D. Nuñez, I. Agudo, and J. Lopez, "Leveraging Privacy in Identity Management as a Service through Proxy Re-Encryption", *Ph.D Symposium of the European Conference on Service-Oriented and Cloud Computing (ESOCC) 2013*, 2013.
NICS Lab. Publications: https://www.nics.uma.es/publications

Leveraging Privacy in Identity Management as a Service through Proxy Re-Encryption

David Nuñez, Isaac Agudo*, and Javier Lopez*

Network, Information and Computer Security Laboratory, Universidad de Málaga, Málaga, Spain
dnunez@lcc.uma.es

Abstract. The advent of cloud computing has provided the opportunity to externalize the identity management processes, shaping what has been called *Identity Management as a Service* (*IDaaS*). However, as in the case of other cloud-based services, IDaaS brings with it great concerns regarding security and privacy, such as the loss of control over the outsourced data. As part of this PhD thesis, we analyze these concerns and propose BlindIdM, a model for privacy-preserving IDaaS with a focus on data privacy protection through the use of proxy re-encryption.

Keywords: Identity Management as a Service, Cloud computing, Privacy

1 Introduction

Within the internal processes of most organizations, identity management stands out for its ubiquitous nature, as it plays a key role in authentication and access control. However, it also introduces an overhead in cost and time, and in most cases, specialized applications and personnel are required for setting up and integrating identity management systems. As has already happened for other services, the cloud paradigm represents an innovative opportunity to externalize the identity management processes. *Identity Management as a Service* (*IDaaS*) is the cloud industry's response to the problem of identity management within organizations, allowing them to outsource these services from their internal infrastructures (*on-premise model*) and deploy it in the cloud (*on-demand model*).

Althought cloud computing has raised great expectations regarding efficiency, cost reduction and simplification of business processes, it has also increased security and privacy risks. This very same conflict also applies to the IDaaS case: although it offers organizations a great opportunity to cut capital costs, it also introduces a variant of one of the classic problems of cloud computing, namely, the loss of control over outsourced data, which in this case is information about users' identity. Users entrust their personal information to identity providers, which then have a privileged position in order to read users' data that is in their custody. Although there are several regulatory, ethical and economic reasons for discouraging this possibility, the fact is that nothing actually prevents

* Supervisors of this PhD thesis

identity providers from accessing users' information at will. Even if we assume that the identity provider is not dishonest and that its internal policy is respectful regarding identity information, it is still possible that a privacy disclosure occurs, for example through security breaches, insider attacks, or legal requests [1]. Traditionally, cloud providers have tackled these problems defining Service Level Agreements (SLAs) and internal policies; however, these measures simply reduce this issue to a trust problem. It is therefore desirable to count with more advanced security mechanisms that enable users to benefit from cloud computing and still preserve their privacy and the control over their information, ideally through criptographic means [2].

Hence, the principal motivation behind this research line is putting the identity provider into the cloud landscape, where data storage and processing could be offered by possibly untrusted cloud providers, but still offer an identity management service that guarantees user's privacy and control. To this end, we define BlindIdM, a privacy-preserving IDaaS system where identity information is stored and processed in a blind manner, removing the necessity of trusting that the cloud identity provider will not read the data.

2 Identity Management as a Service

The federated identity management model enables information portability between different domains, which permits both a dynamic distribution of identity information and delegation of associated tasks, such as authentication or user provisioning. One of the key aspects of this model is the establishment of trust relationships between the members of the federation, which enables them to believe the statements made within the federation. The federated model is widely used in organizations, deployed as an on-premise service.

The main actors that participate in the identity interactions are [3]: (i) *Users*, the subjects of the identity information, and generally the actors that request resources and services through their interaction with applications and online services; (ii) *Service Providers* (*SP*), the entities that provide services and resources to users or other entities; and (iii) *Identity Providers* (*IdP*), which are specialized entities that are able to authenticate users and to provide the result of this authentication to service providers. Figure 1a shows a high-level view of a federated identity setting, where a host organization acts as a federated identity provider. In this setting, an employee from the host organization requests a service from the service provider, who in turn asks the organization for identity information about its employee.

Although federated identity management has led to great advantages with respect to interoperability of identities, it has also introduced cost and time overheads, since it usually requires specialized applications and personnel for setting up, integrating and managing this process. IDaaS can be seen as a refinement of the federated model, which takes the efficiency of the cloud in its favour for offering specialized outsourcing of identity management. Among the benefits of Identity Management as a Service we find: (i) more flexibility, scalability and

stability for high demand environments, with a growing number of users and thousands of identities; (ii) reduction of costs, since IDaaS providers can focus on providing more efficient and specialized identity services to organizations; (iii) better security measures, implemented in dedicated systems and facilities; and (iv) improved compliance and business processes audits due to the high specialization and security standards that an IDaaS provider can achieve. However, there are also risks associated with Identity Management as a Service, such as:

- Identity providers are appealing targets to attackers as they represent a single point of failure because they centralize users' personal information.
- Cloud providers are susceptible to being subpoenaed for users' data, in the case there is some legal, administrative or criminal investigation running.
- In the absence of cryptographic means, it is not possible to actually limit the access of cloud providers to the data they steward. That is, there is almost no risk of being discovered accessing users' information without their consent.
- Cloud providers may be located in foreign countries with different, and possibly conflicting, laws and regulations regarding privacy and data protection.

Hence, it is obvious that externalizing the management of identity information to the cloud implies a loss of control for users and organizations. This in turn signifies an empowerment of cloud identity providers and facilitates the users to incur damages, losses or risks in the case of a disclosure of private data.

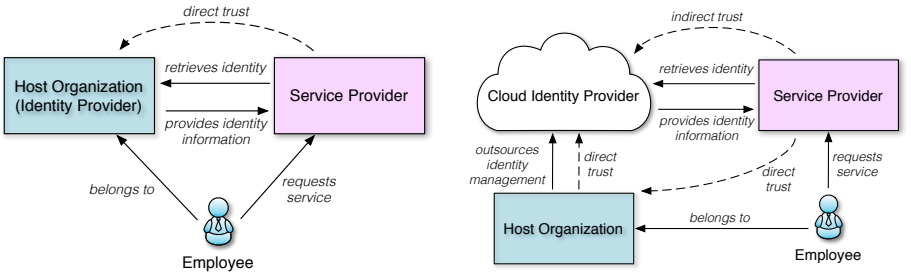
3 BlindIdM: Privacy-Preserving IDaaS

The aforementioned concerns led us to conceive of the concept of *Blind Identity Management* (BlindIdM), a model whereby the cloud identity provider is able to offer an identity information service, without knowing the actual information of the users; that is, it provides this service in a *blind* manner. This is a great innovation with respect to current identity management systems, where users' identity information is managed by the identity provider and the user is obliged to trust that the provider will make proper use of his data and will guarantee its protection. Our intention is that this model will enable organizations to choose a cloud identity provider without necessarily establishing a strong bond of trust with it. The novel aspect of our proposal lies in the protection of data: the host organization encrypts users' identity information prior to outsourcing it to the cloud, in such a way that it is still manageable by the cloud identity provider.

It is interesting to think about what kind of incentives may motivate a cloud identity provider to offer its services in a blind manner. Among them we find: (i) compliance with data privacy laws and regulations, since a privacy-preserving approach like ours, which achieves data confidentiality through encryption mechanisms, could be very useful to help cloud identity providers to comply with data protection regulations; (ii) minimization of liability, since outsourced data is encrypted prior to arriving the cloud and the cloud provider does not hold the decryption keys, and (iii) data confidentiality as an added value, as offering secure data processing and confidentiality could be considered as a competitive

advantage over the rest of identity services, and in the future can lead to a business model based on the respect for users' privacy and data confidentiality.

In our model, we will assume a federated identity setting, similar to that shown in Figure 1a, but where the host organization partially outsources the identity management processes to a cloud identity provider, while retaining the authentication service on-premises. The cloud identity provider now acts as an intermediary in the identity interactions, and is also in charge for storing and supplying identity information; Figure 1b shows this setting.



(a) Federated Identity Management (b) BlindIdM model

Fig. 1: Relation between entities in different models

With regard to trust assumptions, we consider the cloud identity provider as an adversary, and in particuar, we will assume it to be *data-curious*, a type of honest-but-curious adversary, which behaves correctly with respect to protocol fulfillment, but has no hindrance to try to access users' data.

In [4], we describe a particular instantiation of BlindIdM that uses SAML 2.0 as the underlying identity management protocol and proxy re-encryption techniques to achieve end-to-end confidentiality of the identity information, while allowing the cloud to provide an identity service. From a high-level viewpoint, a proxy re-encryption scheme [5] is an asymmetric encryption scheme that permits a proxy to transform ciphertexts under Alice's public key, p_A, into ciphertexts under Bob's public key, p_B. In order to do this, the proxy is given a re-encryption key, $r_{A \to B}$, which makes this process possible.

In the scenario proposed by this model, the host organization (including all the employees) acts as the user, and the identity management of the organization is outsourced to a cloud identity provider. Identity information flows from the user (in our case, from the host organization), acting as a source of information, to the service provider, acting as a consumer of information. Specifically, the host organization encrypts the identity information under its public key p_H prior sending it to the cloud identity provider. The use of proxy re-encryption enables the identity provider to transform these ciphertexts into encrypted attributes under the public key of the service provider, p_{SP}; in order to do so, the identity provider needs a re-encryption key $r_{H \to SP}$ generated by the host organization

and provided beforehand. More details are given in [4] on how this process is framed within the SAML protocol using standard extension mechanisms.

The first ideas towards our proposal were presented in [6], where we describe a user-centric IDaaS system based in OpenID and proxy re-encryption. Although conceived as a proof of concept, this is the first work that achieves blind processing of identity information; however, trust issues arise as OpenID does not provide proper mechanisms for establishing trust. BlindIdM solves these problems and provides more solid mechanisms of integration with the identity management protocol.

From a practical point of view, it is also crucial to determine whether our proposal is economically feasible. Most of cryptography-based proposals only provide theoretical analysis of security and complexity, but do not tackle the economic viability. In [4], we provide an economic assessment of our proposal and estimate the cost of proxy re-encryption operations in USD cents; these expenses are a consequence of the incurred cost of the cryptographic computations in a cloud environment. For instance, it can be seen that the re-encryption operation, which is the one executed by the cloud provider, has an estimated cost of 4.79E-04 USD cents; in other words, the cloud identity provider can perform approximately 2087 re-encryptions for one USD cent. From these figures we can conclude that the cryptographic overhead is reasonable, as it permits an IDaaS system to serve thousands of encrypted attributes for a few cents, considering the costs that an organization could incur in the case of a security breach.

4 Research Plan

This PhD thesis is aimed to tackle with the following research challenges:

- Leveraging user-centricity in identity management: Most current identity management systems are provider-centric. Identity providers are in a privileged position to learn information about users. We want to create means for empowering the users with respect identity providers.
- Enhancing users' privacy in digital transactions that involve their identity: Privacy and confidentiality of identity information is threatened on a daily basis. Ideally, strong safeguards for protection this information should be in place. We believe that cryptographic tools are needed for solving this issue.
- Interoperability of the solutions: Any new solution to these problems should take open standards in consideration in order to facilitate and enhance interoperability.
- Solutions that reduce the trade-off between anonymity and accountability: it is a big challenge to design solutions that support both aspects; we need to enhance accountability in digital transactions, but at the same time, it is necessary to respect users' privacy.

5 Conclusions and Future Work

As part of this PhD thesis, we propose a solution to the problem of privacy for Identity Management as a Service. IDaaS is a recent trend, powered by cloud computing technologies, that allows companies and organizations to benefit from outsourcing identity management processes. The reduction of costs and time-consuming tasks associated with managing identity services are the main reasons behind this externalization. However, as is the case for other cloud-based services, there is much concern regarding the inversion of the control of the data, as users lose almost all control over their data.

We propose BlindIdM, a privacy-preserving model for IDaaS system that guarantees user's privacy and control even when data storage and processing is performed by untrusted clouds. In this model, the cloud identity provider is able to offer an identity information service without knowing the actual personal information of the users. We believe that the approach presented in this paper opens up new possibilities regarding privacy in the fields of identity management and cloud computing.

With regard to forthcoming work, we plan to deploy a prototype of our system in a real cloud setting, such as Amazon EC2 or Google AppEngine; in addition, more recent proxy re-encryption schemes could be used in order to provide more efficiency and security. As to future research, we are exploring other cryptographic techniques and investigating how to extend the protection of privacy to users' access behaviour.

Acknowledgements

This work was partly supported by the Junta de Andalucía through the project FISICCO (P11-TIC-07223). The first author has been funded by a FPI fellowship from the Junta de Andalucía through the project PISCIS (P10-TIC-06334).

References

1. Cloud Security Alliance. Top threats to cloud computing, version 1.0, 2010.
2. Isaac Agudo, David Nuñez, Gabriele Giammatteo, Panagiotis Rizomiliotis, and Costas Lambrinoudakis. Cryptography goes to the cloud. In *Secure and Trust Computing, Data Management, and Applications*, pages 190–197. Springer, 2011.
3. E. Maler and D. Reed. The venn of identity: Options and issues in federated identity management. *Security & Privacy, IEEE*, 6(2):16–23, 2008.
4. D. Nuñez and I. Agudo. BlindIdM: A Privacy-Preserving Approach for Identity Management as a Service. *International Journal of Information Security*, In Press.
5. G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC)*, 9(1):1–30, 2006.
6. D. Nunez, I. Agudo, and J. Lopez. Integrating OpenID with proxy re-encryption to enhance privacy in cloud-based identity services. In *4th IEEE Intl. Conf. Cloud Computing Technology and Science (CloudCom)*, pages 241–248. IEEE, 2012.