CRYPTOMATHIC

Cryptomathic's Response to Eurosmart Paper on Server Signing

1 Background information

In September 2014, Eurosmart published a position paper[1] on server signing within the eIDAS regulation. The eIDAS is driven by the European Commission Directorate General and has received a mandate to provide a comprehensive and predictable legal framework in view of boosting user empowerment, convenience and trust in the digital world, especially for promoting the widespread use and uptake of electronic identification and trust services (eIDAS)[2] within the internal market.

Central to this is the use of electronic signatures by citizens and their empowerment capacity for conveying trust in the digital world. By law, eIDAS has made a Qualified Electronic Signature (QES) equivalent to a handwritten signature. The initial intention was that a QES would be calculated on smart cards that have undergone a Common Criteria evaluation to be recognized as a Secure Signature Creation Device (SSCD).

Yet, deployments based on smart cards remain extremely scarce. In contrast, some countries have deployed Signature Server Solutions and have already proven more than strong enough with national solutions in Denmark, Norway, Sweden, Luxemburg and Austria with a total of more than 10 mill users – and there is no intention in these very successful solutions to use smartcards for cost and usability reasons.

A task force consisting of industry leaders, government organisations and standardisation bodies has therefore been formed to set some security standards for remote server signing such that solutions may be certified as Qualified Electronic Signature Creation Device (QSCD)[3], i.e. empowering EU citizens to generate QES using a remote signature server. The first step is to identify the scope of the security target and define a protection profile to be enforced by the server signing solution if they want to be recognised as QSCD. This enforcement will in the future be validated by a laboratory as part of a Common Criteria evaluation. It is currently being debated in the working group whether a client side sole control component should be included in the protection profile.

Eurosmart, a Brussels based lobby association founded by large players active in smart card or integrated circuit industry, has issued a position paper where they *urge the CEN WG 17 to finalize the server signing PP [Protection Profile] as a key issue, so that it can be referenced by the secondary legislation*. A clear position is taken, which – not surprisingly - is strongly favouring the introduction of Secure Element based user and data authentication, prior to generating a qualified electronic signature through a remote QSCD signature server.

Eurosmart states: *The smart security industry believes only a solution using a certified hardware device known as a Certified Secure Element meets the requirements of the definition of the eIDAS Regulation for Qualified Electronic Signature*. Such a statement emphasises the strong microcontroller bias of the Eurosmart paper, which lacks technical content and a vision for central signature services. In this document, we explain why this would go against the spirit of server signing and then propose a technology neutral alternative based on work carried out recently by the European Central Bank. This is food for thought rather an urge from the software industry to adopt an industry biased protection profile to protect our market.

2 Spirit of the revision

Favouring chip centric solutions is not the intention of the European Commission for the new eIDAS regulation. The main purpose is to foster the use of QES by EU citizens. In [2], one of the top level targets for the eIDAS is for 50 % of citizens to use eGovernment by 2015, with more than half returning completed forms. This can only be achieved through increased usability, lower costs and a fair level security based on interoperable solutions available on the market.

If one follows the Eurosmart position paper, where one must use a smartcard with a Secure Element to log on and authenticate against the remote signature server, then not much is won. Then you might as well generate the signature in the secure element – and handle everything locally on a legacy SSCD, closing the door to QSCD entirely, which is probably the hidden agenda behind the Eurosmart paper but certainly not eIDAS's intention. Whilst (strong) user authentication is important to help ensure sole control of the user over his/her signing key, it is important to remind the reader that there are other ways to achieve strong user authentication without relying on a secure element (e.g. using 2 factor authentication popular for online banking). Additionally, the security of remote signing servers does not solely rely on strong user authentication.

3 Usability

Eurosmart suggests introducing a Secure Element in the scope of the protection profile. This position is difficult to understand when the entire payment industry is moving away from it or at least lowering its requirements to bypass this technology that has been available for a decade and rarely used in everyday life.

[1] http://www.eurosmart.com/images/doc/Publications/Eurosmart%20Position%20Paper%20-%20Server%20Signing%20within%20the%20eIDAS%20Regulation.pdf

[2] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond

[3] http://ofti.org/wp-content/uploads/2013/09/FeasibilityStudyonanElectronicIdentificationAuthenticationandSignaturePolicyIAS.pdf

Google, VISA, MasterCard and Apple have recently learned the lessons from the slow uptake of TSM technology and launched Host Card Emulation to tackle this issue and allow low value mobile proximity payments to be carried out without relying on a Secure Element.

At the same time, as pointed out above, there are already a number of nationwide solutions implemented, which are so successful that all communication between citizens, companies, public entities and banks is now digital, e.g. in Scandinavian countries, without depending on the Secure Element approach.

Client side applications should remain out of scope of the protection profile as it would otherwise force every application provider to certify its applications and renew this certification over time. This is too strong a barrier to effectively foster the uptake of electronic signatures, which desperately need to be available to a countless number of business or eGovernment applications including fat clients for email signing, document signing etc., and thin web-enabled clients integrated with a web application server. Digital signatures need to be integrated in a business workflow as they are only a means to an end. The signature capability alone is pointless if it is not integrated with client apps to allow for documents / data / transactions to be signed by their intended signatories.

4 Lower costs

It is important to stress that the slow uptake of signature solutions is partially caused by its current cost impairment.

Any solution that drives up the deployment costs will have a negative impact on the deployment figures. Contrarily, a solution that has a low per-unit cost and which can leverage existing technology will make business players and end-users strongly consider QES.

It is therefore crucial to ensure that the security requirements are targeting the signature service provider operating the central signature solution and not the end-users or application providers since the latter currently need convincing arguments to embrace the technology.

5 Fair level of security

There is no need to make central server signing technology stronger than smart cards. In most cases, local SSCDs offer low authentication and no data authentication. When the smart card is connected to the device, any malware or Trojan can take control of the smart card and sign data without the user´s consent and leaving virtually no trace to be used in case of disputes[4].

In case of server signing, it is important to note that although the contents of the signed message is hidden from the server, the signature generation process will always leave a system trace (log) on the server which can be stored in an integrity protected database table, to be used in case of disputes. This gives a considerable security advantage to central server signing as centralised trustworthy logging will, by design, never be available to SSCDs. This certainly creates a different security paradigm shifting the security requirements towards back-end security design and communication protocols as opposed to client/application side for local SSCDs. What matters more in remote signature solutions is to enforce that a secure signature activation protocol is used in combination with a Signature Activation Data (SAD) and to address of the key challenges of all, namely ensure that what you see is what you sign (WYSIWYS)[5] which Secure Element does not even remotely address.

[4] In 2011 Alienvault detected a new version of Sykipot, a computer Trojan.
The virus is understood to run a so-called "spear phishing" attack against smart card keyboard based PIN entry.
The attack occurs when a smart card is inserted into a reader, at which time the malware acts as an authenticated user which can be controlled by the attackers thereby enabling attackers to access both card based information and on-card functionality, such as creation of a digital signature.
Another attack was on the US Department of Defence PKI cards. A paper has shown that using a DoD CAC on a untrusted workstation can allow a variety of attacks to be performed by malicious software. These attacks range from simple PIN phishing, to more serious attacks such as signatures on unauthorized transactions, authentication of users without consent, unauthorized secure access to SSL enabled web servers as well as remote usage of the DoD CAC by attackers.
http://cactus.eas.asu.edu/partha/papers-pdf/2007/milcom.pdf

[5] Information Security Technical Report 01/1999; DOI: 10.1016/S0167-4048(98)80005-8
http://www.researchgate.net/journal/1363-4127_Information_Security_Technical_Report

6 Signature activation protocol

The purpose of this protocol to authorise the signature operation on a given message (or a representation thereof such as a hash value of the message to be signed)[6] using a private signature key associated to a signatory. This process is defined in order to keep the signature operation under sole control of the signatory even if executed on a remote server. The signature activation protocol uses Signature Activation Data (SAD) in order to reach the sole control assurance level 2.

In addition, it is a natural requirement that the vendors demonstrate that the protocol is resistant to man-in-the-middle attacks and ensures the integrity and confidentiality of the message to be signed is not tampered with during transit. The assumption that Two-factor OTP solutions are prone to hacking from man-in-the-middle/browser/phone attacks [1] (page 6) comes from a lack of knowledge in security protocols which go beyond simple SSL session protection. Protocols such as Secure Remote Password (SRP) addresses this specifically[7]. Two Factor Authentication is more than just hardware authentication and can feature multiple authentication mechanisms, including the use of two independent channels, which is a very effective showstopper to man-in-the-middle attacks.

7 Signature Activation Data

Please recall that a digital signature is useless without guarantying the integrity of the data to be signed in the first place, and that the signature shall also be validated. This includes verifying the integrity of the signed data.

It is therefore not of primary importance for the SAD to be linked to the DTBS. The main purpose is to link the SAD to the signatory. The protocol may, in addition, bind the submission of the SAD to a particular electronic signature creation operation.

Strong user authentication - used to strengthen the SAD with non-predictable data -has been defined by the European Central Bank in its *recommendations for the security of internet payments*[8] derived from the EC Payment System Directive[9].

Though the scope differs, we believe the paper can be used as a reference as it sets some security recommendations which need to be enforced by Feb 2015. The release follows a two-month public consultation carried out in 2012 and is technology neutral.

The main recommendations include:

• to protect the initiation of internet payments, as well as access to sensitive payment data, by strong customer authentication;

• limit the number of log-in or authentication attempts, define rules for internet payment services session "time out" and set time limits for the validity of authentication;

• […]

• implement multiple layers of security defences in order to mitigate identified risks;

• provide assistance and guidance to customers about best online security practices, set up alerts and provide tools to help customers monitor transactions.

The detailed recommendations will be integrated into existing oversight frameworks for payment schemes and supervisory frameworks for PSPs [Payment Service Providers] and are to be considered as common minimum requirements for internet payment services. The members of the Forum are committed to supporting the implementation of the recommendations in their respective jurisdictions and will strive to ensure effective and consistent implementation within the EEA.

Given that electronic signatures are a way to consent approval for transactions, we strongly propose this paper be taken as a reference as discussed below. The enforcement process targets the financial industry, which is one of the key markets for electronic signatures. Harmonisation is therefore of primary importance to ensure that the security requirements yield in the same direction.

[6] Also denoted in the ETSI/CEN working group as Data To Be Signed (DTBS) and Data To be Signed Representation (DTBS/r)
http://srp.stanford.edu/analysis.html

[7] The SRP protocol, version 3 is described in RFC 2945.

[8] https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

[9] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007,

In addition, providing digital signature services is a natural value-added enhancement for internet payment service providers providing cards, credit transfers, e-mandate or e-money services[10] online. Building a security framework that leverages the existing ECB security requirements is therefore a natural step forward.

In particular, paragraph 3 defines strong user authentication as:

Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:

i) something only the user knows, e.g. static password, code, personal identification number;

ii) something only the user possesses, e.g. token, smart card, mobile phone;

iii) something the user is, e.g. biometric characteristic, such as a fingerprint.

In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.

This 2FA definition by the ECB has been drafted to remain **technology neutral.** *It does not attempt to set specific security or technical solutions. Nor does it redefine, or suggest amendments to, existing industry technical standards or the authorities' expectations in the areas of data protection and business continuity.*

It is probably useful to mention that signatures engage their signatories to the data that they sign in such a way that any vis-a-vis person can reasonably rely on them to complete an action or transaction. This liability is also present when someone agrees to a transaction presented by an internet PSP.

8 Conclusion

Whilst 2FA is just one security aspect of the entire security design for the user to retain control over his signing key, as well as the signing process from anywhere in the world, it is important that this step remains completely technology neutral and the position of the ECB can probably set the benchmark. On the contrary, the Eurosmart position paper has a strong chip bias and contradicts the spirit of the iDAS. Additionally, it does not set any recommendation on the protocol side, neither does it help solve the WYSIWYS challenge. In light of the poor technical substance, it is preferable to disregard the publication for the definition of a security standard relating to trustworthy server signing.

[10] Extracted from page 2

Disclaimer

Jægergårdsgade 118, DK-8000 Aarhus C, Denmark

This document is protected by copyright. No part of the document may be reproduced in any form by any means without prior written authorisation of Cryptomathic. Information described in this document may be protected by a pending patent application.
This document is provided "as is" without warranty of any kind.

Cryptomathic may make improvements and/or changes in the product described in this document at any time. The document is not part of the documentation for a specific version or release of the product, but will be updated periodically.

ABOUT CRYPTOMATHIC

Cryptomathic is a leading innovator and provider of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With more than 25 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing and advanced cryptography and key management, utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at www.cryptomathic.com