SkIDentity - Trusted Identities for the Cloud[1]

Detlef Hühnlein[2], Gerrit Hornung, Michael Kubach, Vladislav Mladenov, Heiko Roßnagel, Stephan Sädtler, Johannes Schmölz, Tobias Wich

Abstract The goal of the SkIDentity project (http://SkIDentity.de) is to build a solid bridge between electronic identity cards (eID) and the existing and emerging cloud computing infrastructures. Based on the results of the project it will be possible to provide trusted identities for the cloud and secure complete business processes and value chains. For this purpose the existing components, services and trust infrastructures are integrated into a comprehensive, legally valid and economically viable identity infrastructure for the cloud and tested in attractive pilot projects. Special attention is given to the demands of small and medium enterprises and authorities. For this purpose the SkIDentity infrastructure in particular contains an "Identity Broker", which bundles the various eID-Services in a form, which is accessible even for very small companies and municipal authorities.

Keywords: SkIDentity, eID, smart card, strong authentication, SAML

1. Introduction

Against the background of the economic advantages of the industrialization of IT-services and the big economical potential of the "Internet of Services" [2] increasingly new and enhanced offers of cloud-based applications are established [23]. While a reliable identity management is an essential requirement for trustworthy cloud computing and the German Federal Office for Information Security Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI) recommends the use of strong authentication processes also for cloud users [7], it is still surprisingly common in practice to use rather weak [20, 5, 16] password-based au-

[1] This work has been partially funded by the Federal Ministry of Economics and Technology, Germany (BMWi, Contract No. 01MD11025A). The responsibility for the content of this article lies solely with the authors.

[2] Detlef Hühnlein
SkIDentity – c/o ecsec GmbH,
Sudetenstraße 16, 96247 Michelau, Germany
e-mail: detlef.huehnlein @ecsec.de

thentication mechanisms and attempts to move towards stronger authentication in the cloud only appeared fairly recently [9, 1, 19, 8, 17].

On the other hand there are existing and further emerging electronic identification (eID) infrastructures across Europe [13] and there is a proposal for a regulation on electronic identification, authentication and electronic signature (eIDAS) [6, 24], which aims at harmonizing eID-based authentication, electronic signatures and related trust services across Europe. Against this background the SkIDentity project aims at bridging the gap between secure electronic identity cards and the existing and emerging cloud computing infrastructures, to provide trustworthy identities for the cloud, so that complete process and value chains can be secured. The combination of the two previously independent domains creates significant chances for innovative products: The German market volume for identification, authentication including biometrics and RFID will nearly reduplicate from 920 Mio. € in year 2008 to 1.720 Mio. € in year 2015 [29]. But more auspicious are the perspectives in the area of cloud computing: There the market volume in the area of public clouds is expected to rise from nowadays 702 Mio. € to 21,99 Mrd. € in year 2025 [2]. Hence, the SkIDentity project addresses strategically extremely attractive markets.

2. The problems addressed by SkIDentity

In order to provide trustworthy identities for the cloud there have been several technical, organizational, legal and economic problems to solve:

- **Missing integration of eID and cloud computing infrastructures:** The infrastructures for eID cards and cloud based services have not been combined and there has not been a straightforward way to integrate both domains in a secure manner.
- **eID-Services are currently only available for the German eID card:** Currently eID-Services in Germany are just offered for the German eID card (Neuer Personalausweis, nPA). While there exist approaches which cover alternative eID cards [28, 27], the integration of existing Public-Key Infrastructures (PKI) and alternative authentication services into a comprehensive ”eID-Service Cloud” is completely missing.
- **eID service for the nPA are not ”tradeable” and hence unsuitable for small and medium size organizations:** The main problem is the fact that eID-Services for the German eID card have not been ”tradeable in an Internet of the Services” because every service provider requires his own authorization certificate and the commercial transmission of data to third parties is explicitly forbidden due to privacy reasons (cf. § 29 (1) Nr. 1 PAuswV).
- **Open security questions for electronic identities in the cloud:** In [26] it was shown that even the authentication systems of leading cloud service providers

were vulnerable and hence there is a great demand for stronger authentication in cloud computing environments.

- **Open legal question with respect to electronic identities in the cloud:** There has been legal uncertainty with respect to the usage of eID service broker acting as intermediary, because the concept so far has been focussed on the relations between two entities [22, 3]. Furthermore there have been open questions with respect to the law of evidence and compliance in enterprises.
- **Missing or unclear business models for identity services in the cloud:** eID-Services for the nPA are currently not usable for small and medium sized companies and municipal agencies because of the economic factors. The solution of the problem could be that ”Identity Brokers” act as information intermediates and provide the eID-Services in a bundled and rehashed way [31].
- **Missing standards for electronic identities in the cloud:** While cloud computing has been among the most important IT trends for quite a while, the related standardization has just started recently.

3. The SkIDentity Reference Architecture

In order to solve the above problems the ”SkIDentity Reference Architecture” [25] has been introduced. This architecture builds upon the concept of Federated Identity Management, as explained in [18, 15, 4, 21] and refines the classical components ”Client”, ”Service Provider” and ”Identity Provider” in order to support arbitrary authentication mechanisms, eID-tokens, credential technologies and federation protocols.
An overview of the SkIDentity Reference Architecture is depicted in Figure 1.

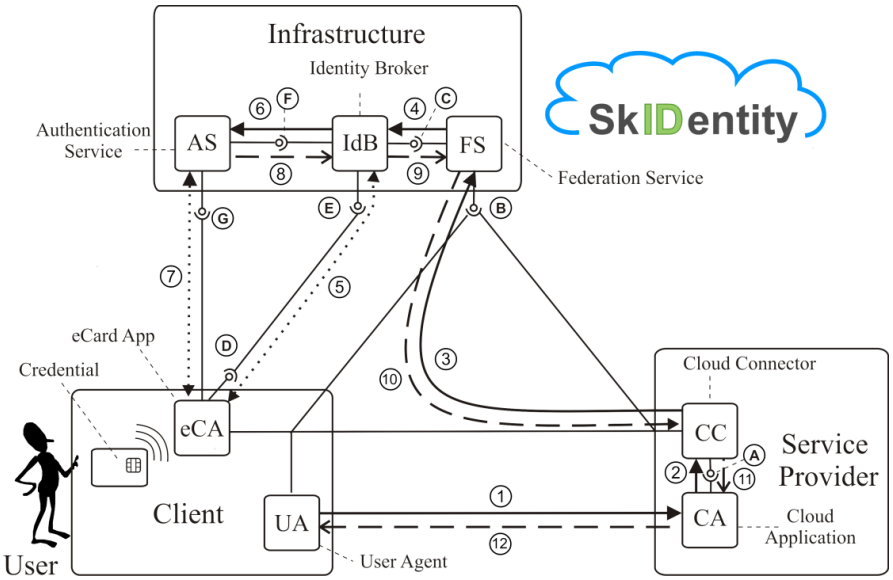

Figure 1: SkIDentity Reference Architecture

There are components at the Client, the Service Provider and in the SkIDentity Infrastructure.

3.1 System Components at the Client

The system of the User (Client) comprises the User Agent (UA), which can be realized by an arbitrary browser, and an appropriate eCard-App (eCA) (cf. [14, 30]), which enables the User to authenticate at an Authentication Service (AS) using some credential.

3.2 System Components at the Service Provider

The system of the Service Provider (SP) comprises the Cloud Application (CA) and an appropriate Cloud Connector (CC), which allows to communicate with an appropriate Federation Service (FS) in the SkIDentity Infrastructure using an appropriate federation protocol such as [4, 21, 10, 11, 12] for example.

3.3 SkIDentity Infrastructure

In the SkIDentity Infrastructure there are various Federation Services (FS) and a variety of Authentication Services (AS), which are connected via the Identity Broker (IdB). The Identity Broker acts information intermediary and provides the different eID-Services in a bundled and rehashed way. This offers the possibility to use the different services and tokens (German eID card, other European citizen cards, electronic health cards, health professional cards, bank and signature cards, company ID tokens, etc.) with an easy and consistent interface for the secure authentication in cloud based applications.

4. References

1. Amazon Inc.: AWS Multi-Factor Authentication (2013). http://aws.amazon.com/de/mfa/
2. Berlecon Research & al.: The economic potential of the Internet of Services. in German, Study on behalf of the Federal Ministry of Economics and Technology (2010). http://www.berlecon.de/idd
3. Borges, G.: Legal questions with respect to liability related to eID. in German, Study on behalf of the Federal Ministry of the Interior (2010). http://www.personalausweisportal.de/cln_102/SharedDocs/Downloads/DE/Studie_Recht_Volltext.html?nn=830468
4. Cantor, S., Kemp, J., Philpott, R., Maler, E.: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15.03.2005 (2005). http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
5. Dhamija, R., Perrig, A.: Déja vu: A user study using images for authentication. In: Proceedings of the 9th USENIX Security Symposium (2000)
6. European Commission: Proposal for a regulation of the European parliament and of the council on electronic identification and trust services for electronic transactions in the internal market. COM(2012) 238 final, 04.06.2012 (2012). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF
7. Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, B.: Security recommendations for Cloud Service Providers – minimum security requirements. (in German) (2011). http://docs.ecsec.de/BSI-MSACC
8. FIDO Alliance: (2013). http://www.fidoalliance.org/
9. Google: Advanced sign-in security for your google account (2011). http://googleblog.blogspot.de/2011/02/ advanced-sign-in-security-for-your.html
10. Hammer-Lahav, E.: The Oauth 1.0 protocol. Request For Comments – RFC 5849 (2010). http://www.ietf.org/rfc/rfc5849.txt
11. Hardt, D.: The Oauth 2.0 authorization framework. Request For Comments – RFC 6749 (2012). http://www.ietf.org/rfc/rfc6749.txt
12. Hardt, D., Jones, M.: The Oauth 2.0 authorization framework: Bearer token usage. Request For Comments – RFC 6750 (2012). http://www.ietf.org/rfc/rfc6750.txt
13. Houdeau, D.: Landscape eID in Europe in CY 2013. In: Proceedings of Open Identity Summit 2013, vol. 223, p. 163. GI e.V. (2013)
14. Hühnlein, D., Petrautzki, D., Schmölz, J., Wich, T., Horsch, M., Wieland, T., Eichholz, J., Wiesmaier, A., Braun, J., Feldmann, F., Potzernheim, S., Schwenk, J., Kahlo, C., Kühne, A., Veit, H.: On the design and implementation of the Open eCard App. In: Sicherheit 2012 GI-LNI (2012). http://subs.emis.de/LNI/Proceedings/Proceedings195/95.pdf

15. Hühnlein, D., Rossnagel, H., Zibuschka, J.: Diffusion of federated identity management. In: Tagungsband “Sicherheit 2010”, LNI, vol. 170, pp. 25–37. GI (2010). http://www.ecsec.de/pub/Sicherheit2010.pdf
16. Ives, B., Walsh, K.R., Schneider, H.: The domino effect of password reuse. Communications of the ACM 47(4), 75–78 (2004)
17. Lindemann, R.: Not built on sand – how modern authentication complements federation. In: Proceedings of Open Identity Summit 2013, vol. 223, pp. 164–168. GI e.V. (2013)
18. Maler, E., Reed, D.: The venn of identity: Options and issues in federated identity management. IEEE Security & Privacy Magazine 6(2), 16–23 (2008). DOI 10.1109/MSP. 2008.50. URL http://www.computer.org/portal/web/csdl/magazines/security#4
19. Microsoft Inc.: Microsoft account gets more secure (2013). http://blogs.technet.com/b/microsoft_blog/archive/2013/04/17/microsoft-account-gets-more-secure.aspx
20. Neumann, P.G.: Risks of passwords. Commun. ACM 37(4), 126 (1994). DOI 10.1145/175276.175289. http://portal.acm.org/citation.cfm?id=175276.175289
21. OpenID Foundation: OpenID Authentication 2.0. Final, December 5, 2007. http://openid.net/specs/openid-authentication-2_0.html
22. Roßnagel, A., Hornung, G., Schnabel, C.: The eID function of the German eID card from a privacy perspective (in German). Datenschutz und Datensicherheit (2008)
23. S. Shankland and J. Kaden: Gartner: Cloud computing wird wichtigster it-trend 2010. ZDNet Beitrag, 21.10.2009 (2009). http://docs.ecsec.de/ShKa09
24. Sädtler, S.: Identity management in cloud computing in conformity with European union law? - Problems and approaches pursuant to the proposal for a regulation by the European commission on electronic identification and trust services for electronic transactions in the internal market. In: Proceedings of Open Identity Summit 2013, vol. 223, pp. 118–130. GI e.V. (2013)
25. SkIDentity-Team: SkIDentity - Reference Architecture. Version 1.0 (2012)
26. Somorovsky, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.L.: All your clouds are belong to us: security analysis of cloud management interfaces. In: C. Cachin, T. Ristenpart (eds.) CCSW, pp. 3–14. ACM (2011)
27. STORK 2.0 Consortium: Secure Identity Across Borders Linked 2.0. https://www.eid-stork2.eu/
28. STORK Consortium: Secure Identity Across Borders Linked. https://www.eid-stork.eu/
29. VDI/VDE: Market potential of security technologies and security services (in german). Study on behalf of Federal Ministry of Economics and Technology (2009). http://www.asw-online.de/downloads/Studie_Sicherheitstechnologien_09.pdf
30. Wich, T., Horsch, M., Petrautzki, D., Schmölz, J., Hühnlein, D., Wieland, T., Potzernheim, S.: An extensible platform for eID, signatures and more. In: Proceedings of Open Identity Summit 2013, vol. 223, pp. 55–68. GI e.V. (2013)
31. Zibuschka, J., Fritsch, L., Radmacher, M., Scherner, T., Rannenberg, K.: Enabling privacy of real-life lbs. In: New Approaches for Security, Privacy and Trust in Complex Environments, pp. 325–336. Springer (2007)