Towards eIDAS as a Service

Dr. Detlef Hühnlein

ecsec GmbH
Sudetenstraße 16, 96247 Michelau, Germany
detlef.huehnlein@ecsec.de

Abstract

Cloud computing promises to provide great advantages and many analysts expect a significant growth of the cloud services market. In a similar manner the forthcoming European regulation on electronic identification and trusted services for electronic transactions in the internal market **[eIDAS-EP]** is expected to ease electronic identification, authentication and signatures (eIDAS) in Europe. The present contribution discusses whether and how the two approaches can be combined in order to provide services for electronic identification and authentication of entities, the creation, verification, validation and preservation of electronic signatures and the registered delivery of documents in an efficient manner using cloud computing techniques.

1 Introduction

Cloud computing is deemed to save costs, boost efficiency, improve user-friendliness as well as security and accelerate innovation **[TC-Europe]**. Furthermore the market for cloud services is expected to grow significantly **[MaM14]**. In a similar manner the forthcoming European regulation on electronic identification and trusted services for electronic transactions in the internal market (eIDAS) is expected to boost user convenience, trust and confidence in the digital world (cf. **[eIDAS-PR]**, **[COM(2012)238]**). Against this background it seems to be very rewarding to combine the two approaches and use trusted cloud computing techniques to provide services addressed by the forthcoming eIDAS-regulation. The present contribution discusses whether and how the different services addressed by the proposed regulation, which has recently been adopted by the European Parliament **[eIDAS-EP]**, can be provided in a secure and trustworthy manner as cloud service.

The rest of the paper is structured as follows: Section 2 contains the necessary background on the eIDAS-regulation and trustworthy cloud computing. Section 3 focusses on the different service addressed by the proposed regulation and in particular discusses whether and how electronic identification and authentication, electronic signatures and registered delivery can be provided as trustworthy cloud service. Based on related work from respective research projects Section 2 will introduce a reference architecture and discuss the cloud-based provision of trust services regulated in **[eIDAS-EP]**. Section 4 will finally summarize the main results and draw conclusions.

2 Background

This section carries together the necessary background information with respect to the eIDAS regulation and trustworthy cloud computing.

2.1 eIDAS in a Nutshell

The eIDAS-regulation **[eIDAS-EP]** (cf. Article 1), "lays down conditions under which Member States shall *recognise electronic identification means* of natural and legal persons falling under a notified electronic identification scheme of another Member State, lays down *rules for trust services*, in particular for electronic transactions and *establishes a legal framework* for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificates services for website authentication." Hence this regulation is meant to complement and replace the European Signature Directive **[1999/93/EC]**, which is repealed with effect from July 1st, 2016 (cf. Article 48), and covers besides general aspects (cf. Article 1-5, 13-24 and 44-50) in particular

- electronic identification (Article 6-12),
- electronic signature (Article 25-33),
- electronic seals (Article 34-38),
- electronic time stamps (Article 39-40),
- electronic registered delivery (Article 41-42) and
- website authentication (Article 43).

2.1.1 Electronic identification

The main accomplishment of the eIDAS regulation with respect to electronic identification (eID) is the mutual recognition (cf. Article 6) of electronic identification means for cross-border access to public sector services under certain conditions, which in particular require that Member States notify their eID schemes according to Article 9 and ensure the availability of authentication services, which shall be provided free of charge for cross-border public sector services (cf. Article 7, f)). For this purpose Article 8 defines the assurance levels "low", "substantial" and "high", which roughly correspond to the Level of Assurance (LoA) 2, 3 and 4 defined in **[ISO29115]** and similar levels defined in **[STORK-D2.3]** or **[NIST-800-63-2]** respectively. As stipulated in Article 11 the notifying Member State shall be liable for damages due to incorrectly issued eID means or failures within the authentication services (cf. Article 7, d) and f)).

2.1.2 Electronic signature

Article 24 Nr. 1 states that if a qualified certificate is issued for a trust service[1], it needs to verify the identity of the subsequent certificate holder "by appropriate means and in accordance with national law". Furthermore paragraph b) clarifies that this may happen "remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out according to Article 8 with regard to the assurance levels 'substantial' or 'high' ".

The Articles 25-33 roughly contain similar stipulations with respect to electronic signatures as **[1999/93/EC]**, where the noteworthy passages comprise the following: According to Article

[1] Note that **[eIDAS-EP]** does not seem to regulate in detail how the identity of a certificate holder needs to be verified if the qualified certificate is *not* issued to a trust service. The only pertinent regulation seems to be that a qualified certificate for electronic signatures "shall contain […] at least the name of the signatory, or a pseudonym" (cf. Annex 1, paragraph c).

26 par. 5 the Commission shall adopt implementing acts defining reference formats of advanced electronic signatures and one may expect that the corresponding {C,X,P}AdES and ASiC Baseline Profiles will be referenced in a similar manner as in **[2014/148/EU]**. As stipulated in Article 30 the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices, which may contain similar information as the "Directory of Signature Creation Devices" http://opensignature.org/devices/ maintained by the Open Signature Initiative. Articles 32 and 33 introduce "Qualified validation services for qualified electronic signatures" and "Qualified preservation services for qualified electronic signatures" respectively.

2.1.3 Electronic seals

Electronic seals as defined in Article 34-38 and Annex III are similar to electronic signatures with the difference that the creator of the seal is not a natural but a legal person.

2.1.4 Electronic time stamps

Unlike the existing signature directive **[1999/93/EC]** the eIDAS regulation **[eIDAS-EP]** addresses (qualified) electronic time stamps in Articles 39 and 40, whereas Article 39 Nr. 3 stipulates that "a qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States."

2.1.5 Electronic registered delivery

Article 41-42 regulate electronic registered delivery services, which are provided by one or more qualified trust service providers, which must ensure the trustworthy identification of the sender and addressee and apply advanced electronic signatures and qualified electronic time stamps to protect the authenticity and integrity of the delivered data and corresponding metadata.

2.1.6 Website authentication

Article 43 and Annex IV regulate the issuance of qualified certificates for website authentication, which need to contain the name of the natural or legal person to whom the certificate is issued, elements of the address, including at least city and State, and for legal persons the registration number as stated in the official records, if applicable.

2.2 Trusted Cloud Computing

In order to evaluate the applicability of cloud computing technologies (cf. **[NIST-800-145]**, **[BYV+09]**) for the provision of trust services one needs to pay special attention to security and trust-related aspects. A general treatment of security aspects in cloud computing environments can be found in **[TJA10]** and **[SuKa11]**. Recent research results from the "Trusted Cloud" research program supported by the German Federal Ministry of Economics and Energy can be found in **[KRR14]** and on the corresponding project websites, which are accessible via http://trusted-cloud.de. One of these projects is SkIDentity (http://SkIDentity.com) **[HHK+14]**, which provided the foundation for the Reference Architecture for eIDAS as a Service presented in Section 3.1.

3 eIDAS as a Service – Fact or Fiction?

This section discusses whether and how the different services addressed by **[eIDAS-EP]** can be provided as trustworthy cloud service. For this purpose we will first introduce a "Reference Architecture for eIDAS" and then discuss

- eID as a Service
- Electronic Time Stamps as a Service
- Electronic Signature as a Service, which comprises
  - Certificate Management as a Service
  - Signature Creation as a Service
  - Signature Verification and Validation as a Service
  - Preservation of Evidence as a Service
- Electronic Registered Delivery as a Service

3.1 A Reference Architecture for eIDAS as a Service

Based on existing reference architectures developed in pertinent research projects, such as SkIDentity (http://skidentity.de) **[HHK+14]** and FutureID (http://futureid.eu), and the previous discussion, Figure 1 introduces a reference architecture for the cloud-based provision of eIDAS-related services, which may facilitate the implementation and utilization of cloud services for electronic identification, authentication and signatures.

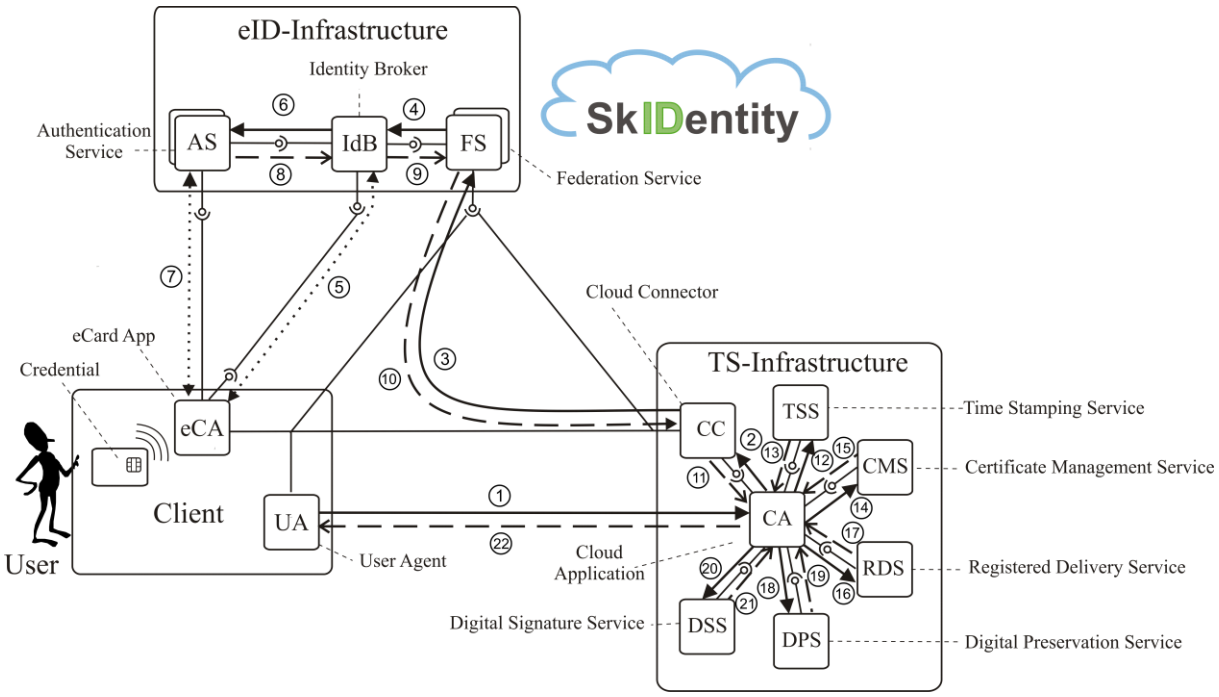

Figure 1: Reference Architecture for eIDAS as a Service

This reference architecture comprises system components at the Client, within the eID-Infrastructure and within the Trust Service (TS) Infrastructure.

3.1.1 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. **[HPS+12]** and **[WHP+13]**), which enables the User to authenticate at an Authentication Service (AS) using some credential.

3.1.2 System Components within the eID-Infrastructure

In the eID-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 as 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.

3.1.3 System Components within the TS-Infrastructure

The TS-Infrastructure comprises the central Cloud Application (CA), a Cloud Connector (CC), which allows to communicate with an appropriate Federation Service (FS) in the eID-Infrastructure using some federation protocol such as **[SAML(v2.0)]** or **[RFC6749]** for example and various trust services, such as a Time Stamping Service (TSS), a Certificate Management Service (CMS), a Registered Delivery Service (RDS), a Digital Preservation Service (DPS) and a Digital Signature Service (DSS) for example.

3.2 eID as a Service

The provisioning of electronic identification services within the eIDAS reference architecture depicted above is straightforward and typically comprises the following steps:

1. *UA → CA:* The *UA* contacts the *CA* in order to access some service.
2. *CA → CC:* The *CA* initiates the authentication procedure.
3. *CC → FS:* The *CC* creates an `AuthnRequest` according to **[SAML(v2.0)]** for example, which is addressed to the *FS*.
4. *FS → IdB:* The *FS* sends `Authenticate` according to **[CEN15480-3]** to the IdB.
5. *IdB → eCA:* The *IdB* contacts the *eCA* in order to detect the available credentials and allow the User to choose the credential in case there are ambiguities.
6. *IdB → AS:* The *IdB* calls the appropriate Authentication Service *AS* in order to retrieve the required set of attributes using calls specified in **[CEN15480-3]** or **[STORK-D.5.8.1b]**.
7. *AS ↔ eCA:* The *AS* performs the authentication of the User based on the available Credential.
8. *AS → IdB:* The *AS* returns the authentication result to the *IdB*.
9. *IdB → FS:* The *IdB* returns the authentication result to the *FS*.
10. *FS → CC:* The *FS* has created a `Response` according to **[SAML(v2.0)]** for example, which contains the requested identity attributes.

11. *CC* → *CA:* The *CC* verifies the received `Response` and returns the received attributes to the *CA*.

The identity attributes gathered in this process may be used in various use cases as explained below.

3.3 Electronic Signature as a Service

The eID-based authentication procedure sketched above may be used for various applications and in particular the trust service related use cases explained in the following.

3.3.1 Certificate Management as a Service

The protection of electronic transactions requires (qualified) certificates for natural and legal persons. Such certificates may be issued and managed by an appropriate Certificate Management System (CMS), which is connected to the central Cloud Application. A qualified certificate, which needs to contain the name of the signatory or a pseudonym (cf. Annex 1, paragraph c)) may be created by performing the steps (1) through (11) as sketched above followed by the creation (cf. steps (14) and (15)) and delivery (cf. step (22)) of the certificate.

3.3.2 Signature Creation as a Service

Depending on the technical capabilities of the available credential and the details of the advanced electronic signature one may either simply create local signatures at the client or use the Digital Signature Service (DSS) in steps (1) and (20) - (22). In the latter case one may additionally use steps (2) through (11) in order to determine the identity of the User based on his credential, which may be usable for authentication though not able to create signatures, as it is the case for the German eID in its basic configuration.

3.3.3 Signature Verification and Validation as a Service

For the verification of signatures and the validation of certificates one may simply use the Digital Signature Service (DSS) in steps (1) and (20) - (22).

3.3.4 Preservation of Evidence as a Service

In a similar manner one may access a Digital Preservation Service (DPS) in steps (1), (18)-(19) and (22)[2] in order to submit and retrieve documents and obtain evidence records according to **[RFC4998]**.

3.4 Electronic Time Stamps as a Service

Electronic time stamps may be obtained in steps (1), (12)-(13) and (22) using the Time Stamp Protocol according to **[RFC3161]** for example.

3.5 Electronic Registered Delivery as a Service

The provision of electronic registered delivery services may be based on existing specifications such as **[ETSI102640]** and/or a combination of the services mentioned above. While the trustworthy identification of the sender and the addressee may be performed with the eID-

[2] The DPS may support the interfaces specified in **[BSI TR-03125]**.

based authentication procedure sketched in Section 3.2, the transported data and meta data may be protected using the DSS and TSS mentioned above.

4 Conclusion

As discussed above the various trust services regulated in **[eIDAS-EP]** are very well suited to be provided and consumed in a service-oriented fashion. This opens up the opportunity for cost-efficient implementation using trusted cloud computing technologies as developed in the SkIDentity-project **[HHK+14]** for example.

References

[1999/93/EC] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

[2014/148/EU] *Commission Implementing Decision of 17 March 2014 amending Decision 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market*, notified under document C(2014) 1640, Text with EEA relevance, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014D0148

[BSI TR-03125] Federal Office for Information Security: *Preservation of Evidence of Cryptographically Signed Documents*, BSI TR-03125, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03125/BSITR03125.html

[BYV+09] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg & I. Brandic: *Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*, Future Generation computer systems, 25(6), 599-616, 2009, https://svn.inf.ufsc.br/luis.custodio/TCC-Dantas/Artigos/Bom/10.1.1.144.8937.pdf

[CEN15480-3] Comité européen de normalisation (CEN): *Identification card systems — European Citizen Card — Part 3: Interoperability using an application interface, CEN/TS 15480-3*, 2014

[COM(2012)238] European Commission: *Proposal for a regulation of the European Pariament and of the Council on electronic identification and trust services for electronic transactions in the internal market*, 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF

[eIDAS-PR] European Commission: *Draft Regulation "on electronic identification and trusted services for electronic transactions in the internal market"*, Press Release 20.09.2012, http://ec.europa.eu/digital-agenda/en/news/draft-regulation-electronic-identification-and-trusted-services-electronic-transactions-0

[eIDAS-EP] European Parliament: *Electronic identification and trust services for electronic transactions in the internal market*, as adopted by the European Parliament on 3rd of April 2014, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0282

[ETSI102640] ETSI TS 102 640: *Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM)*, Part 1-6

[HPS+12] D. Hühnlein, P. Petrautzki, J. Schmölz, T. Wich, M. Horsch, T. Wieland, J. Eichholz, A. Wiesmaier, J. Braun, F. Feldmann, S. Potzernheim, J. Schwenk, C. Kahlo, A. Kühne, H. Veit: *On the design and implementation of the Open eCcard App*. In: Sicherheit 2012 GI-LNI (2012), http://subs.emis.de/LNI/Proceedings/Proceedings195/95.pdf

[HHK+14] D. Hühnlein, G. Hornung, M. Kubach, V. Mladenov, H. Roßnagel, S. Sädtler, J. Schmölz, T. Wich: *SkIDentity - Trusted Identities for the Cloud*, to appear in **[KRR14]**

[ISO29115] ISO/IEC 29115: *Information technology — Security techniques — Entity authentication assurance framework*, International Standard, 2013

[KRR14] H. Krcmar, R. Reussner, B. Rumpe (ed.): *Trusted Cloud Computing*, Springer, to appear

[MaM14] MarketsandMarkets: *Cloud Computing Market (IaaS, PaaS, SaaS) to Reach $121.1 Billion by 2015 – New Report by MarketsandMarkets*, Press Release 08.02.2014, http://www.prweb.com/releases/cloud-computing/market/prweb11560677.htm

[NIST-800-63-2] NIST: *Electronic Authentication Guideline*, Special Publication 800-63-2, August 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[NIST-800-145] National Institute of Standards and Technology: *The NIST definition of cloud computing*, NIST special publication 800-145, http://csrc.nist.gov/publications/PubsSPs.html#800-145, 2011

[RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: *Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)*, IETF RFC 3161, 2001, www.ietf.org/rfc/rfc3161.txt

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: *Evidence Record Syntax (ERS)*, IETF RFC 4998, 2007, www.ietf.org/rfc/rfc4998.txt

[RFC6749] D. Hardt, Ed.: *The OAuth 2.0 Authorization Framework*, IETF RFC 6749, 2012, www.ietf.org/rfc/rfc6749.txt

[SAML(v2.0)] S. Cantor, J. Kemp, R. Philpott, E. Maler: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS Standard, 15.03.2005, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 2005

[STORK-D2.3] B. Hulsebosch, G. Lenzini, and H. Eertink: *Quality authenticator scheme*, STORK Deliverable D2.3, final, 03.03.2009, https://www.eid-

stork.eu/dmdocuments/public/D2.3_final._1.pdf**[STORK-D.5.8.1b]** J. Alcalde-Moraño, J. L. Hernández-Ardieta, A. Johnston, D. Martinez, B. Zwattendorfer: *STORK Deliverable D5.8.1b – Interface Specification*, 08.09.2009, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=960

[SuKa11] S. Subashini, V. Kavitha: *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications, 34(1), 2011, pp. 1-11

[TJA10] H. Takabi, J. B. Joshi, and G. J. Ahn: *Security and Privacy Challenges in Cloud Computing Environments*, IEEE Security & Privacy, 8(6), 2010, pp. 24-31

[TC-Europe] European Commission: *Establishing a Trusted Cloud Europe*, A policy vision document by the Steering Board of the European Cloud Partnership, 2014, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935

[WHP+13] 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, LNI, vol. 223, 2013. pp. 55–68, http://www.ecsec.de/pub/2013_OID_Platform.pdf