/~/media/files/industryresearch/quocirca-digital-i dentities.pdf
9. Alliance, C.: Security guidance for critical areas of focus in cloud computing v3.0. Cloud Security Alliance (2011)
10. Nunez, D., Agudo, I., Lopez, J.: Integrating openid with proxy re-encryption to enhance privacy in cloud-based identity services. In: 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 241–248 (2012)
11. Brodkin, J.: Gartner: Seven cloud-computing security risks (2008)
12. Pearson, S., Benameur, A.: Privacy, security and trust issues arising from cloud computing. In: 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp. 693–702 (2010)

13. Takabi, H., Joshi, J., Ahn, G.-J.: Security and privacy challenges in cloud computing environments. IEEE Security Privacy 8(6), 24–31 (2010)
14. Angin, P., Bhargava, B., Ranchal, R., Singh, N., Linderman, M., Ben Othmane, L., Lilien, L.: An entity-centric approach for privacy and identity management in cloud computing. In: 2010 29th IEEE Symposium on Reliable Distributed Systems, pp. 177–183. IEEE (2010)
15. Architecture serving complex Identity Infrastructures, http://www.trustindigitallife.eu/actor/tdl-publications.html
16. Chow, S., He, Y.-J., Hui, L., Yiu, S.: Spice simple privacy-preserving identity-management for cloud environment. In: Bao, F., Samarati, P., Zhou, J. (eds.) ACNS 2012. LNCS, vol. 7341, pp. 526–543. Springer, Heidelberg (2012), http://dx.doi.org/10.1007/978-3-642-31284-7_31
17. Bertino, E., Paci, F., Ferrini, R., Shang, N.: Privacy-preserving digital identity management for cloud computing. IEEE Data Eng. Bull. 32(1), 21–27 (2009)
18. Sabouri, A., Krontiris, I., Rannenberg, K.: Attribute-based credentials for trust (ABC4Trust). In: Fischer-Hübner, S., Katsikas, S., Quirchmayr, G. (eds.) TrustBus 2012. LNCS, vol. 7449, pp. 218–219. Springer, Heidelberg (2012)
19. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24(2), 84–90 (1981)
20. Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., Shacham, H.: Randomizable proofs and delegatable anonymous credentials. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 108–125. Springer, Heidelberg (2009)
21. Brands, S.A.: Rethinking public key infrastructures and digital certificates: building in privacy. MIT Press (2000)
22. Camenisch, J.L., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
23. Camenisch, J.L., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)
24. Camenisch, J., Dubovitskaya, M., Lehmann, A., Neven, G., Paquin, C., Preiss, F.-S.: Concepts and languages for privacy-preserving attribute-based authentication (2013)
25. Microsoft U-Prove, http://www.microsoft.com/uprove
26. Identity Mixer, http://idemix.wordpress.com/
27. D2.1 Architecture for Attribute-based Credential Technologies Version 1, https://abc4trust.eu/download/ABC4Trust-D2.1-Architecture-V1.pdf