ISSE 2012 Securing Electronic Business Processes

Helmut Reimer • Norbert Pohlmann
Wolfgang Schneider (Eds.)

ISSE 2012 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2012 Conference

Springer Vieweg

Editors
Helmut Reimer
TeleTrust Deutschland e.V., Erfurt
Germany

Wolfgang Schneider
Wiesbaden
Germany

Norbert Pohlmann
Aachen
Germany

ISBN 978-3-658-00332-6
DOI 10.1007/978-3-658-00333-3

ISBN 978-3-658-00333-3 (eBook)

Library of Congress Control Number: 2012948599

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Springer Vieweg

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE. Springer DE is part of Springer Science+Business Media
www.springer-vieweg.de

Contents

About this Book

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by eema and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar.

The range of topics has changed enormously since the founding of ISSE. In addition to our ongoing focus on securing IT applications and designing secure business processes, protecting against attacks on networks and their infrastructures is currently of vital importance. The ubiquity of social networks has also changed the role of users in a fundamental way: requiring increased awareness and competence to actively support systems security. ISSE offers a perfect platform for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the tenth ISSE book – another mark of the event's success – and with about 30 carefully edited papers it bears witness to the quality of the conference.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- **Ammar Alkassar**, Sirrix AG (Germany)
- **Ronny Bjones**, Microsoft (Belgium)
- **John Colley**, EMEA & (ISC)2 (United Kingdom)
- **Roger Dean**, eema (United Kingdom)
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, Security4Biz (Belgium)
- **Jos Dumortier**, KU Leuven (Belgium)
- **Walter Fumy**, Bundesdruckerei (Germany)
- **Michael Hartmann**, SAP (Germany)
- **Jeremy Hilton**, Cranfield University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)

- **Frank Jorissen**, tygris (Belgium)
- **Marc Kleff**, Siemens Enterprise Communications (Germany)
- **Hasse Kristiansen**, Ernst & Young (Norway)
- **Jaap Kuipers**, DigiNotar (The Netherlands)
- **Manuel Medina**, ENISA
- **Patrick Michaelis**, Research In Motion (Germany)
- **Norbert Pohlmann** (chairman), Institute for Internet Security, Westfälische Hochschule, Gelsenkirchen (Germany)
- **Bart Preneel**, KU Leuven (Belgium)
- **Helmut Reimer**, TeleTrusT (Germany)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jon Shamah**, EJ Consultants (United Kingdom)
- **Claire Vishik**, Intel (United Kingdom)

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers. With this book TeleTrusT aims to continue documenting the many valuable contributions to ISSE. We would like to thank Bundesdruckerei GmbH Berlin and itWatch GmbH Munich for their support.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

TeleTrusT – IT Security Association Germany

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities.

TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is carrier of the "European Bridge CA" (provision of public key certificates for secure e-mail communication), the quality seal "IT Security made in Germany" and runs the IT expert certification program "TeleTrusT Information Security Professional (T.I.S.P.)". TeleTrusT is member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Keeping in mind the raising importance of the European security market, TeleTrusT seeks co-operation with European and international organisations and authorities with similar objectives. Thus, this year's European Security Conference ISSE is being organized in collaboration with eema and LSEC and supported by the European Commission and ENISA.

Contact:

TeleTrusT – IT Security Association Germany
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17
10115 Berlin
GERMANY
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
http://www.teletrust.de

eema

For 25 years, EEMA has been Europe's leading independent, not-for-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

EEMA's remit is to educate and inform over 1,500 Member contacts on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and reports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by EEMA and its members is available to other members free of charge.

Examples of recent EEMA events include The European e-ID interoperability conference in Biel, Switzerland (Featuring STORK, TDL (Trust in Digital Life), SSEDIC & GINI) and The European e-Identity Management Conference in Paris.

EEMA and its members are also involved in many European funded projects including STORK2, SSEDIC, ETICA and Future eID

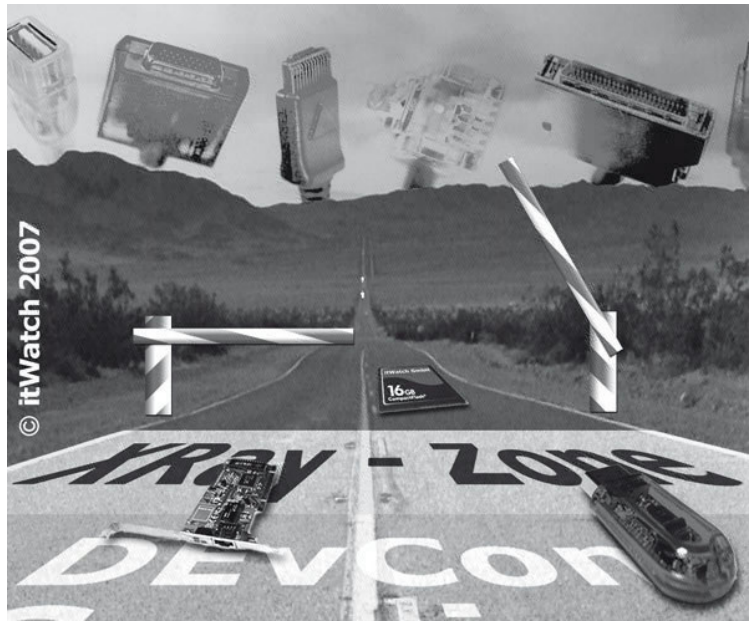
Any organisation involved in e-Identity or Security (usually of a global or European nature) can become a member of EEMA, and any employee of that organisation is then able to participate in EEMA activities. Examples of organisations taking advantage of EEMA membership are Siemens, Hoffman la Roche, KPMG, Deloitte, ING, Novartis, , TOTAL, PGP, McAfee, Adobe, Magyar Telecom Rt, Nets, National Communications Authority, Hungary, Microsoft, HP, and the Norwegian Government Administration Services to name but a few.

Visit www.eema.org for more information or contact the association on +44 1386 793028 or at info@eema.org

Data Loss Prevention in Real Life

Thorsten Scharmatinat

Key Account Manager
itWatch GmbH, Aschauer Str. 30
info@itWatch.de



1 Protection against data theft and security for devices

Stuxnet, PDF-exploits, Flame, tax CDs and Liechtenstein – there are various threats out there in the real world. And they all have one thing in common: the attacks are far from being trivial offence but are pursuing clear economical or even political goals. Government agencies and businesses are equally exposed to attacks on IT systems and sensitive data. How to protect yourself and your company against data theft and other prevailing risks, is subject to the following article.

Almost every day new security gaps and vulnerabilities in applications are made public. Often attacks, that exploit these vulnerabilities, are already there at - or even before - the time of publication, that is before a patch is available. The cause of almost 90% of the threats, according to the Microsoft Security Report 2009, are brought about by vulnerabilities in applications. What is more, the user usually doesn't even notice, that his computer has been infiltrated by malicious code and that an attack has happened. That is because the specially crafted applications use the permissions of the logged-in users, and without him noticing it withdraw data (apparently well-protected by disk encryption) via imported DLLs, Java scripts or embedded executables.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2012), 1-8

H. Reimer et al. (eds.), *ISSE 2012 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-00333-3_1,

Thus encrypted (http-s) sensitive data could be uploaded to rented storage space in the internet by a standard browser., Due to the encryption the firewall system will not even notice. Encrypted objects, nested archives and embedded objects in standard files may pose particular risks, since they can't be verified without the knowledge of the user.

Attackers may infiltrate malicious code into organizations, the malware being hidden in actually permitted file formats, or transported via email, web or even on USB sticks – without anybody noticing. A recent example is the Stuxnet worm, which among other things took advantage of a vulnerability in the LNK interface and was funneled into the company with the help of USB sticks. Stuxnet, which can target its attack and manipulation on industry control systems, clearly shows the fact, that nowadays the attacks aren't anymore trivial offences but purely economically and politically motivated attacks.

There are further reasons, why sensitive data is at risk, like improved attack methods, a lack of risk awareness and poor technical knowledge of the users, but also deliberate data theft by internal staff. Daily, there are reports on criminals selling highly sensitive data achieving good profit. The stolen information is brought through black channels to illegal markets. The reason behind the action could be personal vendetta, as it happened in Liechtenstein, or data being resold.

A lack of risk awareness or imprudence results in sensitive data not being treated with due care. During transport on mobile media for example the information is not adequately protected against loss or theft, be it by encryption or other appropriate measures.

2 Means of protection against threats

In the past service agreements were often used as a means of protection against the above threats. These measures alone can't guarantee effective protection anymore.

2.1 Service agreements

Service agreements are part of an organization's IT security policy, and are meant to regulate the use of information and communication media, such as PCs and mobile phones. With the help of organizational rules the use of email, surfing the web, network contacts as well as external storage devices like USB sticks is regulated. But even if very narrow limits for the use of these media are set, and the private use would be completely forbidden, a purely organizational policy cannot provide effective protection against modern attacks and a compromise of IT security or against a loss of confidential information. The reason is quite simple: An employee might not act against a valid rule of the security policy but even so his computer may still become the victim of attacks.

Information Security Strategy

Enterprise and Cloud Computing Security

Threats, Risks and the Derived Information Security Strategy

Lenka Fibikova[1] · Roland Mueller[2]

[1]Daimler Northeast Asia Ltd.
[2]Daimler Financial Services AG
{lenka.fibikova | roland.g.mueller}@daimler.com

Abstract

This article concentrates on the development of an information security strategy.

An information security strategy needs to focus on an overall objective, usually the objectives laid out in an organization's business strategy and its derived information technology strategy, where it takes the status quo and reflects the main objectives derived and postulates how and when to close the identified gaps. This strategy approach for improving information security is intended for an organization which supports an automotive and captive finance enterprise but is not restricted to this. The approach is aligned to the scope of ISO 270002 "Code of Practice for an Information Security Management System" [ISO05]. However, compliance is left out of the scope.

The strategy concentrates on four areas considered the relevant areas for information security: people, business processses, applications and infrastructure and has therefore a clear focus on processes, stability, resilience and efficiency which are the pillars of a successful enterprise.

1 Introduction

There are two main streams related to a security strategy nowadays – either it is considered an information security strategy and its main focus is on the three common objectives of information security which are confidentiality, integrity and availability (CIA) or it is considered a cyber security strategy and there are various discussions why cyber security has a broader view in addressing also objectives which go beyond the CIA objectives such as reputation and legal consequences.

Although a strategy should consider the latter objectives as well, we will make use of the more common term "information security" throughout this article. Therefore, we concentrate on an information security strategy and the main objective is the establishment of a "process driven organization with stable and efficient operations."

Today's information technology is in a flux where well-known techniques are now used in a way offering new opportunities for security and stability as well as for cost savings. Areas like virtualization, cloud computing, and big data are based on technologies which were examined and discussed for decades but can now be handled by the underlying technical equipment and the technical development. Also, the Internet is on a threshold which is not only triggered by higher speed but also by technical standards such as Internet Protocol version 6 (IPv6) and the Domain

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2012), 11-20

H. Reimer et al. (eds.), *ISSE 2012 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-00333-3_2,

Name Service Security Extensions (DNSSEC)[DNSS11]. Finally, the work life is changing and the limits between work and leisure are also in a move; the trend of BYOD or "bring your own device", social computing and social networks and tools like smart phones and tablet PC have played a major role in bringing work to the people.

2 Scope

The goal of implementing information security in an organization is to protect the organization's information by ensuring its confidentiality, integrity and availability.

Information is created and processed by employees, contractors and third party users (also known as information users) within business processes using applications and tools which are hosted in the IT infrastructure (see also Figure 1).

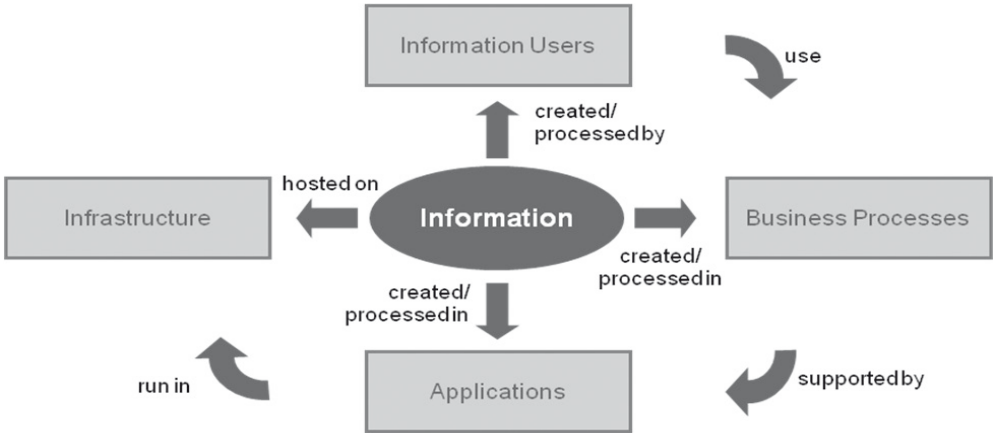


Fig. 1: Aspects of the information processing

Consequently, four areas need to be taken into account when implementing information security:

- **Information users,** or how people handle information and use tools and applications properly to protect information
- **Business processes**, or how information security is embedded within working practices
- **Applications,** or how well they are developed to ensure the protection of information stored and processed
- **Infrastructure**, or how well it provides sufficient capacities and adequate protection of information and applications against unauthorized access and modification

Information security is ensured via implementation of various measures. These measures need to

- cover all aspects of the four areas—information users, business processes, applications and infrastructure (**completeness**)
- provide adequate protection for information (**effectiveness**)
- be seamlessly integrated into the processes (**integration**)
- be supported by efficient tools and simple templates (**support**)
- avoid putting an unacceptable burden on the employees (**simplicity**)

Security and Privacy Impact of Green Energy

Human Factors of IT Security

Privacy-Preserving Smart Metering

Alfredo Rial[1] · George Danezis[2]

[1]IBBT and KU Leuven, ESAT-COSIC (Belgium)
Alfredo.Rial@esat.kuleuven.be

[2]Microsoft Research, Cambridge (UK)
gdane@microsoft.com

Abstract

Smart grid proposals threaten user privacy by potentially disclosing fine-grained consumption data to utility providers, primarily for time-of-use billing, but also for profiling, settlement, forecasting, tariff and energy efficiency advice. We propose a privacy-preserving protocol for general calculations on fine-grained meter readings, while keeping the use of tamper evident meters to a strict minimum. We allow users to perform and prove the correctness of computations based on readings on their own devices, without disclosing any fine grained consumption. Applying the protocols to time-of-use billing is particularly simple and efficient, but we also support a wider variety of tariff policies. Cryptographic proofs and multiple implementations are used to show the proposed protocols are secure and efficient.

1 Introduction

The concept of smart grid refers to the modernization of the existing electrical grid, including bi-directional communication between meters and utilities, more accurate meter readings and flexible tariffs [CPW09]. Expected electricity savings depend on matching generation and demand, achieved partly through dynamic tariffs with higher rates during peak consumption periods. Further savings are expected through the use of smart meter data for more accurate forecasting, more accurate settlement of costs between suppliers and producers (in the UK energy market) as well as customised energy efficiency advice. Both the United States and the European Union currently promote the deployment of smart grids.[1]

Currently, most smart grid deployment projects lean towards an architecture with severe privacy problems [AF10]: meters send all fine-grained measurements to the utilities or a centralised database. Yet, it is recognised that meter readings leak personal information. For example, load monitoring [Har92, LLC+] allows the identification of specific electrical appliances. As a result, detailed consumption data would facilitate the creation of user lifestyle profiles, including but not limited to house occupancy, meal times, working hours, or prayer or fasting patterns.

To alleviate such concerns, privacy impact assessments (PIA) are included in ongoing standardization processes. The National Institute of Standards and Technology (NIST) [The] lists fine-grained readings as being used for load monitoring, forecasting, demand-response, efficiency analysis and billing. Time-of-use billing is a major reason for collecting and storing all fine-

1 US Energy Independence and Security Act of 2007 and EU directive 2009/72/EC.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2012), 105-115

H. Reimer et al. (eds.), *ISSE 2012 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-00333-3_11

grained readings, and thus we use it to illustrate our techniques. Other computations on readings are also supported.

Consumer privacy concerns have already jeopardised the mandatory deployment of smart meters in the Netherlands [Cui], leading to a deployment deadlock. This deadlock stems from the assumption that smart metering is necessarily privacy invasive and that a balance needs to be struck between privacy and the social utility of fine-grained billing. Our work refutes this assumption: we demonstrate an architecture that guarantees privacy and high integrity for a very broad set of smart-metering and billing applications.

Our contribution. We propose a set of privacy-preserving protocols amongst a provider, a user agent and a simple tamper-evident meter. The meter outputs certified readings of measurements and gives them to the user, either directly or through a wide area network secure channel. For billing, the user combines those readings with a certified tariff policy, to produce a final bill. The bill is then transmitted to the provider alongside a zero-knowledge proof that ensures the calculation to be correct and leaks no additional information.

Our solution has the following advantages compared with other approaches.

- Complex non-linear tariff policies can be applied over individual meter readings or arbitrary periods of time (i.e. per day, per week). Other calculations can also be performed and certified to support forecasting, profiling, settlement, or fraud detection. Complex calculations are enabled by our scheme for applying non-linear functions as well as look-ups to certified readings, with efficient zero-knowledge proofs based on re-randomizable signatures. We provide concrete constructions for complex non-linear policies, and an evaluation of their performance.
- The need for certifying meter readings is the only modification necessary to the meters. Users can delegate the calculation of their bill or other computations to any device or service they trust without compromising the integrity of the scheme. Our key aim is for users to be able to perform all privacy friendly operations within a web-browser, keeping their experience of interacting on-line with their provider unchanged. We have implemented a web-browser Silverlight control that performs private billing computations to illustrate the practicality of this approach on deployed web technologies.
- We have optimized protocols to require *no additional communications* by the meter making it practical for immediate deployment. In fact, we have implemented and tested meter modifications on real-world meters in collaboration with a team from the Elster Group SE.
- When a simple tariff policy is applied, we can construct a very efficient protocol Fast-PSM for billing that requires no zero-knowledge proofs and is particularly well suited for time-of-use billing.
- Finally, our schemes have been shown to be cryptographically correct - i.e. our concrete protocols comply with an ideal functionality that expresses the privacy and integrity properties claimed.

Outline of our paper. We discuss related work in smart metering privacy in Sect. 2. Then we present the requirements and purpose of our protocols in Sect. 3 and we describe our system model in Sect. 4. We give a high level description of our protocol in Sect. 5 and we evaluate its performance Sect. 6. We conclude in Sect. 7.

Due to the space constraint a number of aspects of our privacy metering schemes are not described in this paper, but are available in the full report[2]. These include:

- A formal definition of security, a formal description of our protocols and the proof.
- A scheme that eliminates covert channels when meters are actively malicious.
- Different billing policies, including policies to encode splines and approximate arbitrary functions.
- A discussion of deployment and interoperability issues.
- Extensions of the scheme beyond the electricity metering setting.

2 Related Work

Smart meters privacy concerns have previously been studied both from a technical [LW08, MM09] and a legal perspective [CPW09, Qui09]. These works propose enforcement of privacy properties based on procedural means and assume that fine-grained billing inevitably requires the sharing of detailed meter readings.

Little work exists on the design of technical solutions to protect privacy in the smart grid. Wagner et al. [WSRH10] propose a privacy-aware framework for the smart grid based on semantic web technologies. Garcia and Jacobs [GJ10] design a multiparty computation to compute the sum of their consumption privately. The NIST privacy subgroup [The] suggests anonymizing traces of readings, as proposed by Efthymiou et al. [EK10], but also warns of the ease of re-identification. Molina et al. [MMSF+10] highlight the private information that current meters leak, and sketch a protocol that could use zero-knowledge proofs to achieve privacy in metering.

Some work focuses on more general aspects of smart grid security. Anderson and Fuloria [AF10] analyze the security economics of electricity metering. McLaughlin et al. [MMP09] analyze security of smart grids and conclude that they introduce new vulnerabilities that ease electricity theft. The design of algorithms that schedule energy consumption to reduce costs has also been addressed [hMrWJS]. Proposals to enhance the security of the smart grid infrastructure include Fatemieh et al. [FCG10]. No complete and thorough solution exists for computing privately individual bills when complex time-of-use tariffs are applied, or perform general private computations needed to run a modern grid (the special case of linear policies was independently studied in [JJK10] - yet it does not include the optimizations to reduce meter communication costs we present, making their approach very expensive).

Smart-metering is a special case of metering. LeMay et al. propose an architecture for attested metering [LGGG07] based on calculations performed on trusted hardware. Troncoso et al. [TDKP07] propose an architecture in which secure meters are used to calculate final bills for pay-as-you-drive insurance. Our protocol follows an approach similar to the one described in [BRT+10, dJJ08] for the design of a privacy-friendly electronic toll pricing system. We extend their paradigm of proving some aspects of a metering system using cryptography by providing full end-to-end verifiability for computations.

2 http://research.microsoft.com/apps/pubs/?id=141726

Future work. The work presented in this paper has already been extended in several works. In Kohlweiss et al. [DKR11] it is extended to obscure inferences that can be drawn from the final bill using a combination of differentially private mechanisms and oblivious payments. Kursawe et al. [KKD11] propose an aggregation protocol to privately sum readings from multiple meters, including protocols that are compatible with the protocols presented in this work, as well as making use of our low-communication overhead techniques to make aggregation practical. Finally, Fournet et al. have verified an implementation of the Fast-PSM protocol in Fine [SCF+10], and Aizatulin et al. [AGJ11] have done verification work on the concrete C implementation of our protocols for real-world meters. We will not be discussing further these extensions to the basic protocols presented here.

3 Design Goals and Rationale

We propose a protocol to preserve user privacy in smart metering applications that is flexible enough to be applied in a number of settings including electricity, water and gas metering. Our protocol guarantees the following security properties. First *integrity*: the utility provider is assured that the user reports the correct results of calculations. Second *privacy*: the provider does not learn any information but the result of computations. For the case of billing, the provider is ensured the correct fee is calculated based on the actual readings and time-of-use tariffs, without learning any fine grained readings. Finally, the provider cannot claim that a user must pay an incorrect fee.

The aim of our protocols is to keep meters extremely simple and to rely on cryptographic calculations outside the tamper-evident part of the meter for the integrity or specific calculations like billing. Meters need to be cheap and as a result have limited connectivity and bandwidth. They offer only a very limited user-interface that cannot deliver information about energy usage, efficiency advice, or detailed billing. Our protocols have been designed to impose a small computational overhead on meters, and a negligible communication overhead - both of which should be achievable without any additional hardware.

Once meter readings are certified and output from the meter, our protocols provide flexibility about where calculations are performed without compromising integrity. This flexibility means that devices and software performing the actual billing, or other computations on readings, can evolve over time while the meters remain the same.

Solutions for Mobile Applications

Identity & Access Management

Security of Mobile Devices, Applications and Transactions

Daniel Borleteau[1] · Nicolas Bousquet[2] · Thierry Crespo[3] · Xavier Dubarry[4] · Jan Eichholz[5] · Virginie Galindo[6]

Eurosmart
Rue du Luxembourg 19-21, B-1000 Brussels
eurosmart@eurosmart.com

[1]daniel.borleteau@renesas.com
[2]n.bousquet@oberthur.com
[3]thierry.crespo@st.com
[4]xavier.dubarry@morpho.com
[5]jan.eichholz@gi-de.com
[6]virginie.galindo@gemalto.com

Abstract

The world is going mobile! The usage of internet services is rapidly moving from PC systems to Tablets and Smartphones. Main drivers for this are user convenience and mobile connectivity. To ensure reliable transactions, user privacy and fraud prevention, secure solutions are the key for the user acceptance and a strong growth in the future.

The European security industry already offers the necessary technologies like secure elements in a variety of form factors, the SIMalliance Open Mobile API to allow an easy integration of secure elements in transactions and the Trusted Execution Environment to execute secured code.

Only a combination of these technologies will result in the right level of security.

1 Introduction

Mobile devices like smartphones and tablets have been conquering the market over the past 5 years. Consequently, a large amount of user transactions have been moved from PC-based environments to mobile devices. This includes banking, trading, shopping, data storage, eGovernment as well as other security sensitive procedures. As outlined in the recent European Commission Action Plan on eCommerce **[COMEC]**, the usage of online services and e-Commerce opens up a huge business potential. Security and interoperability are key factors in deploying those services successfully.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2012), 149-160

H. Reimer et al. (eds.), *ISSE 2012 Securing Electronic Business Processes*,
DOI 10.1007/978-3-658-00333-3_15

1.1 Mobility: driving factors

In the consumer area, the two main factors driving the adoption of new technologies are on the one hand, user convenience, and on the other, regulation (national or international authorities enforcing rules, standards). Mobile and permanent connection to social networks, email on mobile or tablet from your sofa, geo-localised based services: these new usages and applications are proving to be extremely convenient for users. The success of smartphones and tablets is clearly driven by user convenience. However, standards and regulations are key success factors to guaranteeing interoperability, contributing very much to user adoption (e.g. user privacy, security certification, etc.).

1.2 Mobility: enabling factors

Such user-friendly mobile devices have been made possible by the following enablers:

- Deployment of 3G and LTE cellular networks, as a viable alternative to ADSL networks for Internet browsing.
- Better performance/power consumption ratio for the application processors, enabling good user perception.
- Rich connectivity (WIFI, Bluetooth, NFC, GPS/geolocalisation, FM, etc.) enabling numerous new applications in various configurations.
- Thousands of applications made available through ecosystems built for facilitating development and distribution of applications.

In this environment, it is very clear that the mobile devices represent a major source of growth for the high-tech industry. This will continue and accelerate in coming years.

1.3 Mobility: What about security?

A few years ago, mobile phones had only one task to handle: to ensure that end-users were able to receive and send calls, delivering a voice service with high quality.

Today, since the onset of the smartphone, these devices have the responsibility of handling many new tasks; making voice calls almost a minor feature. The more features end-users have on their device, the less they call. They can play games, browse the Internet, take photos, play videos, exchange over social networks and so on. Smartphones embed and handle a great deal of sensitive assets that concern our privacy.

To this end, a strong growing trend is to make one's smartphone a mobile wallet. Although this trend is natural in an increasingly "paperless" world, new consequential threats have to be considered. Indeed, the more sensitive and valuable assets one's phone embeds, the more the need for security will grow.

We are seeing a convergence of most secure NFC applications, such as transportation and payment, into a single device; all sharing the same resources. As a consequence, the different kinds of assets need to be strictly separated within the device.

2 Secure Mobile Transactions in Practice

In the following sections we will sketch selected use cases in the field of ePayment and eGovernment. These use cases demonstrate the demands of users in respect to convenience and security.

2.1 Payment

Secure mobile payment can be achieved in the following ways:

- Contactless payment: the phone – if NFC enabled - can be used in a card emulation mode (the phone behaves like a payment card) and relies on the NFC interface to communicate with a contactless payment terminal.
- Remote payment: the phone provides access to:
  - banking applications / websites performing credit transfer. The financial institution is in charge of strongly authenticating the consumer.
  - e-commerce applications / websites for the purchase of goods or services. Card payment schemes are involved for a strong authentication of the consumer.
  - SMS services, billed through the mobile network operator. The operator is in charge of filtering SMS Trojans and authenticating the consumer.

For a remote payment, once the customer is ready to approve a sensitive operation (validating a purchase, consulting a bank account and validating a transfer), he or she is prompted to enter a password he or she knows (a specific PIN code for instance, but different from his bank card PIN). The password is checked by an external device (contactless card, token) or internal (SIM card, etc.) which then will open a secure channel with the distant server to perform a mutual authentication.

As expressed in the Green Paper **[COMEM]** "Towards an integrated European market for card, internet and mobile payments" from the European Commission, any sensitive personal information must remain in a secure payment infrastructure, whether for data processing or storing.

This protection rule concerns the PIN code, which must be protected when sent to the authentication device, and any credentials or cryptographic data sent to the remote server for ID verification. The Green Paper also recommends that parties having access to authentication data must be limited to those necessary in performing the transaction.

For mobile payment, the use of a Secure Element in the authentication mechanism appears necessary; access rights and methods to this Secure Element must be deeply controlled and secure.

2.2 eGovernment

Most European countries have issued electronic identity cards (eID) over the past years. One big benefit of these new eID cards in comparison to the classical paper-based identification cards is the possibility to use them for electronic government (eGovernment) services such as tax declaration, eVoting or other registry office related services.

Fig. 1: Mobile eID Infrastructure

As explained in chapter 1, the usability of services with mobile devices such as smartphones and tablets is growing in importance. This is especially true for eGovernment services. With the emergence of the NFC technology in these devices, the mobile use of contactless eID tokens is becoming natural (e.g. contactless national identity card). Beside eGovernment services, enterprises would like to use these electronic identity cards for Internet services (eBusiness-Service), such as retailers, banks and insurance organisations.

Imagine the case of a citizen who wants to check his pension records. To get access to these records, a strong authentication with his eID token is necessary. The eID token supports the contactless protocol and hence the citizen can use his tablet with NFC technology in combination with his eID. After entering his PIN code for identification purposes, the authentication process is performed and a secure channel is established from the back-end service to the tablet. The sensitive data is transferred through this channel and the user can check his or here records.

3 Threats for Mobile Devices

According to the Malicious Mobile Threats 2010/2011 report from Juniper Networks **[JMTR]**, instances of malware on mobile devices grew 250 percent between 2009 and 2010. Both banks and consumers need to understand how to detect and prevent fraud so that malware attacks do not grow at the same rate, nor exceed the rate, of mobile banking adoption.

3.1 Network vulnerabilities

Contrary to computers or tablets, phones are always connected to a network through various interfaces (Wi-Fi, Bluetooth, NFC, GSM, etc.) and thus become more sensitive to fraudsters.

3.1.1 Wireless interface

Even when users are careful selecting a Wi-Fi or GSM network, in places like airports, hotels or libraries, they can fall prey to «Man in the Middle» attacks on mobiles. Here, a fraudster who is positioned between the end-user and the server will eavesdrop or redirect transactions through his computer.

Trustworthy Infrastructures

Separation & Isolation

pohlmann@internet-sicherheit.de

eConsent Management and Enforcement in Personal Telehealth

Muhammad Asim[1,2] · Paul Koster[1] · Milan Petković[1,2] · Martin Rosner[1]

[1]Healthcare Information Management Department, Philips Research
{muhammad.asim | r.p.koster | milan.petkovic | martin.rosner}@philips.com

[2]Eindhoven University of Technology, The Netherlands

Abstract

Advances in information and communication technologies are expected to bring large benefits in the healthcare domain. Personal telehealth is one such example that has the potential to address some of the important challenges currently faced by healthcare such as improvement in the quality of healthcare delivery while at the same time reducing the cost. However concerns about information security and privacy are primary reasons for the lack of deployment of personal telehealth systems, besides problems with regard to safety and integration of multi-vendor systems. In this paper we present consent principles crucial to the privacy protection of individuals. Further, based on these principles, we describe consent management and enforcement functionality as outlined by the Continua Health Alliance and elaborate on how it can enable different usage scenarios with different trust levels and security requirements.

1 Introduction

Healthcare is one of the most important service sectors, and the largest in the US economy, that is under constant pressure to become more efficient. Currently, healthcare is facing fundamental challenges around the globe. The growing number of elderly people is one of the root causes for the increase in the healthcare cost. The costs are increasing because of a growing number of chronic diseases which make most of the costs. Furthermore, quality issues are becoming more important for the healthcare services. The demands of people for enhancing the quality of the healthcare services and reducing the medical errors through advancement in medical science and technology are increasing continuously. Patients are taking a more active role in the management of their own healthcare, which includes obtaining their disease information, discussing them with doctors, tracking and management of their symptoms and illnesses. They are becoming much more responsible and aware of their own health. Consequently, there is a trend for the patient empowerment, which means to include patients in the decision making cycle of their health and encouragement to proactively manage their health through lifestyle changes.

In response to the aforementioned challenges, there is a proliferation of information technologies in healthcare aimed at patient empowerment and reducing the medical errors with the expectation that they will solve the above challenges and will improve the quality of healthcare services. Both literature and everyday experiences confirm that such technologies have already influenced the practices in healthcare. Recent statistics show that 75-80% of the Internet users in the US search

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2012), 209-216

H. Reimer et al. (eds.), *ISSE 2012 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-00333-3_20

the Internet for health-related information [PIA]. Statistics in the European Commission reports [EC08] that 66% of European physicians use computers for consultations; among general practices, while 80% and 92% electronically store administrative patient data and medical data respectively.

However, concerns about information security and privacy are one of the primary reasons for the wider adoption of eHealth products and services. The patients' interest in the privacy protection and their safety needs to be balanced. The current data protection and healthcare legislations ask for an individual's consent whenever individuals' personal health records are accessed and used. Consent requirements are specified in different regulations such as the US Health Information and Portability Accountability Act, the Directive 95/46/EC of the European Parliament. Technical means are required to empower patients to manage their consent and afterwards enforce it whenever healthcare services are provided to the patient.

In this paper, we present the approach taken by the Continua Health Alliance in the domain of the personal telehealth services for the privacy protection of individuals taking their consent into account. Focusing on electronic consent (eConsent) principles in Section 3, we then describe eConsent management and enforcement solution as outlined by the Continua Health Alliance in Section 4 and elaborate on how it can enable different consent usage scenarios. In the following Section we give an introduction to the Continua Health Alliance and its end-to-end (E2E) architecture.

2 Continua Health Alliance

The Continua Health Alliance, formed in 2006 [FJLM10], is an open industry organization with more than 200 members. Its vision is to establish an ecosystem of interoperable personal telehealth devices and services that bring individual independence and empowerment and enable organizations to better manage health and fitness of their customers. Towards these objectives, Continua Health Alliance has identified the following barriers:

1. Technical: lack of interoperable personal telehealth products and services.
2. Regulatory: safety regulations hinder creation of the multi-vendor personal telehealth solutions.
3. Financial: economic value of the personal telehealth systems for the personal telehealth service providers is unproven yet.

Continua Health Alliance is working to provide solutions to the abovementioned barriers by providing the interoperability guidelines that foster the interoperability between the multi-vendor products, working with regulatory agencies to safely and effectively manage diverse vendor solutions and working together with the healthcare industry leaders for developing new financial models for addressing the cost of providing personal telehealth services.

2.1 Continua E2E Architecture

Continua specifies a reference architecture and interoperability guidelines [CGL12] for personal telehealth systems. The E2E architecture provides the definition of common concepts, topology constraints for devices in the Continua ecosystem and a basis for the development of the interoperability guidelines. The E2E architecture distinguishes different interfaces and device classes. An interface connects two reference device classes. In a real world deployment scenarios, a reference

device class can be considered as a role and a real world device can implement more than one role in order to support various deployment scenarios. Figure 1 provides an overview of the Continua E2E reference architecture. In the following we describe the Continua reference device classes and their functions in the Continua E2E architecture.

- ***PAN and LAN devices.*** These are medical observation devices, which measure vital signs such as weight, blood pressure, glucose, etc. These devices can be stationary, portable, body-worn, and have wired or low-power wireless connectivity to transmit the measurements to application hosting device (AHD) through PAN or LAN interfaces using semantics and format specified by IEEE-11073. The wired connectivity is based on USB while the wireless connectivity to the AHD can be based on low power personal area network technologies, such as Bluetooth-Low Energy, or can be based on low-power local area network centered wireless technologies such as ZigBee, which provides connectivity within a house.
- ***Application Hosting Device (AHD).*** This device acts as an interface for communication with the outside word. It extracts vital signs information from observation devices in a patient's house and forwards it in a secure fashion to the remote monitoring service using the WAN interface. Remote monitoring service could be a disease management organization (DMO) located on the WAN device. For vital signs communication, the WAN interface makes use of the IHE Patient Care Device transaction standard and SOAP-based web-services. The AHD can be stationary (e.g. PC, dedicated observation router) or portable (e.g. mobile phone, PDA). The AHD can also be potentially used to gather subjective information (e.g. surveys) from a patient.
- ***WAN device.*** This device hosts remote monitoring services that collects and analyzes the observation data in order to provide care. In case measurements fall outside the expected range, a nurse may prepare a Personal Health Monitoring (PHM) report and forward it to care providers e.g. a patient's family physician. The HRN interface facilitates the exchange of PHM documents.
- ***HRN device.*** This device hosts a set of health record services such as electronic health record (EHRs), personal health record (PHRs) and electronic medical records (EMRs). A service on the HRN device interacts with a service on the WAN device e.g. DMO using IHE XDS (Cross-Enterprise Document Sharing) family of standards.

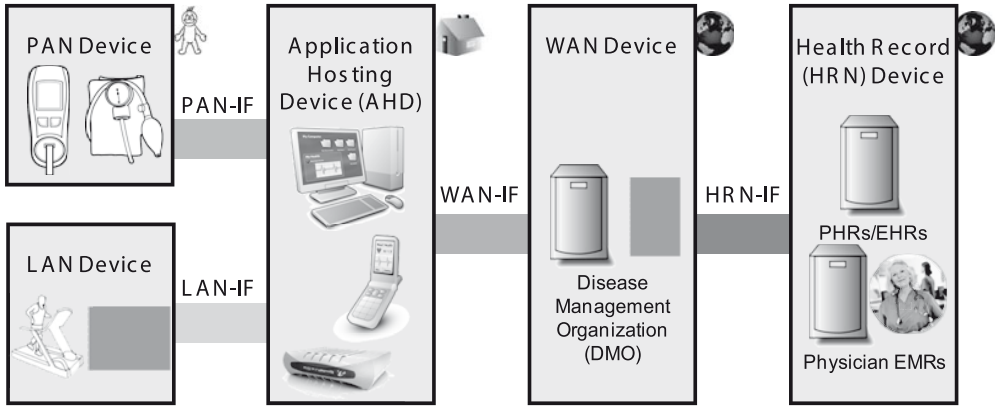


Fig. 1: Continua E2E reference architecture

EU Digital Agenda

Cyber Security: Hackers & Threats

pohlmann@internet-sicherheit.de

ETSI STF 428 – Accelerating Deployment of Interoperable Electronic Signatures in Europe

Juan Carlos Cruellas[1] · Andrea Caccia[2] · Konrad Lanz[3] · Giulana Marzola[4] · Luigi Rizzo[5] · Laurent Velez[6]

[1]Universidad Politécnica de Cataluña
cruellas@ac.upc.edu

[2]UNINFO
Andrea.caccia@studiocaccia.com

[3]IAIK TU
Konrad.Lanz@iaik.tugraz.at

[4]INFOCERT
giuliana.marzola@INFOCERT.IT

[5]INFOCERT
luigi.rizzo@INFOCERT.IT

[6]ETSI
Laurent.Velez@etsi.org

Abstract

This paper provides background information on the strategy of ETSI regarding the production of an integral package of tools for accelerating the production of Interoperable Electronic Signatures across Europe, provides hints on how its different components will fit within the new rationalized framework of European Standards on Electronic Signatures, and finally outlines the main achievements of the ETSI STF-428 project ("Quick fixes to testing of electronic signatures standards").

The paper provides details of two new ETSI Technical Specifications defining test suites for testing interoperability among tools that generate and validate PAdES signatures and ASiC containers respectively.

It also provides details of a new ETSI Technical Specification that defines a test suite for testing conformance of XAdES signatures against the new XAdES Baseline Profile approved by ETSI.

Finally it also provides hints on a tool that checks conformance of XAdES signatures against the aforementioned XAdES Baseline Profile.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2012), 271-281

H. Reimer et al. (eds.), *ISSE 2012 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-00333-3_26

1 Background

The European Telecommunications Standards Institute (ETSI, www.etsi.org) is well known in the ICT arena by its standardization activity. However, ETSI is also well known because the ETSI Centre for Testing and Interoperability (CTI, whose web page may be accessed at http://www.etsi.org/website/aboutetsi/howwework/testingandinteroperability.aspx), regularly organizes some of the major interoperability test events across the world.

Consequently, it is not surprising that ETSI Electronic Signatures and Infrastructures Tehcnical Committee (ESI, http://portal.etsi.org/portal/server.pt/community/ESI/307), in charge of producing standards and technical specifications for Electronic Signatures and Public Key Infrastructure within Europe, started a close cooperation with ETSI CTI as early as in 2003, when it concluded that the organization and conduction of interoperability test events would be a very suitable tool for accelerating the deployment of interoperable electronic signature tools across Europe.

In November 2003, ETSI organized and supported within its premises the first face-to-face interoperability test event on ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)", and in May 2004 ETSI organized and supported a new face-to-face interoperability test event on PKI and XAdES.

After that date, ESI TC and CTI started the inception of a holistic package of tools for supporting and accelerating the deployment of interoperable Electronic Signatures across Europe.

The **first element of this package was a portal** (ETSI Electronic Signatures Portal henceforth) for providing support to the organization and conduction of remote interoperability test events. Participants in these events would not need, by using portal's facilities, travel to ETSI premises and stay there for a whole week, as it is usual in the face-to-face testing events. Obviously this would result in a decrease of the resources required for participating and in the subsequent increase of the participants number. The public part of this portal may be accessed at http://xades-portal.etsi.org/pub/index.shtml.

In March 2008 ETSI organized and conducted the first remote interoperability test event on XAdES, supported by the aforementioned portal. Since that date, ETSI has organized, supported, and conducted a number of remote interoperability test events on the different formats for advanced electronic signatures, namely XAdES, CAdES (ETSI TS 101 733: "CMS Advanced Electronic Signatures (CAdES)") and PAdES (ETSI TS 102 778; "PDF Advanced Electronic Signatures (PAdES)"). The number of participants has increased from event to event, and even attracted entities from Asia and America. ETSI has also organized and conducted two interoperability test events on the so-called Trusted Lists (TLs henceforth) that each EU Member State has to generate and maintain. These TLs list supervised and accredited Certificate Services Providers, according to what is specified in the Annex to Decision 2009/767/EC. The public part of the TSL portal may be accessed at http://tsl-portal.etsi.org/pub/index.shtml).

The **second element of the aforementioned package is two sets of technical specifications**. The first set will include a number of technical specifications containing carefully defined test-suites for testing crucial interoperability aspects of tools that claim alignment with a number of standards or technical specifications. These test-suites will, consequently, be used in future interoperability test events. The second set will include a number of technical specifications defining

test-suites for testing conformance of tools against certain standards and technical specifications. These test-suites will constitute the basement on which the third element of the holistic package will be built.

The **third element of the package is a set of tools** devoted to test conformance of tools against certain standards and technical specifications. So far, two of these tools have been developed. The first one was developed by the UPC during the first interoperability test event on tools claiming alignment with the Annex to Decision 2009/767/EC. It checks conformance of the Trusted Lists generated by EU Member States against the aforementioned annex. At present, EU Member States may continuously check their TLs. The second tool has been developed within the context of the STF-428.

As far as the authors of this paper are aware, ETSI is the only standardization organization in defining such accelerating package and systematizing its construction in parallel with the development of the reference standards.

During 2010, ETSI and the Comité Européen de Normalisation (CEN) raised to the European Commission a number of proposals for, firstly build up a proposal for a new rationalized framework of European Standards related to Electronic Signatures, PKI, and Trusted Services Provision; and secondly for quickly fix a number of issues uncovered in the set of European Standards and technical specifications on Electronic Signatures. One of these last proposals focussed on moving forward the construction of the aforementioned accelerating package, and its approval led to the Specialists Task Force (STF) 428: "Quick fixes to testing of electronic signatures standards". The STF 428 web page may be accessed at http://portal.etsi.org/STFs/STF_HomePages/STF428/STF428.asp.

2 Scoping ETSI Specialists Task Force 428

STF-428 construction process started in January 2011. The team was formally constituted in February 2011. The project finalized in April 2012. When ETSI ESI proposed this project to the European Commission, the following elements were available:

1. The ETSI Electronic Signatures Portal contained one section for supporting remote interoperability tests on XAdES and one section for supporting remote interoperability test events on CAdES. Each section contained its corresponding test-suite and additional material needed by participants for correctly using the portal during the test events (including explanatory material, and communication means).
2. The ETSI Electronic Signatures Portal contained a third section devoted to support interoperability tests of Trusted Lists.
3. Finally, the ETSI Electronic Signatures Portal, also contained a fourth section where the aforementioned Trusted List Conformance Checker Tool had been deployed and made accessible to the EU Member States organizations in charge of generating and maintaining the EU Member States Trusted Lists.

In the view of the status detailed above, and regarding the first element of the accelerating package ETSI ESI decided that the STF-428 should aim at including in the Electronic Signatures Portal two new sections for supporting remote interoperability test events: one section for ETSI TS 102 778; "PDF Advanced Electronic Signatures (PAdES)", and one for ETSI TS 102 918: "Associated

Signature Containers (ASiC)", which specifies a format for containers that associate signed documents with their detached signatures. Once completed these sections, the portal would be able to support test events on each of the Advanced Electronic Signatures (AdES henceforth) formats and also on the ASiC package format.

Regarding the second element (the two sets of technical specifications), ETSI ESI decided to focus the STF-428 activities in defining test-suites for supporting interoperability tests on the two ETSI major Advanced Electronic Signatures formats specifications, namely PAdES and ASiC, for which no work had been previously done. Once completed these two technical specifications, ETSI ESI would have defined test-suites for testing interoperability of each of the AdES formats (XAdES, CAdES, and PAdES), and the package format ASiC.

Finally, regarding the third element, ESI decided to concentrate the efforts in supporting the development of a conformance tool against the ETSI TS 103 171: "XAdES Baseline Profile". This specification has been developed by the brother project STF-426 and defines a profile for XAdES signatures being used "in the context of the Directive 2006/ 123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (…) and any applicable context where qualified signatures are used". ETSI ESI considered this as the first step towards the production of a tool for testing compliance of tools against the ETSI TS 101 903 (XAdES). As a pre-condition of this tool, there was the need of producing a companion technical specification devoted to define the full set of tests that should be performed on any signature claiming conformance against ETSI TS 103 171. This product, actually being part of the second element of the accelerating package, was also incorporated to the set of deliverables to be produced by the STF.

As a consequence of the former considerations, ETSI ESI included in the STF-428 Terms of Reference, the following objectives:

1. To produce one ETSI Technical Specification defining a test suite for testing interoperability among tools generating and validating PAdES signatures.
2. To produce one ETSI Technical Specification defining a test suite for testing interoperability among tools generating and validating ASiC containers.
3. To produce one ETSI Technical Specification defining a test suite for testing conformance of electronic signatures against the ETSI TS 103 171 (XAdES Baseline Profile).
4. To develop a tool that implements the aforementioned test suite and tests conformance of electronic signatures against the ETSI TS 103 171 (XAdES Baseline Profile).
5. To build, within the ETSI Electronic Signatures Portal, one section for supporting remote interoperability test events on PAdES signatures and one section for supporting remote interoperability test events on ASiC containers.

3 ETSI STF-428 Major Achievements

This section provides details of the major achievements of the STF-428. Section 3.1 summarizes the products that have been incorporated in the ETSI Electronic Signatures Portal (first component of the accelerating package); section 3.2 reports on the contribution to the second component, namely, the different technical specifications defining different test-suites, is detailed; finally section 3.3 reports on the contribution to the third component, namely the XAdES Baseline conformance testing tool.