# Assessment of Standards related to eIDAS

## Recommendations to support the technical implementation of the eIDAS Regulation

NOVEMBER 2018

www.enisa.europa.eu

European Union Agency For Network and Information Security

# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Contact

For queries in relation to this paper, please use trust@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

## Contributors

Sylvie Lacroix, Olivier Delos

## Editors

Evgenia Nikolouzou (ENISA), Slawomir Gorniak (ENISA)

## Acknowledgements

The analysis in section 4.4.2 of this document was produced in collaboration with editors of the CEN EN 419 241-1 and CEN EN 419 241-2 standards.

### Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

### Copyright Notice

ISBN: 978-92-9204-273-8
DOI: 10.2824/50750

# Table of Contents

**Executive Summary** 5

**1. Introduction** 7

**1.1 Scope** 8

**1.2 Foreword** 9

**1.3 List of acronyms** 9

**2. The legislative framework** 10

**2.1 eIDAS – supervision versus certification** 10

**2.2 Commission Implementing Decision 2016/650** 12

**3. TYPE 2 QSCD certification: standards requirements** 13

**3.1 Introduction** 13

**3.2 Requirements of Annex II of the eIDAS Regulation** 13

3.2.1 Requirements on the cryptographic module 13
3.2.2 Requirements on the cryptographic module and the TSP 14
3.2.3 Requirements on the QTSP 14

**3.3 Requirements applicability and verification** 15

**4. Eligibility of PPs to support QSCD certification** 18

**4.1 Requirements** 18

**4.2 CID (EU) 2016/650 framework for security evaluation process (ISO/IEC 15408)** 18

**4.3 CEN EN 419 221-5** 19

4.3.1 SCOPE 19
4.3.2 DETAILS 19

**4.4 CEN EN 419 241-2** 19

4.4.1 SCOPE 19
4.4.2 DETAILS 20

**4.5 Other relevant standards** 25

4.5.1 CEN TS 419 221-6 (draft) 25
4.5.2 ETSI TS 119 431-1 (draft) 25
4.5.3 ETSI TS 119 431-2 (draft) 26

**4.6 Annex II requirements by the standards** 26

**5. Opinion** 28

**5.1 Criteria for QSCD certification versus supervision** 28

**5.2 Referencing** 29

6. Bibliography/References 30

6.1 References 30

Annex A: eIDAS and QSCD 31

A.1 Recitals 31

A.2 Articles 31

# Executive Summary

At the time of writing of Commission Implementing Decision 2016/650 there were no available standards for signing devices operated by a trust service provider in a secure environment that aim to meet the requirements in Regulation (EU) 910/2014 Annex II for qualified signature / seal creation devices. However, two major CEN standards (CEN EN 419 241-2 (*Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing dated 2018-05-11*) and CEN EN 419 221-5:2018 (*Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services*)) published by the CEN TC224 cover the following use cases relating to the identified gap:

- trust service providers managing signature creation data on behalf of the user to support the creation of qualified electronic signature / seals and
- trust service providers creating qualified electronic signature / seals on their own behalf.

This study seeks to present the scope of the QSCD certification as well as the scope of the QTSP supervision and to identify the way to combine respective elements therein in a way that the eIDAS Annex II requirements, specifying QSCD, are respected. In this context, this report seeks to support the case for standards CEN EN 419 241-2 (*Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing dated 2018-05-11*) and CEN EN 419 221-5:2018 (*Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services*) to become eligible to be referenced in an amended version of Commission Implementing Decision (EU) 2016/650.

CEN EN 419 221-5 may apply when the electronic signature creation data or electronic seal creation data is held in an entirely, but not necessarily exclusively, user-managed environment. When combined, the two protection profiles (PP) apply to a qualified trust service provider managing the electronic signature creation data or electronic seal creation data on behalf of a signatory or of a creator of a seal. However, the verification of assumptions made by the Protection Profiles (PPs) on the target of evaluation's environment need to be ensured. In the context of eIDAS, for a Qualified Trust Service Provider (QTSP), this is a task carried out by the supervisory body. Consequently a certified QSCD can only be officially recognised as such once the QTSP has been duly supervised to manage the QSCD according to requirements and assumptions on the environment provided in the PPs (and possibly as specified in complementary policy documents like ETSI TS 319 431-1). This requires that the supervisory body supervises the qualified trust service for which the QTSP is granted a qualified status as well as the QSCD management, starting with the verification that the QSCD is certified and then verifying any requirement on the environment which needs to be duly duly implemented by the QTSP.

- ➢ In this report it is also suggested that further work is carried out to compile a checklist with the functional objectives to be supervised (for the supervisory bodies) and a checklist with the related technical criteria to be used when an audit is carried out by CABs, issued from the PPs and related standards.

This report suggests that there is shared responsibility between the TSP managing the QSCD to work with appropriate TSP issuing certificates (CA), and on the CA to work with an appropriate TSP for the management of QSCD. For qualified devices management and qualified certificates issuance, the verification that such requirements are followed falls under supervision by competent supervisory bodies.

Explanations on the role of supervision (that is mandatory), and ideally a pointer to the checklist mentioned above to clearly identify the elements to be checked by the audit underlying the supervision process should be provided directly in the amended version of Commission Implementing Decision (EU) 2016/650. Alternatively, this information could be provided as a link toward a "to be issued" Implementing Act referred to by Article 29.

- Further guidance is needed to confirm whether it is possible to refer to technical criteria for the QSCD supervision process under Article 30 (dedicated to certification). Alternatively an Implementing Act could be issued pursuant to Article 29.2 of the eIDAS Regulation (in which case, the remaining question is how to bind both Implementing Acts).

Given that a certain amount of coordination among stakeholders is required to achieve a global trust level, it would be pertinent to provide a way to advertise the elements of supervision. Besides the official compilation of Member States notification on SSCDs and QSCDs, the trusted list of the country where QTSP operates might provide an indication when the QTSP manages a QSCD duly in accordance with eIDAS. Alternatively, the list of notified SSCDs and QSCDs compiled by the European Commission might also be used for this purpose. This would be important to inform the market and organisations that wish to implement qualified electronic seals or signatures conformant to eIDAS.

Finally, a transition period needs to be foreseen for the entry into force of the amended version of the Commission Implementing Decision (CID) so that stakeholders (devices builders) switch from an Art.30.3 (b) certification process to a process based on the standards newly referenced by the amended version of the CID. This is true even if most of the procedures of Art.30.3 (b) notified by EU MS to the European Commission are based on earlier versions of these standards.

# 1. Introduction

Regulation (EU) No 910/2014[1] (hereafter the eIDAS Regulation[2]), on electronic identification and trust services for electronic transactions in the internal market, stipulates the regulatory framework for electronic identification of natural and legal persons and for a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

By means of the instruments regulated in eIDAS it is possible to use these trust services as well as associated electronic documents as evidence in legal proceedings across the EU Member States contributing to their general usability within Member States and across borders. While the legal validity of trust services is warranted, Courts (or other adjudication bodies) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

Additionally, the eIDAS Regulation identifies trust in the online environment to leverage economic and social development. Standards for trust services need to be available to ensure solutions that are interoperable and provide coherent levels of trust. Whilst the eIDAS Regulation provides a common set of requirements, it does not necessarily identify how these requirements may be met following existing technology and organisational arrangements in place. Standards provide a generally accepted means to meet requirements with existing technology, whilst if necessary the market can develop alternative solutions as new technology emerges to further feed into the standardisation life cycle.

The eIDAS Regulation also lays down requirements for qualified electronic signature (respectively seal) creation devices (QSCD) to ensure the functionality of advanced electronic signatures (respectively seals). In the specific context of QSCD however, the security evaluation and certification process must be carried out in accordance with the list of standards established by means of the implementing act referred to in Article 30.3 of the eIDAS, i.e. CID EU 2016/650[3], unless there is no “applicable” standards mentioned in the implementing act, or when a referred security evaluation process is on-going.

Article 30.3 refers to the security evaluation process and standards for qualified electronic signature creation devices may be referred to in the implementing act referred to in Article 29 to provide presumption of compliance with the eIDAS requirements. The security evaluation process and the underlying technical criteria are tightly bound and the latter are de facto influenced by the security evaluation scheme. This applies to CID (EU) 2016/650, which currently covers the case where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment (here after referred to as **TYPE 1** device).

At the time of drafting the CID (EU) 2016/650, there were no available standards yet for signing devices operated by a trust service provider managing signature creation data on behalf of the user to support the creation of qualified electronic signature / seals (here after referred to as **TYPE 2** device). In a broader

[1] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[2] See Annex A of the present document for more details.
[3] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) 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.

context, there were no standards for remote signing devices either (i.e. where the signatory or the creator of a seal stores its key on a remote cryptographic module).

QSCD management concerns multiple stakeholders: the signatory or creator of a seal (here after both referred to as the signer), the device producer, the TSP managing the QSCD on behalf of the signer when applicable (that TSP must be a Qualified TSP – QTSP), the TSP offering the signature creation application when applicable and to some extent the TSP issuing certificates of the signer (or Certification Authority - CA). Consequently, QSCD security depends on each stakeholder in the signature workflow and the security evaluation process may potentially address several entities. For a TYPE 2 QSCD in particular, between the mandatory certification of the device and the signatory's environment falling outside the eIDAS certification requirement, the supervision of the QTSP managing the QSCD has an important role to play to ensure that the applicable requirements of the Regulation have been met (e.g. Art.19, Art.24.2, Art.26, Art.29/39, Annex II).

This study (see also figure 1 below for more details) seeks to present the **scope of the QSCD certification** as well as the **scope of the QTSP supervision** and to identify the way to combine respective elements therein in a way that the eIDAS Annex II requirements, specifying QSCD, are respected.

In the approach followed by MS and the European Commission the QSCD "management" part does not fall in the scope of the certification but the so-certified device may not be considered as QSCD unless "duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014". The sentence "*IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory/seal creator) by a QTSP that can be only considered as QSig/SealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014* " is referenced on TYPE 2 device certification information in the compilation of Member States notification on SSCDs. QSCDs are used for this purpose[4].

TYPE 2 QSCD related standards could be referenced in an updated version of CID 2016/650 to specify, directly or by reference the criteria enabling supervisory bodies to assess the *operation due by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.*

## 1.1 Scope

CEN technical committee TC 224 and working group WG17, has published or is about to publish new standards for the security assessment of qualified signature and seal creation devices, namely:

- CEN EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing dated 2018-05-11
- CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services.

The scope of this report is to analyse and assess eligibility of the above-mentioned standards as being suitable references in an amended version of CID (EU) 2016/650.

The analysis provided in this report also considers the way these standards need to be used (e.g. possible combination with other standards, certification scheme within which they fit, etc.). It is important to note that in this report **the terms qualified <u>seal or signature</u> creation devices are used invariably as there is no particular differentiation made in** Annex II referring to the qualified seal creation device. Indeed the eIDAS Regulation requires that the private key for signature must be "*with a high level of confidence under <u>sole</u>*

[4] See https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

*control"* and for seal "*under control*" of its owner. In eIDAS Annex II 1.(d) control on the signature creation data is exercised by the owner as to "*be reliably protected by the legitimate signatory against use by others*" and support both requirements. When the key is managed by a TSP the requirement on "sole control" or "control" is warranted by the TSP independently of, and in addition to the device features (and to a certain extent in collaboration with the CA issuing the certificate of the signer and/or any kind of identity provider that would act in the signer's authentication process). In other words, the nuances between signature and seal do not affect the QSCD itself but the TSP managing it; the level and criteria for certification of the device are the same for both qualified electronic signatures and qualified electronic seal creation devices. These criteria shall not be limited or reduced for either seal or signature devices, since in both cases, the signature/seal creation data must *be reliably protected by the legitimate signatory against use by others*.

Given that a certain amount of coordination between the stakeholders mentioned above and the supervisory and certification bodies is required to reach global trust level, it would be logical to **provide a way to advertise on the elements falling under supervision**. Besides the official compilation of Member States notification on SSCDs and QSCDs, the trusted list of the country where QTSP operates might provide an indication when the QTSP manages a QSCD duly in accordance with eIDAS. Alternatively the European Commission compiled list of notified SSCDs and QSCDs might also be used for this purpose.

## 1.2 Foreword

Unless specifically mentioned the text uses indifferently the term *signature* to address electronic seals or electronic signatures such as defined by the eIDAS Regulation, and the term *signer* to address signatory or creator of a seal. The acronym QSCD refers to qualified electronic seal creation devices or to qualified electronic signature creation devices.

## 1.3 List of acronyms

**AdES**: advanced electronic signatures
**CA**: certification authority
**CAB**: conformity assessment body
**PP**: protection profile
**QSCD**: qualified electronic signature (respectively seal) creation devices
**QTSP**: Qualified TSP
**SAM**: signature activation module
**SFR**: security functional requirement
**SSA**: server signing application
**ST**: security target
**SVD**: signature validation data
**ToE**: target of evaluation
**TSP**: trust service provider
**TW4S**: Trustworthy system supporting server signing (editor's note: i.e. TSP deploying the SSA and ToE)

# 2. The legislative framework

The analysis of the legal framework points to a series of key areas addressed in this report.

## 2.1 eIDAS – supervision versus certification

The eIDAS Regulation specifies QSCD and their certification in Articles 29, 30, 39 and Annex II. Further highlights are provided in four recitals. Related articles and recitals are mentioned in Annex A of the present document, but at this stage, it is important to point out that the security assessment of QSCD aims to certify that the device conforms to eIDAS Annex II. One of the requirements of Annex II is that managing QSCD on behalf of signers may only be done by a QTSP.

This fact, like any other requirement listed under Annex II, must be "covered" by the device certification (or at least a certified device may not be considered as QSCD unless "*duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014*"). This shows that the recognition of a QSCD, in the case of a trust service provider generating or managing signature creation data on behalf of the signer, will cover both the hardware and software features of the device as well as the management of the operational environment of the signature creation data. For the sake of simplicity, such hardware or software handling the signature creation data will be further referred to as to the "**cryptographic module**". The crypto module is an element of a QSCD.

**First key point: the QSCD certification, where the QSCD is managed on behalf of the signer, goes beyond the certification of the crypto module handling the signature creation data and it covers the operational environment as well.**

Managing a (Q)SCD or creating a (qualified) signature on behalf of signers are trust services for which the eIDAS Regulation does not specify a qualified level. In other words, only QTSPs that have been granted a qualified status pursuant to Article 21 of the eIDAS Regulation for one or more of the qualified trust services (QTS) specified in the eIDAS Regulation may generate or manage electronic creation data on behalf of the signer. As these TSPs are qualified, they must use trustworthy systems and products that meet the requirements of Article 24(2), in particular points e) and f). Additionally, these TSPs are subject to eIDAS Article 19. In particular:

- Article 24.2 point (e) on trustworthy systems: "use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them"
- Article 19.1 regarding risk based security due diligence stating in substance that the TSP shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.

Moreover, Recital 52 clarifies that "*remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory*".

These requirements may not all be covered by the QSCD certification; they are linked however, to elements that are covered by the certification (listed in Annex II of the eIDAS Regulation) provisions. It is commonly agreed that the due verification of such operation is a task for the supervisory body. In particular, Article 24.2 (e) is covered by the supervision of the QTSP. This requires that the supervisory body supervises not only the qualified trust service for which the QTSP has been granted a qualified status but also for its due operation of the QSCD in the context of Annex II.3.

Consequently, there is a double verification requirement with regard to the trustworthiness of the QSCD: at the certification as well as at the supervision level. Further on the boundaries of these two processes are discussed.

**Second key point: a QSCD managed by a QTSP is subject to certification and supervision (the latter controls that all devices used by the QTSP, including the QSCD, are "trustworthy").**

This supposes that the QTSP notifies the supervisory body about its managing of a (TYPE 2) QSCD on behalf of signers. Article 30.3 refers to the security evaluation process; standards for QSCD may be referred to in the implementing act stemming from Article 29 and concerning the presumption of compliance with the requirements of the eIDAS Regulation. The security evaluation process and the underlying technical criteria are tightly bound together and the latter are de facto induced by the security evaluation scheme. If the standardised protection profile (PP) underlying the certification process is referred to under Article 30 and the related updated CID, it is likely that the technical criteria underlying the supervision process related to QSCD management fall under provisions of Article 29.

**Third key point: it is important to assess which TYPE 2 QSCD related standard(s) need to be referred to in any amended version of CID 2016/650 and if there is a need to complete the amended Commission Implementation Decision with other standard(s), potentially referred to under Article 29 of the eIDAS Regulation.**

While recital 56 mentions that the QSCD should ensure the functionality of AdES (i.e. *a priori* all aspects of the signature creation, including the (sole) control on the signature creation data), it delimits the scope of the certification to specific elements pertaining to signature creation data, which is only one aspect of AdES. In addition, Annex II.2 has a specific requirement relating to data to be signed, that should be covered by the certification (like any element of this Annex II, as per Article 30). However, protection of data to be signed is different from signature creation data handling, hence limiting the certification of the device to the handling of the signature creation data. Finally, Recital 56 states that the scope of the device certification is limited to hardware and software – limitation that is literally not possible to observe since Annex II.3 and II.4 are totally beyond this scope and address the QTSP managing the device and the policies it implements.

**Fourth key point: Recital 56 is not to be strictly considered as a requirement because to a certain extent it may be deemed contradicting Article 30 and Annex II of the eIDAS Regulation; hence, it will not drive the present study.**

Creating advanced electronic signatures (AdES) requires the guarantee on the sole control on the signature creation data by the signatory or the control on the seal creation data by the creator of a seal (Articles 26 (c) and 36 (c)). When a TSP creates signatures on behalf of users, this is likely to be covered by sound implementation of Art.19. But this is not necessarily pro-actively verified by means of supervision because "signature creation" per se is not a qualified trust service (it is a "simple" trust service). In addition, even when the TSP is a QTSP operating a QSCD, the QSCD certification does not necessarily imply that AdES will be created (indeed, Annex II only talks about "electronic signatures" and not specifically "advanced" electronic signatures). The verification that "*the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others* » is warranted through QSCD certification. The difference between an electronic seal and an electronic signature does not affect the QSCD directly; it rather affects the entity managing the device that may apply stricter policies when a QSCD is used for the creation of electronic signatures. As this is not reflected in Annex II of the eIDAS Regulation, it remains out of scope of this report (it could be addressed by TSPs at the TSP policy level).

**Fifth key point: the QSCD must ensure that the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use or misuse by a third party, independently of the service (creation of seals or creation of signature) available.**

## 2.2 Commission Implementing Decision 2016/650

On 25 April 2016, the EU Commission released Commission Implementing Decision (EU) 2016/650 *laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) 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).

Key elements of this Commission Implementing Decision are the following:

1) The distinction between two types of qualified electronic signature creation devices:

- TYPE 1 (Art.1(1)): where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment, and
- TYPE 2 (Art.1(2)): where a qualified trust service provider manages the electronic signature creation data or electronic seal creation data on behalf of a signatory or of a creator of a seal.

2) The security assessment of TYPE 1 device is wholly covered by the CID 2016/650, as per eIDAS Article 30. i.e. the full **assessment scheme** is ruled **AND** this includes **the technical criteria** to be observed. CID 2016/650 indeed lists mandatory standards at three levels:

- level 1 - standards specifying the evaluation criteria for IT security (i.e. ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3)
- level 2 - standards specifying the methodology for IT security evaluation (i.e. ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation)
- level 3 - standards specifying protection profiles for secure signature creation device (i.e. EN 419 211 — Protection profiles for secure signature creation device, Parts 1 to 6, technical criteria to be observed by the device to conform to Annex II of eIDAS).

CID 2016/650 needs to be updated from time to time when standards for the security assessment of TYPE 2 devices are made available.

**Sixth key point: CID 2016/650 covers the assessment scheme and the technical criteria for QSCD TYPE 1. This may/should also be applicable to TYPE 2 devices.**

**Seventh key point: When CID 2016/650 is updated new standards for TYPE 1 devices need to be considered.**

# 3. TYPE 2 QSCD certification: standards requirements

## 3.1 Introduction

This report focuses on standards for TYPE 2 QSCD, i.e. devices in which a qualified trust service provider manages the QSCD on behalf of the signer.

The assumption made in this report is that the standards for TYPE 2 QSCD will be referred to in the update of CID 2016/650 and that this CID will not be drastically modified and in which the higher levels of the certification schemes will remain intact (see section 2.2). Only the protection profiles are discussed in this report. It follows that there is insufficient motivation to discuss how the first two levels that define "how" to assess a security product, would be different for TYPE 1 and TYPE 2 devices when protection profiles for TYPE 2 devices fitting in the ISO/IEC 15408 – ISO/IEC 18045 scheme are available (see key point 6 above).

The security assessment of QSCD for which a qualified trust service provider manages signature creation data on behalf of the signer to support the creation of qualified electronic signature, will necessarily go beyond the security assessment of a "device" (i.e. crypto module), see key point 1 above. The four points of Annex II apply to TYPE 2 QSCD and are covered in this reports. The question is to trace the line between "certification" and "security assessment" (that may fall under the supervision process).

Annex II requirements apply to:

- the cryptographic module only, or
- both the cryptographic module and the QTSP managing it, or
- only to the QTSP managing the device.

For both TYPE 1 and TYPE 2 devices, meeting some of the requirements of Annex II may need to be warranted "beyond" the device, i.e. up to the signer, or up to the signature creation application. This is out of scope of this study. The QSCD shall allow the connection of (or communication with) external elements in a secure way (e.g. secure path and trusted channel from the signer up to its signature creation data and from the signature creation application to the QSCD).

Appropriate standards for TYPE 2 QSCD need to support interface(s) between the cryptographic module, the heart of the device, and the QTSP environment, the cryptographic module and the owner of the signature creation data, the QTSP and the owner of the signature creation data. If more than one PP cover different aspects or components (e.g. the TSP and the heart of the device) they need to be complementary in such a way that an assumption made on a component that is in the environment of a target of evaluation (ToE) in a certain PP, will be stated under the form of a requirement in the particular PP addressing this component.

## 3.2 Requirements of Annex II of the eIDAS Regulation

### 3.2.1 Requirements on the cryptographic module

Items (a) to (c) of Annex II point 1 apply to the cryptographic module only. They apply to both types of devices (TYPE1 and TYPE2).

### 3.2.2 Requirements on the cryptographic module and the TSP

#### 3.2.2.1 Annex II.1.(d) - signature creation data protected by the legitimate signatory

The AdES requirement over electronic signature creation data that the signer can, with a high level of confidence, use under his (sole) control is reflected into Annex II.1 items (a) to (d) for the part of the signature creation data protection undertaken by the QSCD and the QTSP managing it.

Item (d) requiring that "*the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others*", is straightforward for devices under the signer's control (where it is generally admitted that a part of the job is under the responsibility of the signer, e.g. the device protects access to the key with a PIN code and it is up to the signer to keep this PIN secret); this level is more difficult to reach for devices managed by a third party on behalf of the signer. Point (3) of Annex II requiring that only QTSP may manage such device further supports this protection since only supervised (and thus audited) TSPs are allowed to manage QSCD.

Item (d), calls for the implementation of a trusted channel from the signer to her signature creation data. The QTSP must implement procedural means to ensure conformance (this is quoted in Recital 52 as a responsibility of remote electronic signature service providers). A QSCD must be certified against Annex II, and it needs to be covered by the certification process. The eIDAS Art.31.1 Designated Body that certifies QSCD will not only issue a certificate for the cryptographic module but will also seek to certify that the device allows for the protection of the signature creation data by the legitimate owner.

The procedures leading to key activation need to be certified for signer authentication and signature authorisation and it includes elements up to the signer's enrolment procedures. It is noted that the signer's environment is not part of the certification (nor the supervision) process.

#### 3.2.2.2 Annex II.2 QSCD shall not alter the data to be signed

The certification of the QSCD needs to attest that "*Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing*". The device is not the sole element in the signature creation chain to ensure this functionality, but there should be a "trusted channel" [5] from the QSCD all the way to the signer's interface. This goes beyond the scope of the cryptographic module and touches procedural and signature creation application aspects. Even if one does not certify the signature creation application, at least the end of the trusted channel on the QSCD's side needs to be certified.

### 3.2.3 Requirements on the QTSP

#### 3.2.3.1 Annex II.3 - Device managed by a QTSP

Annex II.3 "*Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider*" must be covered by the certification (as mentioned already, conformity of QSCD with Annex II shall be certified, – Annex II.3 appears thus as an element to certify). Obviously this verification occurs beyond the security assessment of the cryptographic module. It may be

[5] A communication path between the QSCD and the signer's interface that is logically distinct from other communication paths and provides ensured authentication of its end points and protection of the communicated data from modification and disclosure.

.

an element that makes a certification “pending” waiting for the QSCD being “*duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014”.*

As demonstrated in section 2.1, because QTSP must use trustworthy systems, the QSCD managed by a QTSP will be certified as any QSCD, and will also have to be checked by the supervisory body as a trustworthy one.

#### 3.2.3.2 Annex II.4 – policy requirements on key duplicates

Point 4 of Annex II is a requirement on the QTSP rather than on the device and is subject to the same considerations as Annex II.3 above. As indicated in key point 2 of section 2.1 some verifications from the supervisory bodies are expected to this regard.

## 3.3 Requirements applicability and verification

Because of Annex II points 3 and 4 being directly applicable to the QTSP, beyond the cryptographic module, the QTSP managing the QSCD is clearly in the scope of the certification process. This means that ALL requirements present in Annex II that concern both the cryptographic module and the TSP (over which the TSP has a role to play beyond the cryptographic module (i.e. Article 1 (d) and Article 2)) and they are covered by certification at the level of the cryptographic module AND at the level of the QTSP.

**There is a major difference between TYPE 1 and TYPE 2 devices: for TYPE 2 devices, there are additional elements to be verified (either certified or, which need to be formally evaluated before the certified QSCD can be considered “QSCD”). A certified cryptographic module is necessary for TYPE 2 devices but it is not sufficient to make a certified device be a QSCD.**

This is why the “*IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory/seal creator) by a QTSP that can be only considered as Qsig/SealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014* ” that is currently accompanying the TYPE 2 device certification information in the compilation of Member States notification on SSCDs and QSCDs **keeps its sense but the market needs criteria to evaluate this is actually met by the device they have chosen and by the QSTP managing it on their behalf.**

NOTE: A certain amount of requirements go beyond the cryptographic module *and* the QTSP (see figure 1 below). This is out of the scope of the certification (for TYPE 1 and TYPE 2 devices).

Considering Annex II.3, the entity “*generating or managing electronic signature creation data on behalf of the signatory”* must be a QTSP. Since operating a QSCD in the context of Annex II.3 is not a qualified trust service, this means that only QTSP that have been granted qualified status pursuant to Article 21, may generate or manage electronic creation data on behalf of the signatory.

The QTSP already benefits from audit and supervision for the provision of the QTS. In addition to that, the QTSP and its operations undertaken under Annex II.3, and potentially Annex II.4, is subject to the following QTSP requirements laid down in the eIDAS Regulation, which are not specific to the provision of a QTS:

- Article 24.2 (a) requires the TSP to notify the supervisory body of an intention to cease (all) its activities
- Article 24.2 (b)
- Article 24.2 (c)
- Article 24.2. (e): use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.
- Article 24.2 (f)
- Article 24.2 (g)

- Article 24.2 (h)
- Article 24.2 (i)
- Article 24.2 (j)
- Article 19.1: take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.
- Article 19.2
- Article 13
- Article 15

The above identified requirements, including those from Article 24.2 are independent of the QSCD certification (it is generally applicable to any system managed, service provided or process operated by QTSPs), but it is linked to elements that should be covered by the certification (listed in Annex II) when addressing a QSCD. Having these elements supervised with regard to the signature creations aspect will further sustain the certification objectives beyond the cryptographic module, through the TSP. Since 24.2. (e) is covered by the supervision there are potentially two processes, supervision and certification, applicable to the trustworthiness of the QSCD and beyond, on the way it is implemented (provided the supervisory body supervises not only the QTS for which the QTSP is qualified but also the QSCD management, see also key point 2 above). **The supervisory body shall check that the QSCD is a *trustworthy system and product that is "protected against modification" and the "technical security and reliability of the processes supported by it" is ensured by the QTSP*.**

The first part of the last sentence shall be satisfied by the fact that the QSCD is certified while the end of the last sentence is not a requirement on the cryptographic module, but on its management by the QTSP.

**This approach draws the line between the scope (boundaries) of the QSCD certification and the scope (boundaries) of the QTSP supervision of the operation of the certified device:**

1) The certification of a cryptographic module against a PP does not grant the QSCD status to the module when it is managed by a TSP – this status needs to be conditioned on the verification that the module is protected against modification and ensure the technical security and reliability of the processes supported by them.
2) There have to be technical criteria in place to assess that the module is protected against modification and that it ensures the technical security and reliability of the processes.

   It is important to be able to sort such criteria between criteria that fall under a certification process (on top of the cryptographic module certification) and criteria that fall under the supervision process (verified by the competent supervisory body and potentially audited by an eIDAS accredited CAB).

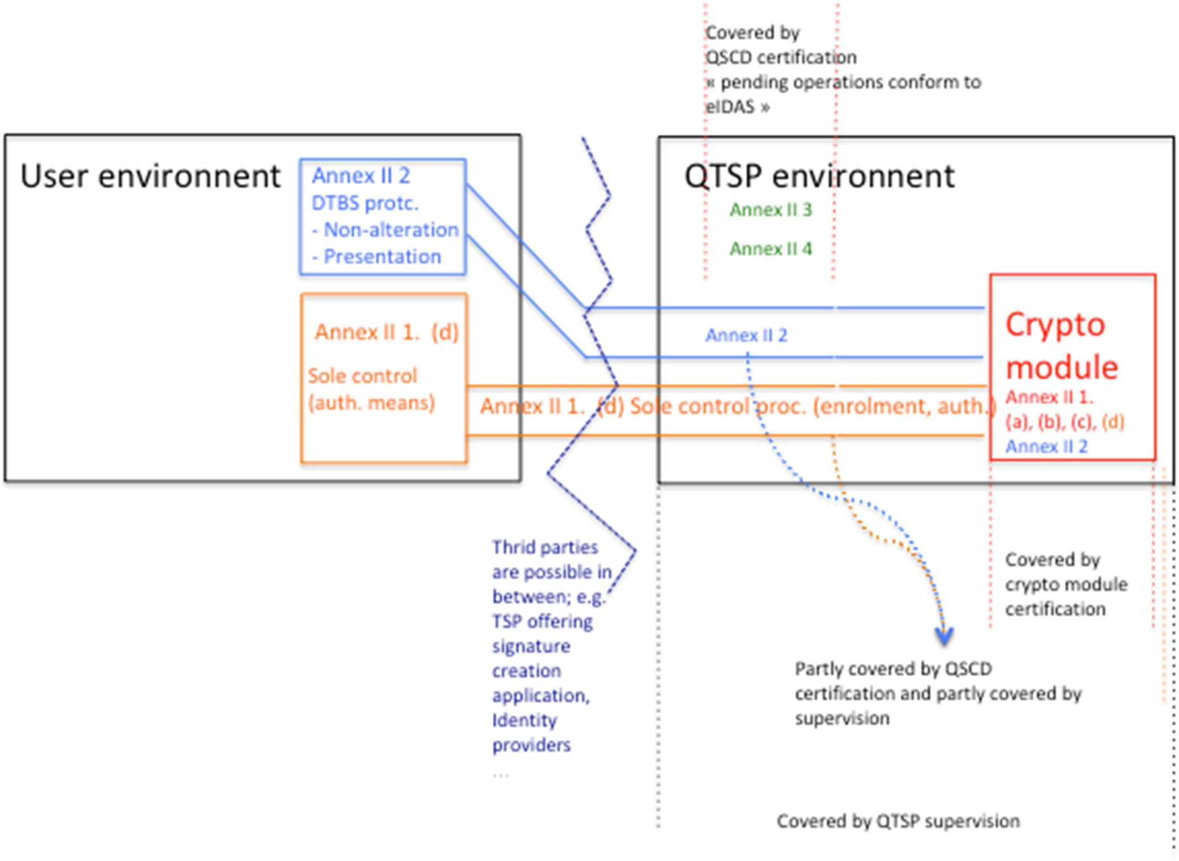

**Figure 1: Annex II requirements applicability for TYPE 2 devices**

# 4. Eligibility of PPs to support QSCD certification

## 4.1 Requirements

The eligibility of PPs to support QSCD certification is conditioned by the following requirements:

1) The PPs shall fit within the framework of Article 30.3 and 39.2 of the eIDAS Regulation for a potential amendment of CID 2016/650, in particular in the framework of ISO/IEC 15408-1:2009 (see key point 6).
2) The PPs, if applicable to TYPE 1 devices, shall cover all elements of Annex II applicable to TYPE 1 device (since once in the hands of the signatory / creator of the seal, the device will not be further controlled it needs to provide all functional requirements on its own) (see also key point 7).
3) The PPs and possibly other related standards shall support secure interfaces with other elements falling beyond the scope of certification but key to fully meet Annex II requirements (e.g. the signature creation application, the TSP issuing the certificates (CA), etc.) (see also key points 2 and 3).

In addition, where the QSCD is managed by a QTSP (TYPE 2 device):

4) The PPs shall cover the elements of Annex II, including beyond the cryptographic module, i.e. pertaining to the cryptographic module and the QTSP managing the device and to the QTSP alone, where possible, or there shall be other standards to be combined to the PPs, that are suitable with supervision goals (see also key point 2).

## 4.2 CID (EU) 2016/650 framework for security evaluation process (ISO/IEC 15408)

The two standards subject of the analysis in this report, CEN EN 419 221-5 and CEN EN 419 241-2 have been drafted within the ISO/IEC 15408 certification model referred to in CID (EU) 2016/650 for TYPE 1 devices.

The first two levels of the scheme referred to in CID (EU) 2016/650 for TYPE 1 devices should be applicable for these new PPs, meeting the requirements of key point 6 of section 2.2.

— ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3 as listed below:
    ○ ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. ISO, 2009.
    ○ ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security Part 2. ISO, 2008.
    ○ ISO/IEC 15408-3:2008 — Information technology — Security techniques — Evaluation criteria for IT security Part 3. ISO, 2008, and

— ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation, and

However, the ISO/IEC 15408/Common Criteria scheme has not been optimised for certification of procedural measures (as stated in the CC general model: “*Common Criteria is only suitable for assessing the correctness of IT countermeasures. Therefore the non-IT countermeasures (e.g. human security guards, procedures) are always in the Operational Environment”).* It means that some procedures might not be covered by a functional security requirement. In this case, they are not assessed by the evaluation process, but the “asset owner” (the QTSP managing the device in our case) needs to check that its environment conforms to the security objectives for the operational environment.

In other words, the certification of a device against a Common Criteria PP will ensure that the evaluated device meets a certain part of the Annex II requirements but this is not sufficient since the security objectives for the operational environment need also to be checked.

This is inherent to the Common Criteria certification scheme and in case of non-conformance, the device, even if certified for the IT security functional requirements, is not considered compliant to the PP.

**The assumptions made in a PP on the ToE's environment need to be verified under the authority of the supervisory body for QTSP in eIDAS[6].**

## 4.3 CEN EN 419 221-5

### 4.3.1 SCOPE

CEN EN 419 221-1 is a Protection Profile for cryptographic modules which are suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services, as identified by the (EU) No 910/2014 regulation (ref to eIDAS – a trustworthy system as in Article 24.2(e)).

As mentioned in CEN EN 419 221-5: "*Cryptographic Modules certified to this PP are intended to meet the security assurance requirements of Qualified Electronic Signature, and Electronic Seal, Creation Devices for use by trust service providers as specified in 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, although its use is not necessarily limited to such services*".

### 4.3.2 DETAILS

The PP covers the following elements of eIDAS Annex II:

- Referring to the Annex of CEN EN 419 221-5 one can be confident that the PP covers Annex II 1. (a) to (c).
- The PP addresses Annex II.1 (d) and II.2 for what regards the role of the cryptographic module.
- The PP does not address Annex II.1 (d) and II for what regards the part of the job in the hands of entity managing the device.
- The PP does not address Annex II.3 and Annex II.4.

Based on the above findings, one could perfectly use this PP for devices that are not managed by a TSP. A device certified against this PP may be used by users that wish to store they signing keys remotely, as it would be the case e.g. for a legal person implementing a QSCD to issue qualified seals.

Even if the PP is suitable for cryptographic modules used by QTSP, the PP can be used for devices other than TYPE 2 ones.

## 4.4 CEN EN 419 241-2

### 4.4.1 SCOPE

This part 2 of CEN EN 419 241 specifies a protection profile for a Signature Activation Module (**SAM**), which is the ToE and which is aimed to meet the requirements of a QSCD as specified in the eIDAS Regulation.

[6] Rationales: see sections 2.1 and 3.3.

It is part 2 of a series of two documents where part 1 specifies the general requirements of systems for server signing. It is a protection profile specifying detailed requirements for one particular component of the system, namely the SAM.

This PP is clearly dedicated to TYPE 2 devices as mentioned in the description of the ToE. It is for systems that offer remote digital signatures as a service.

Fitting in the philosophy of Common Criteria, the PP contains the requirements on the ToE's environment. In particular:

- ⇨ OE.ENV: *The TSP deploying the SSA and ToE (editor's note: i.e. a TW4S) shall be a qualified TSP according to article 3 (20) of Regulation (EU) No 910/2014 [eIDAS] and audited to be compliant with the requirements for TSP's given by [eIDAS]. The audit of the qualified TSP shall cover the security objectives for the operational environment specified in this clause.*

It follows that:

1. The QSCD certification requires the TSP to be a QTSP one "as a condition for the device to be considered as certified as a QSCD under eIDAS".
   - ⇨ The QTSP has been granted a qualified status and is supervised for the provision of a QTS. A certain amount of security criteria, such as the ones in ETSI EN 319 401, have been audited.
2. Security objectives for the QSCD operational environment provided in the PP shall be **audited.**
   - ⇨ the signature/seal creation device is certified as QSCD pending supervision of the QTSP to meet the corresponding PP requirements on the environment.
3. Assessment of security objectives against eIDAS Annex II logically falls under the responsibility of the supervisory body (through the QTSP audit and direct reference to the eIDAS Regulation).
   - ⇨ The QTSP is supervised (and likely audited) within the scope of the applicable eIDAS requirements for the operation of the tasks referred to in Annex II where it manages the electronic signature creation data or electronic seal creation data on behalf of a signatory or of a creator of a seal, while meeting the PP related assumptions and security objectives.

Note that CEN EN 419 241-1 on which the PP is built, further states that "*It is assumed that the Trust Service Provider (TSP) which provides signature creation services, operates the trustworthy system in an environment with a security policy which incorporates general physical, personnel, procedural and documentation security requirements for TSPs providing signature creation services. It is recommended to follow, e.g. ETSI EN 319 401 to ensure that the above requirements are met.*"

### 4.4.2 DETAILS

#### 4.4.2.1 Annex II.1 (a) to (c)

CEN EN 419 241-2 requires certification against CEN EN 419 221-5 for the cryptographic module. This will ensure that **Annex II.1 (a) to (c) are covered** at the heart of the device (see sections 4.3 and 4.6).

#### 4.4.2.2 Annex II.1 (d) and Annex II.2

The scope of CEN EN 419 241-2, the SAM, is mostly designed to implement **Annex II.1 (d) and Annex II.2**. For Annex II.1 (d), it shall cover signer authentication and signature authorisation and this encompasses elements up to the signer's enrolment procedures.

To this regard, the PP identifies the threat T.ENROLMENT_SIGNER_IMPERSONATION that "*may allow a potential incorrect signer authentication, leading to unauthorised signature operation on behalf of signer*". The threat describes the case in which the wrong user identifier (R.Signer) or wrong reference authentication data (R.Reference_Signer_Authentication_Data) being transferred from the registration authority (the RA) to the remote signing service including the QSCD.

At this stage, it is important to remember that a signer will undergo two similar “enrolment” procedures over the whole process made of the certificate issuance and the signature creation. The signer registers under the CA issuing the certificate and on the signing server of the TSP managing the TW4S. In this report the term RA relates to the TW4S service (unless otherwise specified), but the CA also has a registration authority component. When the same TSP issues the certificates and manages the TW4S it may have one single registration service.

Protection against this threat would enable (contribute to) compliance with eIDAS Annex II.1 (d) “*the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others*”. Indeed, if the objectives of the signing service for user identification are not met, then incorrect user identification and possibly reference authentication data could potentially allow for incorrect signer enrolment.

NOTE: Please note that the threat is only on the enrolment stage, the PP includes other sections for how a signature key shall be activated e.g. starting from FDP_ACF.1/Signing.

The threat gives as objectives for the ToE of the PP that it must protect the assets R.Signer and R.Reference_Signer_Authentication_Data in at least integrity and if needed in confidentiality. In particular:

- OT.SIGNER_PROTECTION requiring R.Signer to be protected in integrity and for sensitive parts in confidentiality
- OT_REFERENCE_SIGNER_AUTHENTICATION_DATA requiring the ToE to be able to assign signer authentication data to the signer
- OT.SIGNER_MANAGEMENT requiring the signer to be securely created

The security objectives above address user (signer) management inside the signing server, more precisely within the ToE, the signature activation module.

In addition, the ToE requires that only authorized administrators can provide the information (R.Signer and R.Reference_Signer_Authentication_Data) to the ToE.

Since these assets are delivered to the ToE from an external source by the authorized administrator (e.g. the RA officer from the TSP managing the TW4S), there is an objective that the ToE is operated by a QTSP in an environment conformant with CEN 419 241-1 (OE.TW4S_CONFORMANT). In CEN EN 419 241-1, section SRC_SA.1.1, there are requirements for user identification and authentication.

NOTE: there are additional requirements with regard to these assets when a delegated authentication is used – for the sake of simplicity this use-case is not considered in the present discussion. It is considered as correctly and fully covered by the PP where relevant.

OE.TW4S_CONFORMANT and in CEN EN 419 241-1, section SRC_SA.1.1, with a text that maps back to CIR (EU) 2015/1502, cover the risk upstream, between the “registration authority (RA)” and the signing server (remote QSCD) administration (so before R.Signer is installed on the service) the PP has objectives for the environment. Conformance requires signer enrolment to be handled in accordance with [Assurance] for level at least substantial[7] (at least Sole Control Assurance Level (SCAL 2 level[8]) as further enforced by SFR FIA_UAU). There is also an assumption, A.SEC_REQ - *It is assumed that the TSP establishes an operating environment according to the security requirements for SCAL2* that further reinforces the SCAL 2 requirement.

On top of the above claims, one can also add that T.ENROLMENT_SIGNER_IMPERSONATION is partly covered by:

⇨ OE.ENV requiring the TSP to be audited.

This is important since it will ensure a row of security measures which may not be sufficient at all times because signer enrolment is not covered by general TSP requirements (e.g. ETSI EN 319 401 and the like).

**Requirement SCAL 2 are essential to cover the threat. It is important to be sure that SCAL 2 is sufficient for ensuring Annex II 1.(d) requirements are met.**

This assessment needs to consider the **whole process** (certificate issuance and signature creation) because both TSPs have responsibilities in signer's enrolment. The following tasks must be done and are performed by the TSP issuing the certificate, the TSP managing the TW4s or both:

- The signer's identity data must be collected and validated as belonging to the right person
- The signer's identity data are certified, and
- The signer receives an authentication means that will be used to activate its signing key on the TW4S.

The assumption A.SIGNER_ENROLMENT in CEN 419 241-2 states: "*The signer shall be enrolled and certificates managed in conformance with the regulations given in [eIDAS]. Guidance for how to implement an enrolment and certificate management system in conformance with [eIDAS] are given in e.g. [EN 319 411-1] or for qualified certificate in e.g. [EN 319 411-2].*" This assumption is related to certificate management; not to the enrolment of the signer on the singing service. These ENs and the eIDAS Regulation requirements for issuing a qualified certificate (Article 24.4) require the physical presentation of the signatory (or equivalent)[9]. This is a requirement commonly applied for issuing certificate with a high level of assurance on the identity of the signatory.

SCAL2 refers to a level of assurance "substantial" that does not require a physical presentation of the user. To some extent this might downgrade the level of assurance that is provided when the supporting certificate is a qualified certificate (or is issued under ETSI EN 319 411-1).

[7] Substantial refers to the Assurance levels of electronic identification schemes as defined in article 8 of the eIDAS regulation. Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. Under article 8, the assurance levels low, substantial and high are specified as well as the criteria that should meet.

[8] In EN 419241-1, there are specified two Sole Control Assurance Levels (SCAL) of user authentication for demonstrating "sole control" over the user's server-held signing keys. The first level is where the signing application authenticates the user. The second level requires 2-factor authentication and also that this must be enforced from within an HSM.

[9] Or an eID means for which a physical presence was ensured, or an equivalent to physical presence as confirmed by a CAB.

**Whoever the TSP that performs the task is, it is crucial that the signer's information (identity data, signature validation data (SVD, or public key), certificate and eID means and related signer authentication reference) is consistent and belongs to the very same person.** Otherwise, one faces the risk that the TW4S TSP lets a pretender signing in place of the person actually registered by the TSP having issued the certificate.

This is illustrated by the following use-case in which the TSP issuing certificate and the TW4S TSP are discreet entities:

- The TW4S TSP creates a new account for a new signer, so there is a substantial level identity proofing and the TW4S may then provide the eID means to the pretended signer (without face-to-face or equivalent, as not required). R.Signer, R.Reference_Signer_Authentication_Data and SVD are created.
- A certificate request for the signer's key is brought to a CA (directly from TW4S or via the pretended signer).
- The actual signer, (invited to do so by the bearer of a claimed identity for instance), goes to the CA and undergoes the official registration process with a face–to-face, and then the certificate is added to the signer info (sent by the CA, or by the pretender if the certificate is published).

As the TW4S TSP never saw the person in possession of the eID means, it has no the means to certify that it is the same person that enrolled with the CA.

The (Q)TSP issuing the certificate will issue a certificate with a high level of assurance to a certain user B. User B is expected to be the owner of the signing key residing in the device operated by the QTSP managing the key of behalf of user B, but EN 419 241-1 does not require the (Q)TSP to enrol its user with a physical presentation (or equivalent). The fact that the levels are not the same "substantial (SCAL2)"on the one hand and "face-to-face based substantial (eIDAS Art.24.1)" on the other hand can be exploited by a user A. User A can impersonate user B to receive an authentication means from the TSP managing the key and by this way would be able to create QES in the name of user B (having requested the certificate with a face-to-face level).

NOTE: When the TSP issuing certificate and the TW4S TSP are one single entity, there might be no issue. The level of assurance will quite probably be substantial with a physical presence of the signer (or equivalent) or equivalent (since the TSP's RA will follow the most constringent rules between eIDAS substantial (required by EN 419 241-1) and certificate issuance rules), and one has a good assurance that the eID means is handed over to the right person.

There is no problem when the TSP provides the eID means to the signer since the physical presence of the signer (or equivalent) ensures that the right person is in possession of the eID means.

There are requirements on signer's enrolment for the TW4S service on one hand (through EN 419 241-1, level substantial, there are also requirements on the eID means, assumed to be under control or possession of the person to whom it belongs, as per Annex A.2.1 in EN 419 241-1) and assumption on the certification registration on the other hand (quite probably substantial + face–to-face or equivalent, at least if the certificate is qualified).

Between the two processes one finds the signature validation data (SVD, or public key) to be certified and the signer identity and CEN EN 419 241-1 states " *(…) The TSP (editor's note: the TSP managing the TW4S) should also meet the requirements for certificate enrolment to demonstrate sole control (needed by the RA). These requirements are specified in ETSI EN 319 411-1:2015, 6.3.1.a and 6.3.3.d for example*." This requires the TW4S to cooperate with the CA (or at least to work with a CA of a certain quality). This is however a "should" and not a firm obligation (shall).

CEN EN 419 241-2, via OE.CA_REQUEST_CERTIFICATE, and the mention in EN 419 241-2 that the ToE is expected to "be used in conjunction with the TSP issuing certificates", cares for this requirement:

- ⇨ OE.CA_REQUEST_CERTIFICATE : The operational environment shall ensure that the qualified TSP that issues qualified certificates is compliant with the relevant requirements for qualified TSP's as defined in [eIDAS].

The operational environment **shall use a process to request a certificate**, including SVD and signer information, and CA signature **in a way, which demonstrates the signer, is in control of the signing key associated with the SVD presented for certification**. The integrity of the request shall be protected.

- ⇨ **It is a clear security objective on the cooperation with the CA.**
- ⇨ **Combined with the assumption A.SIGNER_ENROLMENT, such CA should follow best practice for signer's registration.**

CAs following EN 319 411-1 have the obligation to control that the signer is in possession (or has control) of the private key (EN 319 411-1 REG-6.3-01). This requirement, to some extent, obliges the CA to control the relationship between the signer and the TW4s and this "closes the gap". When the CA does not issue high-level certificates (NCP or qualified), both processes are substantial (no face-to-face) and no "downgrading" can be be considered (no one complains, as everybody knows there is more risk with substantial than with high).

- ⇨ **So, when the TSP managing the TW4S provides the eID means to the signer, the way to satisfy EN 319 411-1 REG-6.3-01 (proof of possession) shall be provided to the CA by the TW4S and shall be checked by the CA.**

When the TSP issuing qualified certificates follows EN 319 411-2, the following additional requirements apply:

- SDP-6.5.1-02 The TSP shall verify that the device is certified as a QSCD.
- SDP-6.5.1-03 If the device is managed by a third party TSP on behalf of the subject which is not the TSP issuing the certificate itself, the TSP issuing the certificate shall verify that this third party TSP is meeting the appropriate requirements in terms of qualification.
- SDP-6.5.1-04 The certificate request process shall ensure that the public key to be certified is from a key pair generated by a QSCD.
- SDP-6.5.1-07 The TSP shall monitor QSCD certification status until the end of the validity period of the certificate and shall take appropriate measures in case of modification of this status.

- ⇨ **CAs issuing qualified certificates have the obligation (formal when following EN 319 411-2 and anyway functional) to verify the quality of TSP managing TW4S and related QSCD, and vice versa.**

It is also important to have requirements on the revocation or blacklisting of an authentication means and/or signer key activation (e.g. by destroying the key). The usability of remote signing is relative to the level of protection reserved to the signing key with the use of a secure device and operated in a QTSP environment. Signer flexibility renders matters less secure than in the QTSP environment. The signer needs to have access to sound and rapid means to stop access to her signing key along with the ability to revoke a certificate (which might not be provided by the TSP issuing the certificate under some circumstances, e.g. like for short-term certificates).

This is covered by CEN EN 419 241-1, SRC_SA.1.1 which points to Annex 1 whose section A. 1.4 provides suspension and revocation of the binding.

In CEN EN 419 241-2, this is covered in FDP_ACC.1/Signer Maintenance and FDP_ACC.1/ToE Maintenance, which provides the functions to disable authentication means on either a signer basis or for the complete service. FDP_ACC.1/Signer Maintenance allows for reference authentication data to be deleted and FDP_ACC.1/ToE Maintenance allows for configuration data to be changed. This could e.g. be to remove a certificate from an identity provider, which is used to verify assertions.

## 4.5 Other relevant standards

### 4.5.1 CEN TS 419 221-6 (draft)

Conditions for use of a device certified against CEN EN 419 221-5 as a qualified electronic signature or seal creation device.

This technical specification provides guidance on meeting objectives of the operation environment when the cryptographic module is not implemented by a TSP. It does not need to be listed in CID (EU) 2016/650 since the eIDAS Regulation does not impose requirements on end-users (signers) but it is important that the signer protects its environment. This specification shows that a CEN EN 419 221-5 cryptographic module does not necessarily need to be used by a TSP and can be used as a TYPE 1 device.

It shall also be noted that the TSP issuing the certificates to be stored on such a CEN EN 419 221-5 cryptographic module operated by a signatory or creator of a seal, may require the end-user to follow a guidance like TS 419 221-6 in order to include the QSCD statement in the certificate.

### 4.5.2 ETSI TS 119 431-1 (draft)

This TS provides security and policy requirements for TSP managing a remote (Q)SCD.

This TS provides additional requirements on top of CEN EN 419 241-1 and 241-2. At the time of writing of the present document, it is still a draft, but it appears that this TS will complement CEN EN 419 241-1 / 241-2 with regard to the signer's identity data reconciliation.

In particular, it puts the following requirements on the TW4S:

- GEN-6.2.1-08 [CONDITIONAL]: If the SSASP *(ndlr: the TSP managing the TW4S)* provides the eID means, the procedure of generation of the signing key shall be securely linked to the eID means by the SSASP.
- GEN6.2.1-09 [CONDITIONAL]: If the SSASC *(ndlr: the TSP managing the TW4S)* and the certificate generation service component are managed separately, then the SSASC shall support the requirement defined in clause REG-6.3.1-01 of ETSI EN 319 411-1 [2].
- EXAMPLE: By providing an assertion of the authentication of the signer that is linked to the private key.
- LNK-6.2.2-06: The SSASP shall ensure that the person identification data linked to the eID means reference is the same as the one linked to the subject of the associated certificate.

NOTE: When the eID means reference is provided by the TSP issuing certificates registration service, the conformance to this requirement can be assumed.

**These requirements further analyse the workflow between the TW4S and the CA with the aim to ensure the reconciliation of the signer's identity data.**

This TS also provides security and policy requirements for the management of key duplicates and back-up, relevant in the perspective of eIDAS Annex II.4.

### 4.5.3 ETSI TS 119 431-2 (draft)

This TS provides security and policy requirements for TSP supporting signature creation application. At the time of writing of the present document, it is still a draft.

The signature creation application is out of scope of QSCD certification. However, a QTSP managing a QSCD may collaborate with a TSP offering the signature creation service. In this case, the TS is relevant to ensure the global security over the whole ecosystem, in particular the secure link between the signer and the data to be signed (Signature Activation Data (SAD) authenticity), necessary to support eIDAS Annex II.2.

When there is a TSP supporting the signature creation application between the signatory/creator of a seal and the QTSP managing the signature/seal creation data there must be a trusted channel to transport the data to be signed/sealed maintained over the three actors. Although the creation of signature/seal is not a qualified service, TSPs offering such service fall under passive supervision, even if they are not audited. To this regard, ETSI TS 319 431-2 aimed to be sufficient criteria to be verified by the competent supervisory body.

## 4.6 Annex II requirements by the standards

The following figure illustrates the elements of Annex II that apply in the case where a QTSP manages the QSCD (TYPE 2 devices).

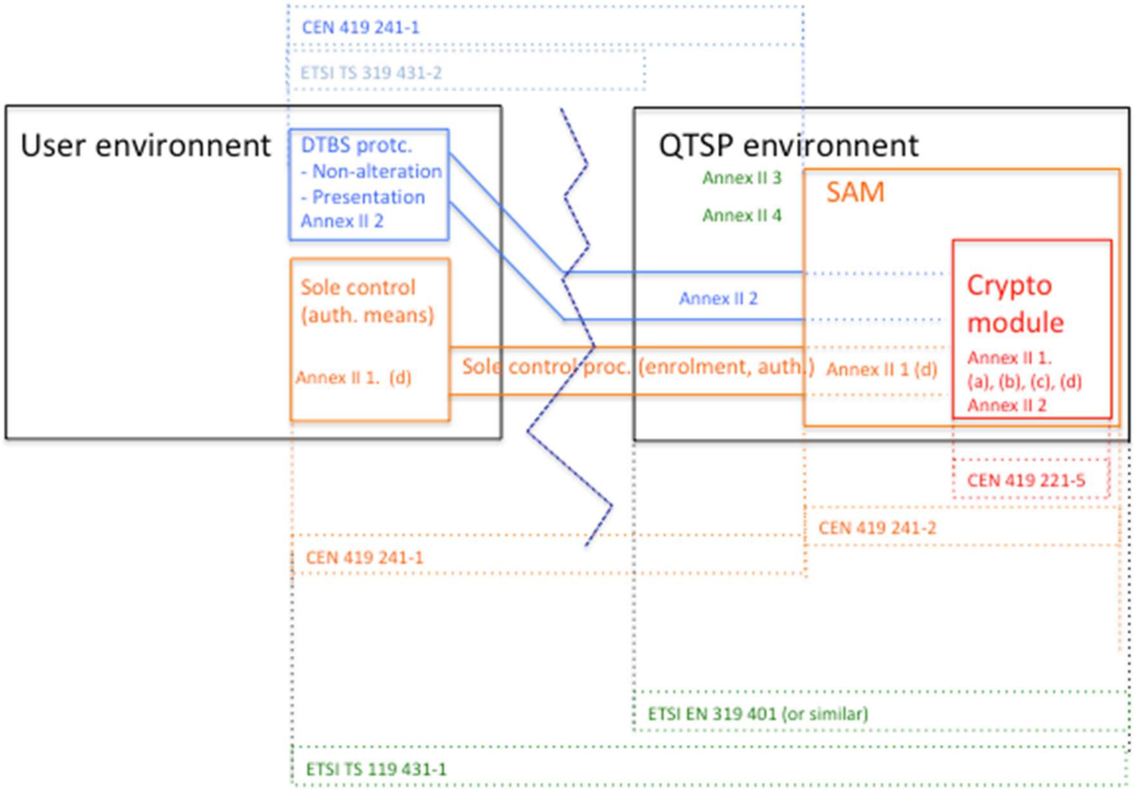

Figure 2: Applicability of the standards to stakeholders

.

# 5. Opinion

## 5.1 Criteria for QSCD certification versus supervision

The Common Criteria evaluation process does cater for the evaluation of a Security Target (ST) that describes how security objectives on the target of evaluation (ToE) and on its environment are met. However, the evaluation only determines if security objectives on the ToE are met (by assessing the SFR) while it is up to the “asset owner” to make sure that, the environment meets the requirements as described in the ST. This means that a series of assumptions or threats are covered by the requirements on the environment that the asset owner must implement correctly.

This is particularly true for the two PPs studied in this report.

These requirements on the environment are validated when the device is managed by a (Q)TSP because a series of eIDAS Annex II requirements are covered by security objectives on the environment. It is difficult to argue they are beyond the scope of the TYPE 2 QSCD certification as there is additional duty to prove trust when a (Q)TSP operating under eIDAS provides the signature services (contrarily to TYPE 1 device, that are in the hand of the user, making that the user is responsible).

As mentioned previously in the text, a series of requirements are covered by the certification process (the actual evaluation of the Security Functional Requirement (SFRs) in the PPs) and a series of requirements fall under the supervision when the device is managed by a QTSP (the requirements on the environment and some assumptions). Such requirements on the environment are further specified by policy requirements such as specified in draft ETSI TS 119 431-1.

Thanks to the organisation of the PPs with requirements covered by the certification process and requirements on the environment (to be covered by the supervision), there are no elements of Annex II that are covered by more than one process (e.g. supervision or certification).

- ⇨ **There are *a priori* no overlaps between the two processes being QSCD certification and supervision of the QTSP managing the QSCD.**

There are some elements from Annex II that are not (fully) covered in the PPs analysed; they concern Annex II.2 and the DTBS.R protection along the whole process and some security measures on the signer’s enrolment and authentication. Policy documents like draft ETSI TS 319 431-1 provide such requirements.

- ⇨ **A certified QSCD can only be officially recognised as such once the QTSP has been duly supervised to manage the QSCD according to requirements and assumptions on the environment provided in the PPs (and possibly as specified in policy documents like ETSI TS 319 431-1).**
- ⇨ **A supervisory body supervises the qualified trust service for which the QTSP is granted a qualified status and the QSCD management; verification starts out with the QSCD and then moves on to any requirement on the environment that may be duly implemented by the QTSP when operating TYPE 2 QSCD.**

There is also joint responsibility on the TSP managing the TW4S to work with appropriate TSP issuing certificates, and on the TSP issuing certificates to work with an appropriate TW4S, in particular to ensure the reconciliation of the signer’s identity data (i.e. the same person is registered by the CA and enrolled on the TW4S).

In particular, a TSP issuing qualified certificate stored on QSCD shall check that the QSCD is certified and managed by a QTSP verified (supervised) for that by its competent supervisory body before certifying the fact that the certificate is stored on such device.

In conclusion, to reach a global security over the whole process it is important that, on top of the CEN 419 241-2 (and CEN 419 241-1):

- ⇨ **The TSP managing the TW4S follows ETSI TS 119 431-1 (or equivalent)**
- ⇨ **The CA issuing the certificates follows EN 319 411-1 (or equivalent)**
- ⇨ **For qualified devices management and qualified certificates issuance, the verification that such requirements are followed, falls under supervision by competent supervisory bodies.**

If the PPs are clear with regard to the requirements subject to the certification, it would be nice to have a checklist that clearly identifies which requirements are audited in the scope of the supervision, originating from the PPs and possibly other policy documents like draft ETSI TS 319 431-1 (basically identified in the present document). Indeed, the sentence currently accompanying the TYPE 2 device certification information in the compilation of Member States notification on SSCDs and QSCDs is vague. If it becomes part of an amended version of CID (EU) 2016/650 it needs to be enhanced with references to applicable norms and related requirements.

It is suggested that a specific work is undertaken to provide such checklist. Two checklists actually could be issued; one with the functional objective to be supervised (for the supervisory bodies) and one with the related technical criteria to be audited by the CABs, issued from the PPs and related standards.

## 5.2 Referencing

The EU publishes a list compiling Member States notifications of SSCDs and QSCDs. Besides this list, and provided that a certain amount of coordination between the stakeholders mentioned above and the supervisory and certification bodies will be required to achieve a global trust level, it would be pertinent to **provide a way to advertise on the elements under supervision**. The trusted list of the country where QTSP operates might provide an indication when the QTSP manages a QSCD duly in accordance with eIDAS. Alternatively, the EC compiled list of notified SSCDs and QSCDs might be used for that. This would be important for informing the market and organisations that wish to implement qualified electronic seals or signatures conformant to eIDAS.

# 6. Bibliography/References

## 6.1 References

| REF. ID | DESCRIPTION |
|---|---|
| [1] | Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.<br>http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG |
| [2] | Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) 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 |
| [3] | CEN EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, dated 2018-05-11; |
| [4] | CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services |
| [5] | CEN EN 419 241-1: Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements, dated 2018-02; |
| [6] | ETSI TS 119 431-1 (draft) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev |
| [7] | ETSI TS 119 431-2 (draft) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation |

# Annex A: eIDAS and QSCD

## A.1 Recitals

(51) It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.

(52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.

(55) IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.

(56) This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.

## A.2 Articles

3 (22) ‘electronic signature creation device’ means configured software or hardware used to create an electronic signature;

3 (23) ‘qualified electronic signature creation device’ means an electronic signature creation device that meets the requirements laid down in Annex II;

3 (13) ‘electronic signature creation data’ means unique data which is used by the signatory to create an electronic signature;

Article 29 - Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 30 - Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.

3. The certification referred to in paragraph 1 shall be based on one of the following:

(a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or

(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

ANNEX II - REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;

(b) the electronic signature creation data used for electronic signature creation can practically occur only once;

(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:

(a) the security of the duplicated datasets must be at the same level as for the original datasets;

(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

ENISA
European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

TP-03-18-507-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-273-8
DOI: 10.2824/50750