The Impact of the European eIDAS Regulation

Understanding the new requirements and the need for hardware security modules
Executive summary

The European Union’s Electronic Identification and Trust Services (eIDAS) Regulation was developed to help establish a single European market for secure electronic commerce. For organisations that handle online transactions with European citizens, the Regulation will present significant opportunities, but it will also create new requirements. This white paper offers a detailed look at the eIDAS Regulation and its implications for organisations. The paper looks specifically at the impact the Regulation will have on companies that provide identification, signing and authentication technologies and services. In addition, the paper examines the role hardware security modules (HSMs) play in complying with the Regulation, and it also describes how Thales e-Security supports organisations looking to address eIDAS requirements.
Introduction to the eIDAS Regulation

1.1. BACKGROUND

eIDAS is a European Regulation that establishes standards for electronic identities, authentication and signatures. The goal of the Regulation is to encourage the creation of a single European market for secure electronic commerce. By assuring security across the EU, the Regulation is helping to accelerate the digitalisation of services and systems in organisations.

eIDAS is a short-hand name for an EU Regulation (Reg.910/2014/EU), which was enacted in July 2014 and took effect in July 2016. The full name is “Regulation of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC”. The text for the Regulation can be found at the following URL:


(For a lighter look at the impact of eIDAS, view the YouTube video at the following URL:

https://www.youtube.com/watch?v=sszErHIwoDCU &feature=youtu.be.)

The eIDAS Regulation replaces the earlier 1999 EU Directive (Dir.1999/93/EC) on electronic signatures, and as a result national implementations of the Directive are being repealed. Rather than a Directive, eIDAS is enforced as a common Regulation, with a single set of rules that is applicable to all EU member states.

The eIDAS Regulation applies to government bodies and businesses that provide online services to European citizens, and that recognise or use identities, authentication, or signatures.

eIDAS requires that government and public commercial services recognise standard signature formats and pan-European identities. This applies to services associated with tax statements, insurance contracts, banking agreements, business-to-business electronic invoicing and pharmaceutical records. It also applies to commercial services that require an EU identity, for example, so-called “know your customer” services in banking. In addition, any trust services associated with these activities will be regulated by eIDAS.

Figure 1: A single European market for trust services
1.2. eIDAS ELEMENTS

There are two key aspects to the eIDAS Regulation. The first part covers the eIDAS identity services for electronic identification of an individual and provides mutual recognition of electronic identification schemes (see Electronic identification below). The second part covers the requirements for eIDAS trust services, including services relating to electronic signatures, time-stamping, web site authentication and registered electronic delivery.

Much of the Regulation covers requirements relating to electronic signatures, based on the earlier Directive. Three elements of an electronic signature are regulated under eIDAS:

1. The electronic signature format, which defines the structure for encoding a cryptographic signature within a particular document structure (for example, PDF, XML or binary). See Standards for electronic signatures and seals for more details.

2. The operation of a trust service provider (TSP) that provides security information (for example, a public key certificate) to support a trust service, such as the creation of an electronic signature. See Trust service providers (TSPs) for more details.

3. The cryptographic signature creation device (for example, a smart card or HSM), which is used to create the cryptographic element of a signature. For more on using HSMs as signature creation devices, see eIDAS legal requirements, standards and Thales HSM products.

For trust services other than electronic signatures which were introduced in eIDAS, the legal requirements concentrate on the rules regarding the operation of the TSP.
eIDAS introduces two concepts that are of particular relevance to the use of HSMs:

- **Electronic seals.** An electronic signature created by an individual can be a legal equivalent of a handwritten signature. However, electronic signatures don’t cover the case in which a document needs to be protected by a digital signature on behalf of an organisation to assure its authenticity. eIDAS introduces a new legal concept called an electronic seal. This is equivalent to an electronic signature but is issued on behalf of an organisation rather than an individual and doesn’t have the same legal significance.

- **Remote signing.** eIDAS allows the use of remote signing services that manage keys on behalf of the service’s users. With local signing, the signature is created using keys held on the user’s device. Remote signing represents an alternative approach to creating electronic signatures, offering a mechanism for remotely managing signature creation. With remote signing, signing keys are held on a service provider’s HSM. With this approach, the need for users to handle their own keys is eliminated. The use of remote signing is growing and having a significant impact on the market.

The eIDAS requirements are specified through four levels:

1. The Regulation, which defines the basic requirements that will be adopted across the EU, overriding any existing national regulation.
2. The standards, which have been recommended by the industry as a practical way of meeting the Regulation’s requirements.
3. EU implementing acts, which either mandate or recommend the use of these standards. Recently, five implementing acts have been published (see Annex C: References). These acts cover electronic identity interoperability and assurance levels, lists of qualified TSPs, signature formats and signature and seal creation devices.
4. National rules that may extend or adapt non-mandatory standards to meet a nation’s perspective.

---

**THALES: COMMITTED TO SUPPORTING CUSTOMERS ADAPTING TO eIDAS**

The eIDAS Regulation will provide opportunities for Thales customers and partners, but it will also require that organisations prepare for the necessary certifications and audits. Thales is committed to helping make it as straightforward as possible for customers to adapt to this new standard. Toward that end, Thales has been actively engaged with a number of governing bodies, including national security authorities and EU regulatory bodies, helping to ensure that the eIDAS Regulation features appropriate standards for the use of HSMs.

The company’s staff members have participated in the development of standards for remote signing, sealing and signing for TSPs, time stamping and more. Thales is participating in a number of outreach activities, including workshops and conferences, to help organisations that are adapting to the Regulation.

Thales is also working to align its solutions with these standards. Thales delivers nShield, a family of general purpose HSMs that can support the fastest cryptographic algorithms and safeguard high volumes of sensitive digital transactions. These HSMs can address a number of critical eIDAS elements:

- Signing certificates, time stamps and other objects issued by TSPs
- Remote document signing
- Local document sealing

In addition, a number of Thales partners have delivered remote signing solutions that use nShield as a root of trust to manage encryption and signing keys. These partner solutions have gained broad acceptance in a number of European countries.

---

Figure 2: Thales eIDAS ecosystem
1.3. AN EXAMPLE OF THE eIDAS REGULATION IN USE

Figure 3 provides an illustration of how the electronic identity services and trust services of the Regulation might be used together. In this example, an Austrian called Max uses an electronic identity provided by his national identity provider to log into a banking application that needs to verify his identity. This identity can then later be used to electronically sign a document supported by a qualified TSP.

1.4. THE IMPORTANCE OF HSMs

HSMs, such as nShield HSMs from Thales, play an important role in securing services that come under the eIDAS Regulation. HSMs have traditionally been used for public key certification services, and they can also be used for the electronic seals and remote signing services introduced by the Regulation. With remote signing, an HSM holds the signing keys and creates signatures remotely on behalf of the user. HSMs address a number of critical elements of eIDAS:

- Signing certificates, time stamps and other objects issued by TSPs
- Remote document signing
- Local document sealing

To be accepted under eIDAS, it is generally required that HSMs are certified under the internationally recognised Common Criteria standard. Also many non-EU governments now require compliance with Common Criteria.

nShield HSMs have a Common Criteria certification that is recognised under the eIDAS Regulation. This certification for nShield HSMs not only facilitates eIDAS conformance, but also benefits customers or partners requiring HSMs with robust security, no matter which part of the world they operate in.
Several EU nations provide access to government services using national forms of electronic identity. Currently, however, it isn’t possible for a citizen of one member state to identify themselves to a service based in another member state, which runs against the EU principle of free movement of EU citizens. The eIDAS Regulation aims to provide a legislative framework for mutual recognition of identification schemes across the EU. A national electronic identity scheme in one member state must be recognised by other member states with equivalent electronic identity schemes. A citizen’s electronic identity is passed from one member state to another in a signed assertion.

These requirements will apply to government services, such as health care or tax registration, and any business service that uses official government-issued identities, such as new bank account registrations (given the know-your-customer requirements in place) or an EU-wide car-hire service.

Given that governments are responsible for the identification of a natural person, identification is at least partially a public sector responsibility rather than a commercial trust service. Therefore, the Regulation is not intended to provide harmonisation of electronic identity standards (for instance there is no EU-wide database), but rather to provide the required cross-border recognition.

STORK (Secure identity acRos boRders linKed) is a European project for identity standards. However, without a legal foundation, the operational adoption of STORK has been limited. eIDAS establishes a legal framework that builds on the technical features of cross-border electronic identity schemes such as STORK.

eIDAS identification schemes have three assurance levels: low, substantial and high. One member state must accept equivalent assurance schemes from other member states. For example, Belgium and Estonia can mutually recognise each other’s identity schemes. As a result, a citizen in Belgium could access an Estonian government service that requires high assurance identity verification, such as using their smart card to establish their citizen ID.

The requirements for each level of assurance are detailed in the implementing act, 2015/1502. Requirements for establishing interoperability between different national schemes were published in 2015/1501 (see Annex C: References).
3

Trust service providers (TSPs)

3.1. TRUST SERVICES

Under eIDAS, a TSP is defined as a provider of trust services to the open community. This includes trust services that support these activities:

- Issuing certificates for signing, sealing and website identification, such as certificate authorities providing public key infrastructure (PKI) services
- Issuing digitally signed time stamps
- Long-term preservation of signed data, for example, ensuring the long-term validity of signatures on archived documents
- Electronic delivery services
- Signature and seal verification

The eIDAS Regulation also applies to cases in which other industry regulations require the use of trust services, for example the bio-pharmaceutical industry. Closed communities, such as bank-to-bank services, are outside the scope of the Regulation. However, the requirements of the EU’s revised Directive on Payment Services (PSD2) may lead many banks to use eIDAS trust services for customer-to-bank interactions.

The scope of the eIDAS Regulation’s rules around trust services is wider than the former Directive, which only covered provisioning of signing certificates. The eIDAS Regulation covers the use of certificates for website authentication and sealing, as well as such services as time stamp creation, signature validation, registered e-delivery and signature and seal preservation.

A TSP will be legally liable for any damage caused by its failure to comply with the Regulation’s security measures, so it’s expected that the TSP will need to employ and demonstrate best practices. This would include the use of an HSM. For TSPs that wish to demonstrate they meet practices approved by all EU governments, the Regulation introduces the concept of “qualified” elements. To be designated as qualified, trust services and cryptographic devices will need to meet more specific requirements. (See the EU qualified and non-qualified section for more information.)

Providers of compliant trust services can benefit from gaining access to the entire EU market. By using a TSP, a business has independent assurance that a transaction is secure. The assurance is provided by independent audit and government oversight. TSP customers can also be confident that any electronic document or transaction will have at least as much legal validity as a paper document with a hand-written signature.
3.2. THE USE OF TIME STAMPING

Time stamping, as specified in IETF RFC 3161, has an important role in ensuring that documents that are stored or archived can be validated many years after they were signed.

CAdES, PAdES and XAdES (see Standards for electronic signatures and seals) all include optional features to ensure the long-term validity of a digital signature using time stamping.

If the signature is to be verified more than a day or so after signing, evidence of the time of signing is required. This is because, if the certificate gets revoked, it is important to ascertain whether the revocation occurred before or after the signing. By time stamping the content before it is signed, organisations can readily establish the sequence of events. While there are other ways to establish evidence of the time of signing, such as via email and audit logs, a content time stamp is the most generally recognised approach.

For longer periods, perhaps over a year or more, public key certificates will expire and cryptographic algorithms will become easier to break. Therefore, on an occasional basis, organisations should apply additional time stamps to archived documents, using contemporary cryptography.

To support validation over the long term, the revocation information and certification authority certificates that were initially used to validate the signature need to be available. The AdES format includes a means of storing this information along with the signature.

3.3. STANDARDS FOR TSPs

ETSI, the European Telecommunications Standards Institute, has established a set of standards for the provision of public key certification and time-stamping services. These standards are not mandated under eIDAS, but they are recommended or required by the supervisory bodies of many EU countries.

These standards ensure that the functionality of a trust service is aligned with industry best practices and that the TSP’s information security management system follows the generally accepted principles defined by ISO 27001. Figure 4 shows the relationship between these standards.

ETSI established the following overarching standards:

- **EN 319 403.** This standard provides detailed requirements for organisations that assess or audit TSPs to ensure legal compliance. Depending on the type of service they provide, TSPs will be audited against one of the specific standards listed below.
- **EN 319 401.** This specifies general policy requirements for the operation and management of TSPs. The TSP may be a certificate issuer (qualified or otherwise), time-stamp issuer, signature verifier or an entity that uses electronic signatures or seals.
Other policy specifications refine and extend these requirements to specific types of TSPs as follows:

- **EN 319 411-1.** This specification defines the policy and security requirements that are common to TSPs issuing either qualified or non-qualified certificates, such as certificate authorities (CAs) and time-stamping authorities. (See the EU qualified and non-qualified section for more information.) It references EN 319 401 for generic requirements and EN 319 412 for certificate format requirements. The standard replaces TS 102 042 and is aligned with the CA/Browser Forum requirements.

- **EN 319 411-2.** This standard defines the policy and security requirements for TSPs issuing qualified certificates in the EU, as specified in the eIDAS Regulation. It references EN 319 411-1 for the majority of the requirements and replaces TS 101 456.

- **EN 319 412.** This standard profiles the use of X.509 certificate formats for individuals, legal entities, website certificates and qualified certificates.

- **EN 319 421.** This covers the policy and security requirements relating to the operation and management of TSPs that issue both qualified and non-qualified time stamps. Such time stamps can be used in support of electronic signatures or for any application that needs to prove a document existed before a particular time.

- **EN 319 422.** This standard covers the use of RFC 3161 for time stamping.

These standards build on, and align with, internationally recognised profiles and standards for PKI services, such as those adopted by the CA/Browser Forum, the banking industry and the SAFE BioPharma Association. Standards for registered electronic delivery are still in the early stages. There is an existing standard for registered electronic mail (ETSI TS 102 640) that will provide the basis for registered electronic delivery.

Signature preservation services are also being developed. Future standards in this area may take into account requirements for archiving documents in general, as well as archiving document signatures as required by the Regulation.
3.4. AUDITING OF TSPs

Given the complexity of the interconnected components required to deliver a trust service, as well as the need to consider physical, operational and technical security, trust services must be regularly audited in their entirety in order to ensure their trustworthiness.

To be designated as qualified, a TSP must be recognised by their national supervisory scheme. Each EU member state publishes a list of qualified TSPs. (See the section titled Trusted lists for qualified TSPs below.) Standards have been published for auditing TSPs. (More information on the standards is covered in Annex B: Standards roadmap.) These standards have been adopted by a number of nations, even though there currently isn’t any implementing act requiring their adoption.

Article 20.1 of the eIDAS Regulation requires that qualified TSPs are audited bi-annually. (For more information, see the EU qualified and non-qualified section below.) Auditing is also a mandatory part of the CA/Browser Forum baseline requirements (see https://cabforum.org/baseline-requirements-documents/), which necessitates an annual audit.

3.5. TRUSTED LISTS FOR QUALIFIED TSPs

Each EU member state is responsible for publishing a list of those TSPs that are recognised as qualified by their national supervisory scheme, either under the eIDAS Regulation or the earlier Directive. (See Auditing of TSPs above.) A standard structure for this trusted list has been defined (TS 119 612) and is applied to eIDAS by implementing act 2015/1505. This standard structure includes an entry for each trust service together with the TSP’s certificate.

The EU publishes an official list that compiles links to every member state’s trusted list. (This list is available at the following URL: https://ec.europa.eu/information_society/policy/esignature/trusted-list/.) However, many application providers are reluctant to incorporate the trusted lists from each member state into their applications, given the complexity and size of these lists. There are currently 1400 entries distributed across 31 national lists, and changes can occur every three days. Currently, Adobe supports trusted lists, as do several providers of custom solutions for government agencies. It is not clear whether other major providers will follow suit.

Trusted lists can be checked on a case-by-case basis using the official EU list. An unofficial tool for browsing the compiled list is available at the following URL: http://eutsl.3xasecurity.com/tools/ (available courtesy of 3XA Security of Sweden).
3.6. EU QUALIFIED AND NON-QUALIFIED

Within the context of the eIDAS Regulation, qualified simply means that a signature creation device (such as a smart card or HSM) or a TSP has government approval for its alignment with specific requirements of the Regulation. Qualified status is also applied to the following:

- Certificates, which must be issued by a qualified TSP
- Time stamps, which must be issued by a qualified TSP
- Electronic signatures and seals, which require a qualified signing device and a qualified certificate

Being qualified is important when selling to governments. In addition, for a number of member states, being qualified adds more legal certainty to electronic signatures. The eIDAS Regulation also seeks to instil consumer confidence, so qualified trust services will be identifiable by a trust mark (see figure 5).

However, if a signing device or TSP is not qualified, that doesn’t necessarily mean that it should be viewed as less trustworthy. Other schemes also aim to ensure trustworthiness. For example, the CA/Browser Forum provides a similar international TSP approval scheme that is accepted by all the major application providers, in spite of being “non-qualified” in relation to the eIDAS Regulation.

Figure 5: EU trust mark for qualified TSPs
4.1. ADOPTION OF ELECTRONIC SIGNATURES

The adoption of electronic signatures has enabled rapid growth in electronic transactions and communications for both government and commercial applications. Figure 6 demonstrates the rapid growth of electronic signatures predicted by Forrester. The analyst firm forecasts that 2017, 700M transactions will use electronic signatures. Forrester interviewed nine leading electronic signature solution providers, who reported combined annual growth of 53% since 2012.

![Figure 6: Adoption of electronic signatures](image-url)

Source: Forrester interviews with 9 leading electronic signature solution providers
*Forrester projection
4.2. FORMS OF ELECTRONIC SIGNATURES

The intent of an electronic signature is typically made clear in the document being signed. Electronic signatures perform two functions:

- Authenticating the signer
- Ensuring a document hasn’t been modified after it’s been signed

An electronic signature can come in many forms, including email signatures, scanned signatures and even click-throughs on web pages or mobile devices. In addition, the eIDAS Regulation defines two types of signatures: advanced electronic signatures and qualified electronic signatures.

An advanced electronic signature, typical of most PKI systems, must be:

- Uniquely linked to the signatory
- Capable of identifying the signatory
- Created in a way that ensures the signatory can maintain sole control
- Linked to the data it relates to in such a manner that any subsequent change to the data is detectable

A qualified electronic signature is an advanced electronic signature that is supported by the following components:

- A qualified signature creation device, such as a smart card or HSM, which is certified by Common Criteria and meets the requirements of the eIDAS Regulation
- A qualified public key certificate issued by a qualified TSP, which has been audited by an accredited organisation and found to address the requirements of the eIDAS Regulation

A qualified electronic signature is assumed to have at least the legal equivalence of a handwritten signature. A judge must determine the veracity of any other type of electronic signature.
4.3. ELECTRONIC SEALS

The eIDAS Regulation has introduced the concept of an electronic seal. A seal can use the same technology as an electronic signature but has a different legal meaning:

- The source of an electronic seal is generally assumed to be a legal entity or organisation, whereas an electronic signature comes from an individual.
- Seal creation need not be under the control of a single individual.
- Seals do not provide the same legal indication of intent by an individual, but they provide assurances as to the authenticity of information provided by the business.

Like electronic signatures, electronic seals can be advanced or qualified.

An electronic signature is specifically for legal signatures, while an electronic seal is concerned with authenticity and integrity. Sealing is likely to be relevant to business-to-business exchanges, such as order processing and invoicing, and business-to-consumer exchanges, such as issuing receipts.

Electronic seals are seen as a useful tool. However, given electronic seals are a new legal concept in many EU countries, this approach has yet to be widely implemented.

4.4. STANDARDS FOR ELECTRONIC SIGNATURES AND SEALS

To date, the standards make no technical distinction between electronic signatures and seals, and the same signing device (HSM or smart card) may be used to create a signature or seal. The technical standards generally refer to digital signatures as forms of advanced electronic signatures and advanced electronic seals. These standards are based on PKI technology and asymmetric cryptography.

eIDAS Article 27 and implementing decision 2015/1506 require that online government services recognise standard formats for advanced electronic signatures and seals, which are often collectively referred to as AdES (see Annex C: References to regulatory requirements).

AdES is based on existing standards, but includes two additional features to ensure that a signature can be validated long after a document was signed:

1. The signing certificate must be included in the calculation of the digital signature’s cryptographic value.
2. Optional time stamps may be added to the signature to assist in long-term validation.

Following are the standards for AdES formats:

- CAdES (EN 319 122): Cryptographic Message Syntax (CMS) Advanced Electronic Signature/Seal. This standard is based on a binary structure, and is applicable to any data format.
- XAdES (EN 319 132): XML Advanced Electronic Signature/Seal. XAdES digital signatures are most appropriate to XML data.
- PAdES (EN 319 142): Portable Document Format (PDF) Advanced Electronic Signature/Seal. Only for PDF documents, this standard covers details of how signatures should be presented and displayed, and integrated into a form submission process. The result is that PDF editing and rendering tools inherently support digital signing, whereas the use of CAdES and XAdES will generally require separate tools for editing and signing.
- ASiC (EN 319 162): Associated Signature Containers. This standard covers the application of signatures to a package of files, such as a ZIP folder.

ETSI EN 319 172 defines the general rules for creating and validating any AdES format. Businesses may use other formats. However, when government services are involved, or other regulations are in place that mandate the use of advanced electronic signatures, it is expected that the AdES formats will be required.
Remote signing

5.1. THE MOVE FROM SMART CARDS TO REMOTE SIGNING

Prior to the eIDAS Regulation, administering digital signatures required that users present a smart card to a signing service provider, with the smart card providing both proof of identity and signing functionality. For example, a bank employee might present their smart card to provide proof of their identity, and use it to generate a signature for a document that they present to a tax collection agency.

Managing smart cards can be costly and unwieldy, particularly for organisations that may have to support millions of users. Cards are frequently lost and have to be replaced, and if a new encryption standard is required, every card has to be replaced. As a result, the adoption of smart cards for electronic signing is low in the EU.

The eIDAS Regulation introduces an important alternative to smart cards by enabling TSPs to hold keys on behalf of their users. This is known as remote signing. Instead of signing with smart cards, users can work with a remote signing service that employs a certified HSM. Through remote signing, users can safely enter their credentials and sign documents using a phone, browser or other device.

HSMs support remote signing services by executing these tasks:

- Securely encrypting credentials for users
- Creating and storing a signing key for each user
- Ensuring that a document can only be signed with an authenticated user’s signing key

Moving forward, the predominant approach for remote signing will be through mobile devices and HSMs. Figure 6 shows how the adoption of mobile devices for identification has taken off in Austria, while the use of smart cards has stagnated. This dramatic market shift is also happening in other countries across Europe.

Austria: Active e-cards and mobile eID

Figure 7: Use of mobile devices (red line) compared to smart cards (blue line)

Source: Presentation on The Austrian mobile ID at the European Telecommunications Standards Institute (ETSI) Security Week; Sophia-Antipolis June 2015
5.2. REQUIREMENTS FOR REMOTE SIGNING

With remote signing, the user creates an electronic signature through a cloud-based service. Users’ signing keys will be held within an HSM operated by a TSP. Users will typically activate their keys through their mobile devices.

The eIDAS Regulation introduces legislation to ensure the trustworthiness of remote signing services, which depends on four elements:

1. The HSM that holds the user’s signing key.
2. Signature activation. This is the process of authentication and key activation. It is important to ensure that this functionality is under the user’s sole control at all times. The security of signature activation depends on functionality that is either provided by an external application or by the HSM. In the eIDAS Regulation, these two options are referred to as level 1 and level 2. (See Standards for remote signing for more information.)
3. The security of the user’s personal device. Personal devices such as smart phones should be protected against malicious software and have controlled access, for example, by using a PIN. If the smart phone is used to hold an authentication key or biometric information, some trust element may be necessary. However, it may not be possible to mandate that every user have a secure smart phone, so some compromises may be required.
4. The TSP that operates the remote signing service, probably as part of a wider TSP service. Regular audits are conducted to ensure the trustworthiness of the TSP. These audits look at the security of the whole system, including physical and operational measures, and the TSP’s ability to meet the functional requirements expected of the remote signing service.

Three of the four elements above are provisioned through two requirements within the Regulation:

- Requirements for the signing device to be certified. This covers both the requirements for the HSM [see Annex C References to regulatory requirements] and any extensions to the functionality for remote signature activation (see Remote signing and eIDAS legal requirements, standards and Thales HSM products).
- Requirements for the TSP to be audited (see Auditing of TSPs).

While the security of the user’s personal device isn’t directly addressed by the Regulation, this aspect will need to be considered within the context of both the certification of the signing device and audit of the TSP. Figure 8 illustrates a potential approach to remote signing using an HSM.

Figure 8: Remote signing
5.3. STANDARDS FOR REMOTE SIGNING

A draft standard, prEN 419 241-1, has been published for review by EU member nations. This draft builds on the published standard, TS 419 241. prEN 419 241-1 identifies two levels of “sole control assurance.”

Level 1 relies on the server signing application to ensure that the appropriate signing key is selected. The functionality supporting signature activation and assuring sole control is implemented as part of the server signing application, as illustrated in figure 9. This can use any suitably certified HSM, for example one aligned with standards like EN 419 221-5 (see eIDAS legal requirements, standards and Thales HSM products).
Level 2 requires that, in order to ensure sole control, signature activation must be implemented by code in the HSM. This code is certified to the same security level as the general cryptographic functions of the HSM. The signature activation data is passed in protected form from the signer’s device into the HSM to ensure that the user’s signing keys can’t be abused, even if the TSP’s server signing application was compromised.

Figure 9 illustrates the role of the standards for ensuring sole control in a level 2 solution. For level 2, a specific Common Criteria Protection Profile is being defined and will be published for review, as draft prEN 419 241-2. This rule is expected to be recognised late in 2017 or in 2018. This requires that the code evaluated under EN 419 241-2 operates within a general purpose HSM conforming to EN 419 221-5 (see eIDAS legal requirements, standards and Thales HSM products).

The eIDAS legal requirement for remote signing is currently ambiguous. The eIDAS implementing decision for qualified signature and seal creation devices, reference EU 2016/650, calls for security that is comparable with a certified smart card device until specific standards for remote signing have been recognised by the commission. For the moment, many countries are opting for a level 1 approach. Once there is a recognised Common Criteria Protection Profile, such as prEN 419 241-2, it is expected that the implementing decision will be changed to reference this standard.

The absence of recognised standards is not stopping the adoption of remote signing. Thales partners are already delivering remote signing solutions within the eIDAS framework. By using the nShield architecture, these partners can provide customers with a clear migration path to standards-based solutions that are recognised throughout the EU.
6.1. THE NEED FOR HSMs

A TSP must be able to demonstrate adherence to best practices. This means they must generally comply with the requirements of the Regulation, which may entail using an eIDAS-compliant HSM. HSMs are essential to ensure the security of keys used by TSPs. With the introduction of electronic seals (see Electronic seals, above), HSMs can be used instead of smart cards. eIDAS also allows TSPs to hold the signing key on behalf of their users in a shared HSM to support remote signing (see Remote signing, above).

Generally, there are three scenarios that require the use of an HSM:

- **TSPs signing certificates, time stamps and other objects.** Certificates and time stamps issued by a TSP must be signed using an HSM. Similarly, revocation information, such as OCSP and CRL, must be signed using an HSM. Other TSPs, such as those for electronic delivery, signature validation or long-term signature preservation, will also have objects that need to be signed and so will require the use of an HSM.

- **Remote document signing.** The Regulation allows a user’s signing key to be held centrally by a qualified TSP on behalf of the user, to allow documents to be signed remotely. Although not yet formalised, it is recognised that the TSP must hold the signing key within an HSM.

- **Local document sealing.** The Regulation recognises a particular form of signature that represents an organisation, called an electronic seal (see Electronic seals above). The signing key for a seal is held in a device that is not under the control of a single individual but is the responsibility of the organisation being represented. Seals are often used to protect information produced by a trusted process initiated on a computer within the organisation’s data centre.

6.2. COMMON CRITERIA COMPARED TO FIPS

Common Criteria is a general framework for certifying security related products, including HSMs. The framework’s adoption has mainly been driven by European governments, who by policy will make procurement decisions in accordance with Common Criteria standards—rather than the Federal Information Processing Standard (FIPS), which was established by the US government.

Standards and regulations adopted by European governments will have an impact on European industry, international companies that want to sell in the EU and non-EU governments that tend to follow EU direction, for example, southern Mediterranean and South American countries. Importantly, Common Criteria is likely to be adopted by the European Commission to provide a practical framework for certifying secure devices like HSMs.

Both EU and non-EU governments increasingly require compliance with Common Criteria EAL4+. Because the eIDAS scheme for HSM certification is based on Common Criteria, this certification will facilitate eIDAS conformance and it will benefit customers or partners requiring HSMs with assured security, no matter which part of the world they operate in.

The US Federal Government is using Common Criteria processes, for instance within the National Information Assurance Partnership (NIAP), a partnership of US government suppliers. In certain regions, for example South America, mistrust in FIPS has encouraged the adoption of Common Criteria standards. Delays in delivering updates to the FIPS HSM standard may further encourage the uptake of Common Criteria.

The following sections discuss the specific eIDAS standards for HSMs and other cryptographic devices such as smart cards.


6.3. eIDAS LEGAL REQUIREMENTS, STANDARDS, AND THALES HSM PRODUCTS

As mentioned above, to be compliant with the eIDAS Regulation and recognised as a qualified signature creation device (known as a secure signature creation device under the Directive), HSMs must be Common Criteria certified. The current nShield models are certified to Common Criteria EAL4+, which is the level generally accepted for government use. Details of the certification can be obtained through the Common Criteria website at the following URL: http://www.commoncriteriaportal.org/products/, under “Products for Digital Signatures”.

The nShield certification is recognised as conforming to the Directive 1999/93. Based on this, compliance with the eIDAS Regulation is recognised through Article 51 (transitional measures). As a result, the current nShield HSMs are also eIDAS conformant. For more information, visit the following URL:


Looking forward to future nShield HSMs, Thales has been proactive in the development of Common Criteria-based standards specifically for eIDAS. The company’s work with WG17 and various EU Commission bodies brings Thales staff into contact with many government agencies and TSPs. Certifying a trust service will be even more straightforward if an organisation uses HSMs certified to EN 419 221-5 and related standards for remote signing.

Part 5 of the EN 419 221 Protection Profile, entitled “Cryptographic Module for Trust Services” is undergoing final stages of review and is expected to be formally approved early in 2017. Thales expects to certify its nShield HSMs to this standard shortly afterwards.

6.4. BRINGING IT TOGETHER

Earlier we looked at three use cases that required HSMs. This section examines the standards required for those use cases.

1. TSPs signing certificates, time stamps and other objects
   - A Common Criteria certified HSM is preferred but many countries accept a FIPS certified HSM. (France requires Common Criteria-certified HSMs that are recognised under their national rules.)
   - The HSM doesn’t have to be a qualified signature and seal creation device.
   - HSM that conforms to EN 419 221-5 will meet a TSP’s HSM requirements under the above EN 319 standards.

2. Remote document signing
   - Regulatory requirements are yet to be agreed across the EU, although some nations have established national requirements. Current expectations are as follows:
     - For the present, the TS 419 241 standard is being used. In a number of countries, certification against TS 419 241 is being achieved by a non-Common Criteria certification process, such as that provided by A-SiT.
     - Once EN 419 241 is approved, which may happen by the end of 2017, it is expected that new systems will follow this standard. This requires:
       i. Using an HSM certified under Common Criteria to EN 419 221-5.
       ii. Using code running within the HSM protected environment (for example, using CodeSafe) that has been certified under Common Criteria to EN 419 241-2.
       iii. The overall server signing system conforms to EN 419 241-1, and has been verified as part of the TSP audit.
   - The HSM must be a qualified signature and seal creation device for remote signing.

3. Local document sealing
   - Local document signing is covered by use case one above.
   - Currently the only recognised certification is EN 419 211 (which is a protection profile based on smart cards) or a device already recognised under the Directive.
   - The intention is that EN 419 221-5 will be recognised for local sealing.

As described above (in eIDAS legal requirements, standards and Thales HSM products), nShield products have the certifications required for use under eIDAS. These products provide the flexibility and scalability to enhance performance and secure the digital assets used in just about any government or business service, whether it’s procurement management, health care, banking, national ID or invoicing.

Clearly, the user will experience the service, not the HSM. Because of the eIDAS Regulation, government agencies and businesses that deliver online services can trust their TSPs to deliver critical security services, so they can focus on delivering a high quality experience to their users.
By using nShield HSMs, TSPs can rely on their HSMs to deliver robust security of essential cryptographic operations and key management. Using an HSM that is certified to EN 419 221-5, or that is otherwise eIDAS certified, will make it much easier for the TSP to achieve compliance with the Regulation. Further, the organisation providing the online service will also be using its own nShield HSMs for sealing, SSL and so on.

As mentioned above (see The move from smart cards to remote signing), users are increasingly likely to authenticate through a mobile device rather than through a smart card and a laptop or desktop computer. However it’s important that users can authenticate through any device they choose, whether their laptop, tablet, smart phone or authentication token. In addition, organisations should give users the flexibility to go through any channel they prefer, whether it’s EMV/ CAP, VASCO, RSA, OATH, SAML assertion or digital certificate. The SafeSign product from Thales supports the necessary authentication between the user, the service and the HSM. The product also enables customers to adapt the level of security according to the user’s location and device, and the sensitivity of the service.

Today, organisations need to establish end-to-end communication security. For instance, the user’s authentication credentials should be transmitted through a secure tunnel to the HSM, ensuring they can never be accessed by the service itself. As discussed in the Remote signing section, the security of remote signing depends on the functionality that operates alongside or within the HSM. The CodeSafe trusted execution environment enables sensitive security software to be loaded and executed within the nShield HSM’s security boundary. CodeSafe applications are accessible through a secure channel, so that Thales’ partners can implement signature activation functionality and tunnel credentials securely through to the HSM.

SafeSign provides a high-level interface for many cryptographic operations, including signing and signature verification, certificate verification and revocation. In addition, the product supports:

- The following ETSI signature format standards: CAdES, XAdES, PAdES
- Remote signing services
- Thales products offer these advantages:
  - **Scalability.** A trust service might have to manage tens of thousands of keys, or even more. The nShield HSM provides scalable key management, offering capabilities for key creation, loading and backup.
  - **Secure logging.** Application-level secure logging is provided by SafeSign, while lower-level logging is supported by the nShield HSM.
  - **Time-stamp capabilities.** The time-stamp server or the time-stamp option pack can be used by services that need trusted time stamps.

![Figure 11: Thales solutions for signing and sealing](image)

Figure 11 takes another look at the earlier example, showing where nShield HSMs, together with SafeSign, can be used for signing and sealing.
Conclusions

This white paper has detailed how the eIDAS Regulation is enabling a single, secure EU market for government agencies and businesses that deliver online services. Thales is committed to helping its customers and partners in adapting to the eIDAS Regulation—and capitalising most fully on the Regulation’s advantages.

The standards being adopted under eIDAS serve to impose specific requirements on HSMs, while the introduction of new concepts, such as electronic seals and remote signing, has increased the role and importance of HSMs. Through their alignment with standards like Common Criteria, nShield HSMs will help TSPs, government agencies and businesses efficiently and effectively address eIDAS requirements for electronic identities, signing and other trust services.

Annex A: eIDAS schedule

July 2014 eIDAS Regulation came into force
Sept 2015 Implementation acts covering:
- Signature formats (see Standards for electronic signatures and seals)
- Electronic identity assurance levels (see Electronic identification)
- Electronic identity interoperability framework (see Electronic identification)
July 2016 Old 1999 EU Directive is invalidated
- All conflicting national rules are repealed and replaced
- Any reference to the 1999 Directive is treated as a reference to the eIDAS Regulation
- Start date for majority of technical requirements on eIDAS
- Start date for existing qualified TSPs to migrate to eIDAS audit
- Newly regulated qualified trust services (such as time stamping and remote signing) must be audited by this date
July 2017 A qualified TSP delivering a service that is currently regulated under the Directive must be audited by this date

Secondary legislation is required to provide regulations for conformance assessment bodies that certify signing devices. No dates have been set for this secondary legislation, however.

Qualified devices will be nominated by national authorities and published through the EU Commission.
Annex B: Standards roadmap

A list of all the standards relating to trust services and signatures are described in the ETSI publication TR 119 000. These standards are grouped together by a numbering scheme, as shown in figure 12.

Figure 12: Framework of eIDAS trust service related standards

Following are references to various standards:

- ETSI standards can be obtained through the ETSI standards search page at the following URL: http://www.etsi.org/standards-search
- CEN standards can be obtained through any European national standards organisation.

Specifications for eIDAS electronic identity services are not issued through the formal standards bodies but are published through a European group comprised of national experts. These specifications may be downloaded at the following URL: https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10
Annex C: References to regulatory requirements

- Trust services and electronic identity in the digital single market:

- Regulation (EU) No 910/2014 (eIDAS):

- Implementing acts supporting eIDAS:
  - Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (text with EEA relevance).
About the authors

Nick Pope, Principal Consultant, Thales
nick.pope@thales-esecurity.com
Nick has been involved with standards relating to Regulations and Directives since 1999. He is vice-chairman of ETSI ESI, a group concerned with eIDAS standards for electronic signature and trust infrastructures. He has edited a number of ETSI specifications on signature formats and trust service policies and is currently the lead of the ETSI specialist task force on electronic signatures and trust services. Within CEN TC 224 WG17, he is the ETSI liaison representative and UK principle expert, as well as attending on behalf of Thales.

Jonathan Allin, Product Manager, Thales
jonathan.allin@thales-esecurity.com
Jonathan is a product manager in Thales. He is responsible for nShield general purpose HSMs and their certifications.
About Thales e-Security
Thales e-Security + Vormetric have combined to form the leading global data protection and digital trust management company. Together, we enable companies to compete confidently and quickly by securing data at-rest, in-motion, and in-use to effectively deliver secure and compliant solutions with the highest levels of management, speed and trust across physical, virtual, and cloud environments. By deploying our leading solutions and services, targeted attacks are thwarted and sensitive data risk exposure is reduced with the least business disruption and at the lowest life cycle cost. Thales e-Security and Vormetric are part of Thales Group.