UNIVERSITÀ DEGLI STUDI
DI TRENTO

SecCord

How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results

White Paper 2013

Fabio Massacci, Olga Gadyatskaya (University of Trento)

Version 11.0
October 2013

This work has been partly funded by the European Commission under the FP7 SecCord Project. Opinions expressed here are not necessarily endorsed by the European Commission. The authors would like to thank the coordinators and technical leaders of the EU FP6 and FP7 Research projects on Security and Trust mentioned in this report (ABC4Trust, ASSERT4SOA, CUMULUS, GEMOM, INTERSECTION, MASTER, OpenTC, PICOS, PrimeLife, RASEN, SECONOMICS, SEPIA, SHIELDS, STORK, STORK 2.0, TURBINE, TRESPASS, WOMBAT) for providing information on their research results and their potential impact. Discussions with Ross Anderson, Jörg Schwenk, Amelia Andersdotter, Arnd Weber, Aljosa Pasic, and Massimo Felici were helpful to shape some of the issues in this report.

Department of Information Engineering and Computer Science
University of Trento
Via Sommarive 14, I-38123 Trento, Italy
tel: +39.0461.282086
fax: +39.0461.282093
https://securitylab.disi.unitn.it/

The Digital Agenda for Europe identified the protection of the EU citizens' personal data and the promotion of EU digital services growth as principal goals. The proposed Regulation on Electronic Identification and Trust Services for Electronic Transactions (eIDAS) can be an important step to achieve those goals. For the next decade it will shape security and trust requirements on the European identification and authentication, and trust services.

Yet considering eIDAS just a simple update of Directive 1999/93/EC on a Community Framework for electronic signatures would be a costly mistake. In the fast-evolving field of cybersecurity a decade is a tremendous amount of time. Looking 10 years ago, the world did not have social networks; mobile devices did not contain third-party applications and were considered relatively secure personal computing environments; and cybercriminals were far less organized [McAfee2011]. Understanding the current trends in security and contemplating the future risks could be pivotal for ensuring sufficient protection of Future Internet services.

This document discusses potential security and privacy issues related to electronic IDs and trust service providers, and proposes recommendations for the eIDAS draft based on the innovative technological contributions of EU Trust&Security Programme projects.

Identification vs Authentication

Scenarios of digital life are quite diverse, and new forms of web applications and services emerge daily. These services have different data protection requirements and require different level of user identification. For the scope of eIDAS we can distinguish *identification* (for the scope of this paper, sharing with a service a set of personal information that can non-ambiguously identify a person or a legal entity, e.g., full name, date and place of birth, or fingerprints) and *authentication* (sharing with a service a set of information that constitutes some personal data but does not allow identification, e.g., age, country of origin or partial cookies of a web session).

The proposal by the Commission consistently outlines the need for electronic identification schemes (e.g., Recitals 9 and 14, Articles 5 and 6, etc.), while authentication is not considered in Regulation and is not defined: only the definition of identification is present.

- **Article 3(1)** "electronic identification" means the process of using person identification data in electronic form unambiuously representing a natural or legal person;

Yet, **full and unambiguous identification may be too strong requirement**. For example, while an online banking site typically involves two factor authentication (user login and password plus a secure hardware token) and its operations are linked to actual physical identities of bank customers, a social network website only uses the login and password pair and typically wants to ensure its customers are older than 13.

- **Authentication corresponds better to the high data privacy standards of EU** (Directive 95/46/EC) and facilitates operations of some web services.
- Requiring always identification may be a risk for citizens and a burden for companies (as they would need to comply with the EU data privacy legislation).

The recent disclosure of massive surveillance programs by U.S. (PRISM), U.K. (TEMPORA) and other countries makes citizens' privacy risks concrete. Large operator provider would likely push for a complete identification of citizens as this would nicely fit their business models based on personalization and advertising. Yet those very personal details could be easily disclosed to a number of governments and potentially to criminal operators who could exploit vulnerabilities in the system (see our next point).

Article 1(1) of the Proposal states the Regulation lays down rules for electronic identification and electronic trust services for electronic transactions with a view to ensuring the proper functioning of the internal market. Absence of a privacy-protecting identification technology from being even defined in the Regulation means that **the EU internal market will offer EU citizens less privacy than it is technically possible**.

On the positive side, by pushing for strong privacy preserving credentials, **EU could also leverage the forward-looking research investment on technological means for authentication**. E.g., the ABC4Trust project is dedicated to an attribute-based authentication technology based on selective disclosure of attributes. It includes two pilots (deployed at a school in Sweden and at a university in Greece) for validation of interoperability and functionality of the technology. The project has demonstrated that notified eID schemes and privacy-preserving authentication schemes could co-exist and complement each other. ABC4Trust has also

issued a position paper advocating the attribute-based authentication required for the privacy data-minimization principle [ABC4Trust2013].
TURBINE has enabled secure and private identification via biometrics. The project has enabled creation of revocable identities from a fingerprint of a person. The identities can be used for authentication, but do not allow to restore the original fingerprint sample from them. A person using the TURBINE technology could create pseudonyms for different applications whilst ensuring those are unlinkable to each other.
Several projects focused on identification technologies and their privacy aspects (e.g., PrimeLife, PICOS, STORK and its current successor STORK2.0) have run multiple pilots with end-users and collected substantial data that might be used for analysis of privacy technology acceptance. Specifically, the SaferChat pilot of the STORK project has demonstrated that attribute-based authentication could be implemented via the eID scheme. STORK and STORK2.0 operate for ensuring identification schemes interoperability at the technical, semantic, organizational, standardization, and legal levels.
The SSEDIC project dedicates itself to a single cross-European digital identity scheme. This project brings together all stakeholders in the European digital identity domain and aims to identify a comprehensive roadmap for enabling the cross-borders single identity scheme.
A recent EU FutureID project desires to build a flexible, privacy-aware and ubiquitously usable identity management infrastructure for EU, which will integrate the existing eID technologies, trust services, emerging federated identity management services and modern credential technologies to provide a system for trustworthy and accountable management of identities. The project has started in 2012 and has not yet achieved its ambitious goal; however, it has conducted a study of requirements for cross-EU identity management and drafted possible solutions for overcoming potential conflicts in an open ID framework.
The innovative results produced by the EU research projects can be used as competitive advantage. If eIDAS requires authentication and other privacy preserving technologies, EU citizens will have more trust in electronic identity schemes and digital services. Otherwise, without being supported by existing Regulations, partial authentication will still lack behind. The Regulation will most likely have an impact also on semi-government-issued schemes (such as notary public associations, chambers of commerce, etc.) and therefore should consider the privacy issues from such a broader perspective.

> ***Recommendation.*** *eIDAS should consider the opportunity to enhance privacy for EU citizens by introducing a link to data protection and privacy obligations, and mentioning privacy-protecting technologies for authentication.*

This recommendation can be implemented by extending the notion of "identification" to "identification and authentication" and defining authentication in Article 3 if needed. This objective could also be achieved by issuing a separate Directive on Authentication (as envisaged by the EU Project STORK) or establishing tighter links with privacy obligation in connection with the Data Protection Directive.

Responsible Signing Requires Reading

Article 20(2) of eIDAS assumes the citizen liable for any document he/she has signed digitally in a merit equivalent to a handwritten signature:

- Article 20(2) A qualified electronic signature shall have the equivalent effect of a handwritten signature

It seems an obvious statement to re-instate from the previous legislation: the cryptographic mechanisms underlying the process of signing have not changed. Yet, **signing is not only about mathematics, it is about intent, and technological changes have made this statement no longer so obvious**.
Fig.1 shows the visualization path from the trusted signing device to the user. This path includes several third-party components from different providers; most of these components are known to be susceptible to attacks in the past. E.g., security companies reported in 2012-2013 on attacks at all popular web browsers and browser plugins (Java plugin, Adobe Flash plugin, etc.); and serious zero-day vulnerabilities were uncovered in OS Windows and Mac OS [Symantec2013], [HP2012]. The RSA Security company was hacked in 2011 and Siemens in 2012. Certificate authorities are not impenetrable either (e.g., DigiNotar and Comodo were hacked in 2011; Trustwave and TurkTrust issued faulty certificates in 2012 and 2011, resp.) [Roosa2013]. In this path, everybody can wave its liability off, only Alice can't. Even the 100+ Entities can walk out by suitable disclaimers (see our next point).

In this scenario, **when the user's machine is potentially compromised, it is not possible to ensure trustworthiness of the digital signature** produced by the machine: even if the signing mechanism is correctly implemented and the signing device is secure, attackers can replace the document to be signed (which is composed on the user's machine) or sign something stealthily. This is not a theoretical threat. A number of malware tools are on sale on the black market, customized for forging banking transactions for most financial institutions on the planet.

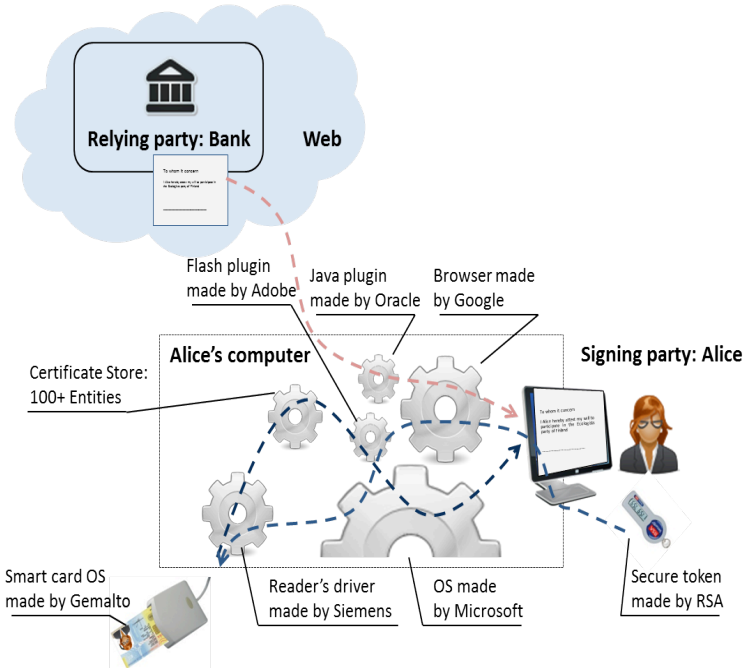

Figure 1 - The Foggy Road from Trusted Device to User's Eyes

Qualified trust service providers under eIDAS have to follow a set of obligations when providing a qualified trust service, including obligations to use trustworthy and temper-proof systems and products to guarantee technical security of the signature infrastructure and signing process. Yet, this is not a warranty (see the DigiNotar audit later in the paper), and this does not address the problem of the chain of trust in the end-user computer.

The assumption of the qualified signature Legislation is that all cryptographic computations are performed inside the signing device, not the user's machine. Nonetheless, the qualified electronic signature creation device specified in Article 3(8) may be secure, but it is hard to argue that holding the last secure bit in the chain makes this chain secure such that the requirements of Article 3(7)(c) will be satisfied:

> Article 3(7)(c) [advanced electronic signature].. is created using electronic signature creation data that the signatory can, with high level of confidence, use under his sole control

Akin problems are known to the banking industry since long time. False-terminal attacks (fake ATM machines placed in a public place in order to collect card data and PIN codes of passers-by) clearly demonstrate that cryptographic features of an ATM are of no help if the end-user cannot understand whether the ATM machine she is using is the one she intends to use. [Anderson2008]. Similarly, the signing device may be secure and reliable, yet the signing process encompasses steps not only by this device but by the end-user machine as well.

EU R&D projects (e.g., WOMBAT, SHIELDS and INTERSECTION) have investigated attacks at all levels of end-user machines and web services. Their results represented by vulnerability databases, malware samples and attack vectors show that computer systems consisting of multiple vulnerable components cannot be considered always trusted.

The concrete risk for lack of meaningful consent is well known to the Commission as indeed the opinion of Article 29 Data Protection Working Party (00461/13/EN WP 202) on apps on smart devices clearly shows:

> Opinion 02/2013 on apps on smart devices […]The key data protection risks to end users are the lack of transparency and awareness of the types of processing an app may undertake, combined with a lack of meaningful consent from end users before before that processing takes place.[…]

Very similar considerations are applicable to the process of digital signing: citizens are not fully aware of the processing that actually takes place on their machine when they exercise digital signing.

> ***Recommendation.*** *The digital signing process can become more secure if eIDAS requires a trusted path for visualization of a summary of the document to be signed.*

A solution to the trusted path problem could be a trusted device with a user interface or a new security technology for existing personal computing devices that will ensure security and trustworthiness of the full

procedure of digital signing. A number of EU research project worked on this field: for example a set of secure services including a trusted user interface was investigated by the FP6 OpenTC project, while the SEPIA project worked on its mobile counterpart.

Liability of Qualified Trust Service Providers

Trust service providers are responsible for issuing digital signatures and enabling identity management infrastructure control. The eIDAS proposal foresees liability for qualified trust service providers, but allows them to disclaim it. E.g., in Article 9 of the Commission's proposal **a trust service provider is deemed liable for any direct damage caused by failure to comply with eIDAS or negligence in the infrastructure protection**.

- Article 9(2) A qualified trust service provider shall be liable for any direct damage caused to any natural or legal person due to failure to meet the requirements laid down in this Regulation, in particular in Article 19, unless the qualified trust service provider can prove that he has not acted negligently.

Yet, **a way out of the liability is provided by Article 19(2)(c)**, which warns users to control the liability limits of trusted service providers:

- Article 19(2)(c) Before entering into a contractual relationship, inform any person seeking to use a qualified trust service of precise terms and conditions regarding the use of that service

Current practice of trust service provider is to use terms and conditions to actually limit liability. For example, the Italian trust service provider Aruba in its terms and conditions for certified email states that its liability is limited up to the amount paid for the service; the Royal Bank of Scotland in its terms and conditions for electronic signing devices limits its liability up to £65000 [T&CExamples2013].

The Legislation could be further strengthened. **The lack of economic incentive of trust service providers to secure their infrastructure and avoid issuing faulty credentials has already led to a critical situation in this area.** Certificate authorities get hacked, but they do not report this until it's too late, because they are not obliged to report security incidents.

This is well exemplified by the DigiNotar case in 2011 [Roosa2013]. DigiNotar was a Dutch certification authority, which was hacked in 2011 and a number of root keys was stolen. The attacker managed to issue a fake certificate for Google website that was subsequently used to spy on Iranian citizens. It has become apparent from subsequent investigations that the company knew that they had been hacked and that their certificates could therefore be falsified. However, they did nothing about it. The breach was discovered only after Iranian citizens reported to Google that Google Chrome would block an invalid Google certificate issued by DigiNotar. Notice that in the meantime the Dutch government believed to provide security to its citizens, while using in reality a certificate authority that was no longer secure. When the scandals erupted to the public, the Dutch government was forced to put down a notice that its web sites were no longer secure.

The eIDAS proposal requires the qualified trust service providers to report their security incidents:

- Article 15(2) Trust service providers shall, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities of any breach to security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

Reporting to a supervisory body is not an obligatory public disclosure: e.g., companies listed in the New York stock exchange must disclose security breaches in their **public** report to SEC [sec.gov2011].

Requiring that certification authorities comply with certain security standards is not a panacea either. Compliance with international standards for IT security, such as for example the US Government SCAP protocol, requires the company to rely on the current software vulnerability metrics to prioritize fixing security holes and updates. However, in the context of the EU Project SECONOMICS it has been shown that such practices do not necessarily lead to a relevant decrease in risk of attacks. On the contrary, they often lead to over- and mis-investments in IT security [Allodi2013].

As a matter of fact, DigiNotar, prior to its fall, was compliant with the EU and the Dutch regulations (including Directive 1999/93/EC). It was regularly audited for, e.g., the ETSI-standardized procedure for issuers of

qualified signatures. Yet, DigiNotar exercised poor security practices: its servers for issuing SSL certificates and qualified signatures were located in the same local network protected by a single weak password. It is highly probable that the qualified signatures server was compromised as well. However, even 1 year after the breach Dutch citizens' taxes could be submitted using DigiNotar certificates [Arnbak2012].

- **Citizens and companies may not have a choice among trust service providers**. For example, the qualified trust service provider of Italian notaries is their own council. The choice is given. This applies to other organizations as well (e.g. Chambers of Commerce) across all member states.

Recommendation. *Existing best practices in security can enhance the EU digital market if they are made applicable also to trust services providers, including immediate public reporting of security incidents and full liability for negligence. For example, trust service providers could be set to the liability laws similar to those of notary public. Notaries are liable for damages caused by negligence or misconduct when performing a notarial act. No prior demonstration of 'terms of use' can bring a notary out of this liability.*

Indeed, the absence of minimum liability limits of trust service providers is mentioned as one of the weak aspects of the eIDAS Proposal in, e.g., a position paper of the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM) [BITKOM2013].

Several EU R&D projects (e.g. MASTER, ASSERT4SOA, GEMOM, RASEN, TRESPASS and CUMULUS) have focused on infrastructure security (automated monitoring, event collection and analysis), compliance, and security and risk metrics; and they could provide the means for trust service providers to link their liability levels to their level of operational security. Techniques for infrastructure security status monitoring that can be leveraged for (semi)automated security breach notification to the authorities are valuable as well (delivered by, e.g. MASTER, ASSERT4SOA, CUMULUS).

Liability sharing could also be addressed by immediate notification provisions for security breaches and obligations for trust service providers to indemnify relying parties (in absence of such notifications). Notifications to relying parties can be implemented by timely revocation instruments. Even authentication based on biometrics can be revoked (as investigated by the EU project TURBINE). Therefore only the technical issue of notification remains to be resolved. In the increasingly connected world where push notifications are the hallmark of everyday devices such as mobile phones, this should not be a major hurdle.

References

[Symantec2013] Symantec "Internet Security Threat Report. 2012 Trends" Volume 18, Apr 2013

[HP2012] Hewlett-Packard "2012 Cyber Risk Report", 2012

[McAfee2011] McAfee "A Good Decade for Cybercrime. McAfee's Look Back at Ten Years of Cybercrime", 2011

[ABC4Trust2013] ABC4Trust "ABC4Trust Position Paper. Privacy-ABCs and the eID Regulation", 2013, at https://abc4trust.eu/download/documents/ABC4Trust-eID-Regulation.pdf

[Anderson2008] R.J. Anderson "Security Engineering. Second Edition". Chapter 10. Wiley. 2008.

[T&CExamples2013] Aruba "Terms and Conditions for Certified Email" http://www.pec.it/documenti/CondizioniFornituraServiziCertificazione_Vers%201.1.pdf (In Italian)

The Royal Bank of Scotland "Terms and Conditions for the TrustAssured Managed Identity Service" http://www.rbs.co.uk/Downloads/corporate/electronic/terms_and_conditions.pdf

[Roosa2013] S. Roosa and S. Schutze "Trust Darknet. Control and Compromise in the Internet's Certificate Authority Model" in IEEE Internet Computing 17(3), 2013

[sec.gov2011] Corporate Finance Disclosure Guidance. Topic Nr. 2 Cybersecurity http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[Allodi2013] L. Allodi and F. Massacci "How CVSS is ddossing your patching policy (and wasting your money)", at http://www.blackhat.com/us-13/briefings.html#Allodi

[Arnbak2012] A. Arnbak and N. van Eijk "Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain", at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409; and H. Ashgari, M. van Eeten, A. Arnbak and N. van Eijk "Security Economics in the HTTPS Value Chain" in Proc. of WEIS'2013

[BITKOM2013] BITKOM "Position paper on the proposal for an EU regulation on electronic identification and trust services for electronic transactions in the internal market" April 2013, at https://ameliaandersdotter.eu/wp-content/uploads/2013/04/20130408-BITKOM-Position-on-eID-regulation1.pdf