Theme [ICT-2011.1.4]
Trustworthy ICT

SECurity and trust COoRDination and enhanced collaboration

Project N° 316622

SecCord

Deliverable 3.1 Whitepapers

Responsible: Fabio Massacci, Olga Gadyatskaya (UNITN)

Document Reference:	D3.1 Whitepapers
Dissemination Level:	PU
Version:	1.0
Date:	October

Research and Innovation Impact of Trust & Security Programme

White Paper 2013

Fabio Massacci, Olga Gadyatskaya (University of Trento)
Frances Cleary (Waterford Institute of Technology)

Version 1.1
October 2013

Executive Summary

This white paper is a summary of key findings on the emerging issues of the Research and Innovation Yearbook 2013 produced by WP3 of the SecCord project. The aim of the Yearbook is to investigate the R&D projects executed under Trust & Security (T&S) Programme and present the discoveries of the study conducted with the project leaders to key stakeholders.

For this white paper we have identified two emerging issues to be presented in more details: the *NIS Platform initiative* and the *status of the EU ICT security domain* as reported by the interviewed R&D project leaders.

We would like to thank all project representatives that have participated in our study.

This work has been funded by the European Commission under the FP7 SecCord Project N° 316622 (http://www.seccord.eu).

Key Finding from Trust & Security Programme Analysis Executed in the Yearbook 2013

The Programmes' goals (as defined in the Work Programmes) were mostly addressed by the selected projects. The only sub-objective of the Work Programmes that was consistently not targeted by the selected projects regards coordination with the national and regional research programmes (of the Member States).

The EU funded T&S research projects are capable of providing expert contributions to the NIS Platform initiative proposed recently by the European Commission. The NIS Platform is an instrument that will work to improve the EU cybersecurity status. In this white paper we list the projects that have gained expertise and developed technologies in the domains currently defined in the NIS Platform:

- risk management and security awareness promotion in organizations;
- threats information exchange across organizations;
- roadmapping for secure ICT research and innovation.

The EU R&D projects produce results that have potential to be utilised in a variety of industry sectors, not only ICT Security: Critical Infrastructures and Emergency Handling; Energy and Utility; Software and IT Services; Healthcare; Telecommunications; Public Administration; Internet Services; and others. Industry players from these domains participate in many of the R&D projects as validation experts and actively seek to identify and adopt delivered technologies with high market potential.

Interviewed project participants actively shared their opinions on the status of the EU ICT Security domain. The interviewees reported their views, highlighting gaps in the industrial acceptance of the technologies delivered by research projects, and suggested addressing it with validation and exploitation-oriented small-scale projects and by putting more efforts into market analysis and technology maturity. Also the skills gap in the EU ICT Security domain was noted, and the lack of security awareness in citizens as well as employees. It is remarkable that the opinions of the project leaders are completely inline with the goals of the NIS Platform and the recent proposal for the new EU Cybersecurity Directive.

More information on the Trust & Security Programme and the details of our findings can be found in the Research and Innovation Yearbook 2013 of SecCord.

Addressing the Emerging Challenges of the NIS Platform

The EU R&D projects have acquired significant expertise in addressing the emerging network and information security issues and have greatly advanced the state of the art in this domain. Moreover, the EU policy makers and coordination bodies (such as the Network and Information Security Platform) can use these results and expertise to gain insights on the technological as well as social, economical and legal challenges in the strategic EU activities. In this section we list the T&S projects whose experience and innovative contributions are the most relevant to the identified security and trust challenges ahead of the NIS Platform (in Table 1).

The NIS Platform comprises three Working Groups[1]:

- *WG1 Risk Management*: will identify best practices to design, implement and maintain cybersecurity risk management processes throughout an organization. In particular WG1 addresses: *information assurance*; *risk metrics to monitor predict, track and evaluate risk exposure*; and *awareness raising practices* to acquire and disseminate cybersecurity knowledge and skills.
- *WG2 Information Exchange*: will identify best practices to exchange information on cybersecurity incidents of different nature (technology failures, human mistakes, natural events, malicious attacks) and on threats and vulnerabilities. The information exchange shall include steps to *communicate information within and outside an organization* including to businesses, government and technical bodies as well as to the public. In particular WG2 will identify *best practices for incident reporting*, including reporting tools and templates; *incident coordination*, including processes for exchanging information on actual incident to engage in a collaborative actions to handle incidents; and *exchange of information on threats and vulnerabilities* affecting systems. WG2 will also address *metrics, measurements and language for information exchange*.
- WG3 Secure ICT Research and Innovation: will identify *key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cybersecurity, privacy and trust*; and propose *new ways to promote truly multidisciplinary research that foster collaboration* among researchers, industry and policy makers. WG3 will serve as a facilitator for the *coordination of and collaboration between research agendas across Europe,* including industry research roadmaps and national research programmes. WG3 will also identify the *elements of a possible European industrial strategy for cybersecurity* and *examine ways to increase the impact and commercial uptake of research results in the area of secure ICT*.

The T&S research projects from Call 1 and Call 5 are over or close to completion; therefore their contribution can consist of already delivered artifacts and expertise gained by the project members. The projects of Call 8 besides providing the artifacts and expertise can also become platforms to execute the relevant actions proposed by the NIS Platform and evangelize recommended practices.
From the T&S research project to NIS Platform mapping, we can see in Table 1 that WG3 can enjoy contributions from the largest share of projects. Also WG1 can receive a rich input from the EU Trust & Security projects. Instead the WG2: Information exchange has fewer projects that have contributed to its goals, most of them from Call 1 and Joint ICT-SEC Call.
Notice that Table 1 lists only the projects that either directly focus on the targets set upon the NIS Platform Working Groups, or provide enablers for these targets. Yet, all the FP7 Trust & Security Programme projects have delivered/are set to deliver results that can be potentially useful for achievement of the NIS Platform goals

Table 1 Projects that can contribute to the goals of the NIS Platform working groups

NIS PPP Working Group	Projects from Call 1	Projects from Call 5	Projects from Call 8
WG1 Risk Management	**INSPIRE**: identification of vulnerabilities and development of techniques for security networked process control	**MASSIF**: a SIEM framework for scalable multi-level event processing and predictive security monitoring	**CYSPA**: a methodology to evaluate an impact of cyber-disruptions on an organization

[1] https://resilience.enisa.europa.eu/nis-platform

	systems **MASTER**: a system for ensuring compliance with regulations and policies by an organization **MICIE**: an alerting system to identify in real time and predict the level of threats induced on a critical infrastructure **VIKING**: estimation of security risks and evaluation of disruption consequences in SCADA networks	**NESSOS**: delivers new curriculum for secure Future Internet services and software engineering **POSECCO**: a framework for enabling traceability between requirements and system configuration **SYSSEC**: delivers a new cybersecurity curriculum and promotes cybersecurity education **VIS-SENSE**: a visual analytics technology for identification and prediction of abnormal behavior patterns in network infrastructure	**MUSES**: a system to enforce corporate security policies and identify risky employee behavior via applying risk metrics **OPTET**: an approach to enable provable trustworthiness in socio-technical systems **RASEN**: enhancements to organizational risk assessment, including legal risk assessment **TRESPASS**: a tool to automate risk assessment for organizational socio-technical systems
WG 2 Information Exchange	**CONSEQUENCE**: a scalable, secure and resilient infrastructure for data sharing across multiple organizations **FORWARD**: a cross-EU platform for monitoring of threat landscape evolution **MICIE**: an alerting system to identify in real time the level of possible threats induced on a critical infrastructure and notify the authorities **PEACE**: an emergency management framework for establishing a secure and reliable communication in critical situations **SECURESCM**: protocols and tools to secure computation on shared data **TAS3**: a trusted service architecture to manage and process distributed sensitive information **SHIELDS**: a software security vulnerabilities repository **WOMBAT**: a repository of cyberthreats and methodologies for threat detection and analysis	**SYSSEC**: works on identification of the Future Internet vulnerabilities	**ACDC**: a EU cyber-defence centre for analysis of analysis of botnets and identification of countermeasures against them
WG3 Secure ICT Research and Innovation	**FORWARD**: coordination of working groups of experts in cyberthreats **INCO-TRUST**: coordination of research agendas, and fostering collaboration in the area of trustworthy, secure and dependable ICT **PARSIFAL**: coordination of research activities in critical finance infrastructure protection **THINKTRUST**: collection and analysis of technical and non-technical requirements of end-	**ACTOR**: supports the Trust in Digital Life consortium in support of the Strategic Research Agenda for Europe **BIC**: coordination of the EU research in trustworthy ICT and alignment of the EU vision with research programmes in Brazil, India and South Africa **EFFECTS+:** coordination and clustering of the FP7 Trust & Security R&D projects and development of	**CIRRUS**: a consortium encompassing different stakeholders for best practices in cloud security **CYSPA**: an association for analysis and prevention of cyber-disruptions and development of an integrated EU strategy for protection of cyberspace. **FIRE**: coordination of the EU Trustworthy ICT research, understanding avenues for its exploitation

	consumers in the area of secure, trustworthy and dependable ICT	future research directions **NESSOS**: a Network of Excellence in the services and systems security engineering that coordinates activities in this area **SYSSEC**: a Network of Excellence in the Systems Security domain that creates a research roadmap in this area	and development of roadmaps in key sub-areas **SECCORD**: coordination and clustering of the EU Trust & Security projects, and providing an outlook on the emerging T&S issues **STREWS**: a roadmap for future research and standardization for Web security

Status of the ICT Security Domain in EU

In this section we report the results of the interviews of project leaders of the Call 5 and Call 8 projects. We have asked the project leaders to identify the market acceptance gaps for their technology, and also to highlight potential strengths and weaknesses of the EU ICT security market. In this section we report the notable findings regarding weak spots of the EU ICT security landscape, specifically weaknesses of the EU projects, and how these can be overcome.

EU R&D Projects' Weaknesses

The projects often **do not execute market studies for their technologies and do not take costs into account** to ensure acceptance of their technology. The business model says security must also be economically viable, or at least have chances to become economically viable.

Often there is **a gap between research results and industry acceptance** and the problem of maturity of technology. Many outstanding research results have not been brought to industry, sometimes due to the usability issues. This could be to be taken into account by **putting more effort and rigour into the validation activities** executed in the projects. This will consume efforts from research, but may prove better for industry acceptance.

However, it may be **difficult for projects to plan validation and exploitation activities well ahead** of actually solving the research problems; moreover because writing a successful proposal requires to promise a lot of exploitation activities that might turn not to be viable in the end. This may be addressed by **introducing two project types**: one for basic research with a focus on innovation and problem solving, another with shorter time line and smaller group of partners to execute validation and exploitation of already produced results (e.g. through pilots and user trials).

Several project leaders have noted that the EU technology often appears when it is too late and the market is already taken by some other non-EU solutions. They have proposed to tackle this by **fostering disruptive innovation**. As an instrument, some projects can be launched that would focus not on improving existing technologies and tools, but on something completely new.

Another aspect mentioned concerns industrial participants of the projects. Typically research units of a company face the challenge that their product units typically are interested in shorter time horizons (1-2 years) than research units can offer (3 years from the project start plus some time for technology maturity). An option here is to **encourage industry partners to develop and demonstrate project results** in their products (e.g. by dedicated exploitation projects discussed above).

Often after the end of the project the technology is not maintained (people involved have changed job, no funding available, etc.). Some of the interviewees have suggested **a dedicated demonstration platform under the umbrella of the European Commission to provide support for technology** after the project lifetime.

As we have discovered, for the projects in Call 1 some websites are already not maintained and it may become difficult to discover the project contributions. An option to solve this problem might be **a centralized repository for public deliverables** (e.g. the Open Access framework or the CSP Forum (SecCord) website[2]). Notice that some active projects even do not publish on their websites all public deliverables. We suggest that it becomes obligatory to publish all public deliverables and maintain them accessible even after the project is finished.

[2] https://www.cspforum.eu/projects

Structural Issues with ICT Security in EU

Several project leaders have mentioned that the ICT Security Domain in Europe is too technology-oriented; it does not look enough at non-technological factors like usability. This highlighted issue also proved to be very relevant also to the EU Trust & Security projects; with it being addressed via the selected projects coming from Call 8;however further steps in these directions are required.

Another gap that the EU security industry might face is the **skills gap**. Most of the interviewees acknowledged the professionalism of EU security experts and leading positions the EU security industry has in most of the security fields, e.g. embedded systems, secure protocols, software verification. However, several project leaders have noted that the amount of students studying security is insufficient, especially in comparison with such countries as US or China. Also, Europe experiences a brain-drain: a lot of security practitioners leave Europe for other countries. **Promotion of graduate and post-graduate security education in Europe** can be an option to mitigate this gap.

Interoperability of legal and technological frameworks across the EU was mentioned to be missing due to the variety of regulations and practices across countries. This in turn implies hindrances of security solutions implementation, and therefore deployed solutions are often insecure or are not compliant with regulations. **Harmonization and standardization actions across the EU are required.**

EU Societal Security Challenges

Advent of Internet of Things and critical infrastructures connectivity to Internet will bring **new cyber threats**. The European Commission is already taking actions (since Call 1 and the Joint ICT-SEC Call). However, it was reported that the manufacturers were not yet taking this into account.

Strengths of the EU technical results, as identified by many interviewees, are strong orientation to an individual and protection of individual's privacy. As one of the project coordinators has put it: "*Europe has strong value system around trust and security"*. However, these **privacy concerns are often missing in the business design**. The coordinators expect that if the **EU will have very well defined security requirements and regulations, everybody will have to adapt**, including big non-European industry players, and this can be an opportunity for Europe.

Finally, one of the most raised concerns is the **low security awareness and lack of security education – in citizens as well as in organizations**. This challenge also aligns with the previously mentioned skills gap, however it is impacting not only the EU ICT security industry, but also the EU society as a whole. The lack of awareness is also a business problem: people are less willing to pay for security and privacy. However, in the end they pay even more in damages or taxes. Latest media scandals (e.g. the recent PRISM and Tempora revelations) and attacks on influential companies (Twitter or Apple) or critical infrastructures (the Stuxnet attack) slowly raise the awareness and situation tends to improve. However, the attacks are also becoming more serious. Therefore, it is necessary to **educate citizens and business professionals in security**, by raising the awareness, bringing more media attention to security issues and best practices in security, and introducing security courses into curriculums.

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, and Arnd Weber 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.

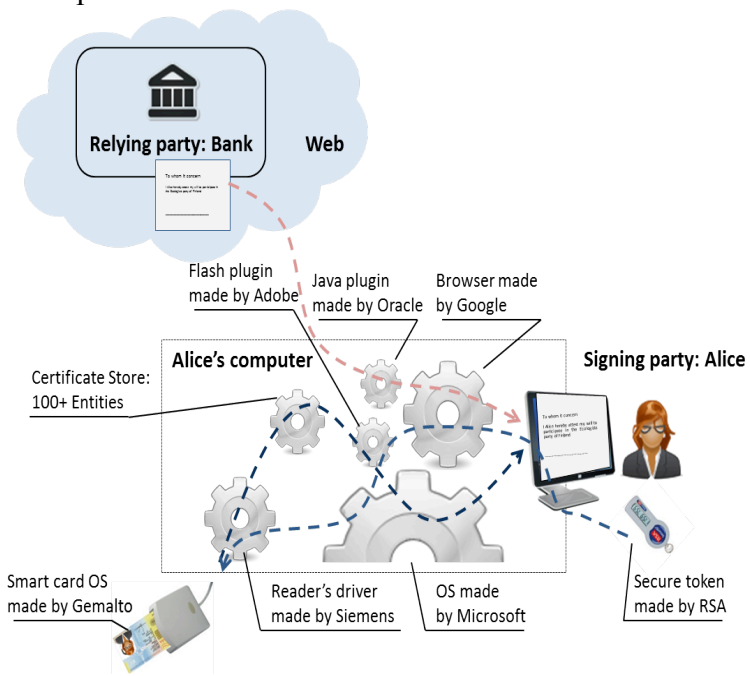

Figure 1 - The Foggy Road from Trusted Device to

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