JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 27-28 (2016) 35–53

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality

Bernd Zwattendorfer *, *Daniel Slamanig*

Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria

ARTICLE INFO

Article history:
Available online 8 December 2015

Keywords:
Electronic identity (eID)
Identity management
Austrian eID system
Public cloud
Privacy
Proxy re-encryption

ABSTRACT

The Austrian eID system constitutes a main pillar within the Austrian e-Government strategy. The eID system ensures unique identification and secure authentication for citizens protecting access to applications where sensitive and personal data are involved. In particular, the Austrian eID system supports three main use cases: identification and authentication of Austrian citizens, electronic representation, and foreign citizen authentication at Austrian public sector applications. For supporting all these use cases, several components — either locally deployed in the applications' domain or centrally deployed — need to communicate with each other. While local deployments have some advantages in terms of scalability, still a central deployment of all involved components would be advantageous, e.g., due to less maintenance efforts. However, a central deployment can easily lead to load bottlenecks because theoretically the whole Austrian population as well as — for foreign citizens — the whole EU population could use the provided services. To mitigate the issue on scalability, in this paper we propose the migration of the main components of the ecosystem into a public cloud. However, a move of trusted services into a public cloud brings up new obstacles, particularly with respect to privacy. To bypass the issue on privacy, in this paper we propose an approach on how the complete Austrian eID ecosystem can be moved into a public cloud in a privacy-preserving manner by applying selected cryptographic technologies (in particular using proxy re-encryption and redactable signatures). Applying this approach, no sensitive data will be disclosed to a public cloud provider by still supporting all three main eID system use cases. We finally discuss our approach based on selected criteria.

1. Introduction

Unique identification and secure authentication are essential processes especially in security-sensitive areas of application such as e-Government or e-Health. In particular, these processes play a key role if sensitive data are processed. To ensure a high level of security for citizen applications in these areas, many European countries have already rolled out national eID solutions supporting unique identification and secure authentication. In Austria, the Austrian citizen card is the official eID for citizens (Leitold et al., 2002).

In general, the Austrian e-Government strategy foresees a thorough eID concept based on the Austrian citizen card, which constitutes the core component for secure identification and authentication of citizens at Austrian e-Government

* *Corresponding author.* Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria. Tel.: +43 316 873 5574; fax: +43 316 873 5520.
E-mail addresses: bernd.zwattendorfer@iaik.tugraz.at (B. Zwattendorfer), daniel.slamanig@iaik.tugraz.at (D. Slamanig).
http://dx.doi.org/10.1016/j.jisa.2015.11.004
2214-2126/

applications. Moreover, the Austrian eID concept also contains representative authentications and authentications of foreign EU citizens, which are treated equally to Austrian citizens in e-Government scenarios. Hence, the main functions of the Austrian eID system are Austrian citizen identification and authentication at online applications, citizen authentication on behalf of a natural or legal person, and the support of foreign citizen authentication at Austrian e-Government applications.

To make these main functions work, the Austrian eID system involves several other components — besides the Austrian citizen card — which are interconnected to each other. Key components, among others, are for instance MOA-ID (Module for Online Applications — Identification) (Lenz et al., 2014), an open source software component locally deployed in each service providers domain facilitating citizen card access; the MIS (Management Issuing Service) (Leitold and Tauber, 2011), which constitutes a central service issuing electronic mandates; or the SPR-GW (SourcePIN Register-Gateway) (Lenz, 2015), which a central gateway supporting registration of foreign citizens in Austrian national population registers. Details on the individual components will be given in Section 4.2. Currently, the Austrian eID system treats several deployed MOA-ID instances as well as the MIS and the SPR-GW as trusted entities. While the local deployment model has indeed some benefits, particularly with respect to scalability, in some situations a centralized deployment approach — besides the MIS and the SPR-GW — also of MOA-ID may be preferable. However, in terms of scalability (theoretically the whole Austrian population could use these central services for identification and authentication at service providers), the existing approaches may reach their limits. This can easily lead to load bottlenecks at MOA-ID, the MIS, or the SPR-GW. While the use of electronic mandates and foreign citizen authentications are still in its start-up phase, frequent usages are to be expected in the future. The use of electronic mandates in Austria gets increasing popularity. For instance, professional representation or natural-to-legal person representation constitute daily business in legal procedures. Additionally, representation of parents for their children or children for elderly people are frequent use cases especially in health services. Furthermore, cross-border identifications are steadily increasing because the European Commission currently heavily pushes the STORK framework (Leitold and Zwattendorfer, 2011), which will be probably the dominant authentication framework across Europe in the future.

Coping with such increased load may not be easy to handle within the current central deployment scenarios, where each entity is deployed in a trusted data center. Therefore, the authors propose a move of important components of the Austrian eID system (e.g., MOA-ID, MIS, SPR-GW) into a public cloud. Deployment in a public cloud could definitely mitigate any scalability issues due to the characteristics (high scalability, high elasticity, cost reduction, etc.) provided by a public cloud environment. However, a move of such trusted service into a public cloud brings up new obstacles, particularly with respect to citizens' privacy (Pearson and Benameur, 2010; Sen, 2013; Zissis and Lekkas, 2012). Although privacy and security are one of the main issues of public clouds, we still consider the public cloud as the most promising cloud deployment model for a migration of governmental services such as the Austrian eID infrastructure into the cloud. The reasons are — among others — particularly the ability to absorb unforeseeable load peaks almost seamlessly and its huge cost savings potential compared to other cloud deployment models (Harms and Yamartino, 2010; Zwattendorfer and Tauber, 2013). While privacy in the current scenarios is ensured through organizational means, in this paper we illustrate how such a move of trusted services of the Austrian eID system into a public cloud can be successfully realized using cryptographic technologies (by particularly using proxy re-encryption and redactable signatures) by still preserving citizens' privacy.

The paper is structured as follows. Section 2 briefly explains the related work in the context of identity management. Cryptographic building blocks, which our work is based on, are described in Section 3. In Section 4, the Austrian eID system and its individual components are described in detail. In addition, the three main supported use cases (identification and authentication of Austrian citizens, in representation, and of foreign citizens) and corresponding process flows are explained. How the individual components can be moved into a public cloud in a privacy-preserving manner and how the process flows will change are elaborated in Section 5. In Section 6, we discuss our approach with respect to security, privacy, and practicability. Finally, we draw conclusions in Section 7.

2. Related work

Identity management is no new topic and thus several identity management solutions exist. In this section we briefly outline a couple of identity management systems that have evolved over the past years (Bauer et al., 2005; Cao and Yang, 2010; Dabrowski and Pacyna, 2008; Ferdous and Poet, 2012).

First systems arose due to the need of managing employee's accounts in single organizations. User and identity data were simply stored in directories such as LDAP (Lightweight Directory Access Protocol). In this case, the scope of the identity management system was limited to this single organization.

Since the need for cross-organizational communication and hence exchanging identification and authentication data across domains gained importance, more sophisticated identity management solutions have established. One early example of such systems is Kerberos (Neuman et al., 2005), which enables secure and uniform authentication in insecure TCP/IP networks. While additionally the WWW became increasingly popular at this time, identity management systems on application level arose.

One example for a central identity management system was Microsoft Passport (latterly called Windows Live ID[1]). Other systems, which follow a decentralized and federated architecture, were the Liberty Alliance Project[2] (that evolved to the Kantara initiative[3]) or Shibboleth.[4] Both projects, Liberty Alliance and Shibboleth, influenced the development of the current version of the Security Assertion Markup Language (SAML 2.0) (Lockhart et al., 2008). SAML defines one of the most

[1] https://login.live.com.
[2] http://www.projectliberty.org.
[3] http://kantarainitiative.org.
[4] http://shibboleth.net.