Why is the Open Signature Initiative necessary?

While there are many standards for electronic signatures, the practical adoption of them has room for improvement. In particular there are still many interoperability problems, which make signature technology hard to deploy and it is not clear which products support which standards. Against this background the Open Signature Initiative aims at enhancing ***transparency*** and ***interoperability*** with respect to electronic signature technology and related trust services.

The existence and broad adoption of suitable standards is clearly a prerequisite for the successful implementation of a single European market of services as envisioned by the directive 2006/123/EC [1]. Technologies and standards for electronic signatures play a crucial role for the implementation of electronic transactions, as they allow to maintain integrity, authenticity and trust.

There are standardised formats for advanced electronic signatures (cf. [2], [3], [4] and the decision of the European Commission 2011/130/EC [5]), standardised interfaces to smart cards used as secure signature creation device (cf. [6] and [7]), standardised application programming interfaces and device capability descriptions (cf. [8], [9] and [10]), standardised interfaces for digital signature services (cf. [11], [12] and [13]) and standardised formats for evidence records (cf. [14] and [15]) for example.

While many of these standards have existed for quite some time now and most of them have reached a considerable level of maturity, it seems that the practical adoption of these standards in Europe has room for improvement. In particular there are still many interoperability problems, which make signature technology hard to deploy in practice. The process of creating and verifying electronic signatures typically involves several components and services. While there are plenty of offerings for the different components and services available in the market, the effective choice of components is rather limited, because of the technical dependencies between the different hardware and software components. The interconnections between the different components make interoperability often hard to achieve and these technical dependencies are often not transparent to the involved stakeholders, because there is a lack of publicly available information about the component's features, which are relevant for interoperability. Against this background the Open Signature Initiative invites

vendors to provide technical information about their products in order to enhance transparency with respect to the available components and services, their technical features and resulting interoperability properties. This information will help operators and users of business and government applications to choose signature-related products and services which verifiably support the relevant standards and hence are already well prepared for the single European market of services.

In a similar manner there are very mature and widely adopted standards for trust services (cf. [16], [17], [18], [19], [20], [21], [22] for example), but the issuance of secure signature creation devices and qualified certificates across borders is not yet mainstream, but may become a customary process as a consequence of the forthcoming European regulation on electronic identification and trust services for electronic transactions in the internal market [23]. Against this background the Open Signature Initiative invites issuers of eID and signature creation devices to provide test devices and corresponding technical specifications in order to facilitate the creation of standardised capability descriptions according to [9] and [8] for example and provide accessible information about the implemented registration process and guidance how to perform the registration in a cross-border setting.

References

[1] *Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:en:pdf, 2006.

[2] ETSI, *CMS Advanced Electronic Signatures (CAdES)*, ETSI TS 101 733, Version 1.8.1, 2009.

[3] ETSI, *Technical Specification XML Advanced Electronic Signatures (XAdES)*, ETSI TS 101 903, Version 1.4.1, 2009.

[4] ETSI, *PDF Advanced Electronic Signature Profiles (PAdES)*, ETSI TS 102 778, Part 1 - 5, 2009.

[5] *Commission decision of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC (...)*

on services in the internal market, 2011/130/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF, 2011.

[6] European Norm 14890-1, *Application Interface for smart cards used as Secure Signature Creation Devices -- Part 1: Basic Services*, 2009.

[7] European Norm 14890-2, *Application Interface for smart cards used as Secure Signature Creation Devices -- Part 2: Additional Services*, 2008.

[8] ISO/IEC 24727, *Identification cards - Integrated circuit card programming interfaces - Part 3: Service Access Layer*, International Standard, 2008.

[9] CEN, Identification card systems - European Citizen Card - Part 3: Interoperability using an application interface, CEN/TS 15480-3, 2008.

[10] ISO/IEC 7816-15, *Identification cards - Integrated circuit cards - Part 15: Cryptographic information application*, International Standard, 2004.

[11] S. Drees, *Digital Signature Service Core Protocols, Elements, and Bindings*, Version 1.0, OASIS Standard, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf.

[12] J. C. Cruellas, *Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0*, Version 1.0, OASIS Standard, http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf, 2007.

[13] D. Hühnlein, *Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0*, OASIS Committee Specification 01, http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf, 2009.

[14] T. Gondrom, R. Brandner and U. Pordesch, *Evidence Record Syntax (ERS)*, IETF RFC 4998, 2007.

[15] A. J. Blazic, S. Saljic and T. Gondrom, *Extensible Markup Language Evidence Record Syntax (XMLERS)*, IETF RFC 6283, 2011.

[16] ITU-T, *ITU-T Recommendation X.509 (2008) - ISO-IEC 9594-8:2008*,

2008.

[17] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF RFC 5280, 2008.

[18] S. Santesson, M. Nystrom and W. Polk, *Internet X.509 Public Key Infrastructure - Qualified Certificates Profile*, IETF RFC 3739, 2004.

[19] ETSI, *Qualified Certificate Profile*, ETSI TS 101 862, Version 1.3.3, 2006.

[20] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, IETF RFC 6960, 2013.

[21] C. Adams, P. Cain, D. Pinkas and R. Zuccherato, *Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)*, IETF RFC 3161, 2001.

[22] ETSI, *Provision of harmonized Trust-service status information*, ETSI TS 102231, Version 3.1.2, 2009.

[23] *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*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:en:PDF, 2012.