Towards global acceptance of eIDAS audits

V1.1

MAY 2019

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 enquiries about this paper, please use press@enisa.europa.eu.

Contributors

Arno Fiedler, Nicholas Dunham, Dr Christoph Thiel, Inigo Barreira

Editors

Evgenia Nikolouzou (ENISA), Slawomir Gorniak (ENISA)

Acknowledgements

We would like to thank the following experts for reviewing this report and providing valuable comments: Nick Pope and Dimitris Zacharopoulos.

ISBN: 978-92-9204-255-4, DOI: 10.2824/74012

Table of Contents

Executive Summary

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereafter the eIDAS Regulation), adopted on 23 July 2014, extended the scope of the Directive 1999/93/EC on a community framework for electronic signatures (eSignatures Directive), by introducing in the legal framework provisions for new types of trust services. These new trust services include electronic seals, electronic time stamps, electronic registered delivery services and, specific to this report, certificates for website authentication. Widely known as SSL/TLS certificates, website authentication certificates play a critical role in the security of online transactions, have long been employed by websites and have been increasing in deployment throughout the online environment.

The eIDAS Regulation introduces a legal framework and establishes a scheme for granting qualified status to these new types of trust services aiming to enhance consumer's trust in the digital environment and to improve the transparency of the trust services market. Following the publication of the eIDAS Regulation, a set of secondary and co-regulatory acts were published in order to provide technical guidance on how to implement the specific requirements of the eIDAS Regulation. Underlying the market for EU qualified website authentication certificates (QWACs) and other trust services is a conformity assessment scheme, whereby the providers of qualified trust services undergo regular assessments by accredited assessment bodies, overseen by national and EU authorities.

The goal of the study was to explore the eIDAS Conformity Assessment Report (CAR), the corresponding audit requirements, gaps arising from comparison with competing audit schemes, and the emergent issues at the core of the global conversation between major stakeholders in the qualified trust service provider (QTSP) audit ecosystem. This report also seeks to accomplish a targeted survey of the non-technical sphere of QWACs, notably the overlapping political and economic environments into which the EU certification scheme was born and has grown in the past few years.

In this study, we discuss these aspects and identify the most prominent recommendations for improvement that can increase global acceptance of eIDAS audits. Towards this goal, this study identifies recommendations for strengthening:

- the clear and formal adoption of a harmonised conformity assessment scheme in the EU and the advancement of these schemes in the international context,
- the promotion and referencing of specific standards covering the auditing of TSPs and the conformity assessment report, and
- the public recognition of the trust generated by the scheme.

The main recommendations deriving from the study are summarised below:

- There is need to agree upon and define a harmonised conformity assessment scheme against which CABs would be accredited and the QTSP/QTS assessed in order to verify conformance to the eIDAS Regulation requirements. Such a process would involve all the stakeholders - EA, ETSI, EC, ENISA, SBs – which would participate from the specification till the enforcement of such scheme.
- A centralised list of all CABs should be maintained (by the European Commission) and regularly updated, where it will be clearly indicated whether a CAB has been accredited under ETSI EN 319 403 by a NAB and whether it has been accredited in line with the ETSI standards concerning the certification scheme in order to be recognised also by the CA/B forum and the browsers.

- It is recommended that ENISA, in cooperation with ETSI and CEN, develop and publish a comprehensive set of auditors' requirements together with best practice examples from the field.
- It is recommended that ETSI ESI should provide further specifications in the detailing of the requirements for TSP procedures and audit best practice to "set up New Roots" and "CA Key Generation.
- There is need to further analyse, test and review how the EU trust mark can be displayed on websites in a tamper-proof manner in order to increase the global visibility of the EU trust mark as a trusted logo for qualified trust services, which would in turn strengthen the acceptance of the audits. This could be done by the European Commission or by ENISA.
- It will be challenging to grow the value of QWACs outside the EU Digital Single Market by convincing the browsers and OS vendors to include the TSL in their respective root stores. Towards this goal face-to-face meetings should be arranged by the European Commission with the browsers also in the context of CA/B Forum meetings.
- Since "banks are taking part in educating customers by offering browser plug-ins for enhanced security and peripheral education" (Timmerman, 2004), a foreseeable next step is the full pan-European usage of the trust mark on bank websites that fall under the purview of PSD2 rules. This agenda might also be extended to the TSL integration for all operating systems and browser vendors operating in the European Union as part of a wider rollout of the trust mark and its potential close association with QWACs.

1. Introduction

1.1 Purpose

This report explores the paths to global acceptance of the eIDAS auditing framework for trust service providers (TSPs) issuing qualified website authentication certificates (QWACs). The goal of the study was to explore the eIDAS Conformity Assessment Report (CAR), the corresponding audit requirements, gaps arising from comparison with competing audit schemes, and the emergent issues at the core of the global conversation between major stakeholders to the qualified trust service provider (QTSP) audit ecosystem. This report also seeks to accomplish a targeted survey of the non-technical sphere of QWACs, notably the overlapping political and economic environments into which the EU certification scheme was born and has grown in the past few years. Developing issues concerning technology shifts, tangled with pronounced ideological struggles in the global geo-political environment will also affect the outcome of the eIDAS trust framework as much as the technical and procedural requirements set forth in the developed European regulatory environment.

In order for stakeholders – such as relying parties and end users – to build and maintain confidence in the security of qualified trust services (QTS), they need to have the assurance that qualified trust service providers (QTSPs) have established a set of procedures, processes and security measures to minimize the associated operational and financial threats and risks. Under eIDAS, this is accomplished by audits carried out by accredited Conformity Assessment Bodies (CABs). To support both the infrastructure of the audit scheme as well as the audits (also called assessments) themselves, ETSI has developed a set of standards to support TSPs (ETSI EN 319 401, 411-1, 411-2, 421) and CABs (ETSI EN 319 403, TS 119 403-2), which meet the corresponding security and policy requirements stemming and policy requirements stemming from the eIDAS Regulation. This report aims to map the requirements of the ETSI framework to other international standards and requirements (as developed, for example, by the Certification Authority/Browser Forum and WebTrust) in order to facilitate the widespread use of qualified certificates for website authentication and the global acceptance of eIDAS audits.

In addition, it is critical for the trust placed in an underlying trust service, such as the provision of QWACs, to be visible to the average end-user. Trust services without a visible metric of trust such as that provided by the QWAC, which is based on accountability, will be difficult to foster and upkeep.

Considering the eIDAS Regulation as a framework, there is significant space for individual interpretation and for development since it does not impose any specific accreditation scheme for which CABs must be accredited against, or any best practice standard that QTSPs or QTS must comply with in order to be granted the qualified status. From a perspective that relates to standards, policies and requirements (less so to economic, political and social forces) upon which much of this report focuses, the success or acceptance of the eIDAS audits depends on several factors that hinder further recognition of the scheme:

- non-existent statutory/mandatory specification of any (but especially the ETSI/CEN) standards, which were developed as a basis for the eIDAS-compliant operation of TSPs,
- the lack of harmonization of requirements within the EU (and thus beyond) at the level of CABs accreditation and certification scheme for TSP auditing, and
- limited visibility of the trust generated by the scheme.

In this study, we discuss these aspects and identify the most prominent recommendations for improvement that can increase global acceptance of eIDAS audits. Towards this goal, this study identifies recommendations for strengthening:

- the clear and formal adoption of a harmonised conformity assessment scheme in the EU and the advancement of these schemes in the international context
- the promotion and referencing of best practice standards against which TSPs can be audited, and standards for how the audit is carried out and reported
- the public recognition of the trust generated by the scheme.

1.2 Methodology

This research method (Figure 1) has been selected in order to combine findings from the audit scheme and underlying standards with input from subject matter experts, relevant literature and practical case examples.

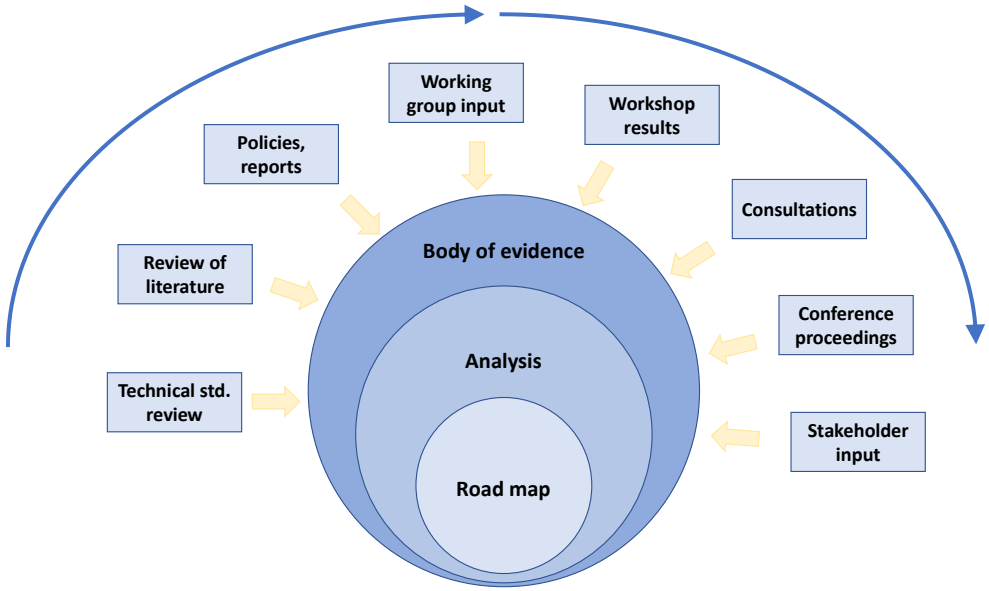

Figure 1: Methodology of the study

The research method for this report consists of three elements:

- a description containing an assessment of the eIDAS regulatory framework for audits and underlying best practices standards, as well as findings from literature research
- an analysis in which findings based on expert contributions and presentations of international task force sessions are substantiated via literature and the best practices standards, and
- a synthesis in which opportunities and directions for improvement are identified and explored.

Ongoing discussions at international working groups and conferences and the opinions and statistics which will emanate therefrom have informed and continue to inform this discussion, and will ultimately be useful to policy-makers in the EU who are searching for a way to achieve the goal set forth in this report: to foster and grow global acceptance of the eIDAS trust framework and its corresponding auditing scheme for QTSPs issuing QWACs. During the course of the drafting and revision processes of this report, several notable discussions between industry actors took place (and continue to take place), partially shifting the

focus of this report towards the search for resolution between leading browsers and the ETSI scheme in support of the European approach to (Q)TSP auditing within the eIDAS framework.

1.3 Structure of the report

This study is divided into six chapters in total, covering how the global acceptance of eIDAS audits can be improved. In brief:

Chapter 2 describes the background of eIDAS and its audit scheme. It sketches a backdrop for this study, focusing on the TSP supervisory scheme as well as the tasks of the stakeholders in the eIDAS organizational hierarchy. It also discusses the conformity assessment criteria and standards, assessment procedures and the conformity assessment report.

Chapter 3 compares the eIDAS regulatory framework for audits with different prevailing trust frameworks (and their respective audit schemes) – e.g. ETSI, WebTrust for CAs, ISO 27000 series and Federal PKI frameworks – and highlights possible shortcomings of the eIDAS audit scheme.

Chapter 4 discusses the underlying standards of the eIDAS regulatory framework for audits, especially certificate policy documents ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 401, and contains a level of detailed assessment, comparing them with others, specifically with a narrow focus on WebTrust.

Chapter 5 presents a dive into the challenges the eIDAS regulatory framework for audits faces to global acceptance. Topics discussed include the current situation regarding the visibility of the use of the EU Trust Mark, especially in current market-leading web browsers and the ongoing struggle to convince browsers to accept the eIDAS TLS scheme.

Chapter 6 offers a roadmap – a concrete set of recommendations – including auditor skills and competences, optimized reports and promotion as a way forward for the eventual, enhanced global acceptance of the audit scheme under the eIDAS Regulation.

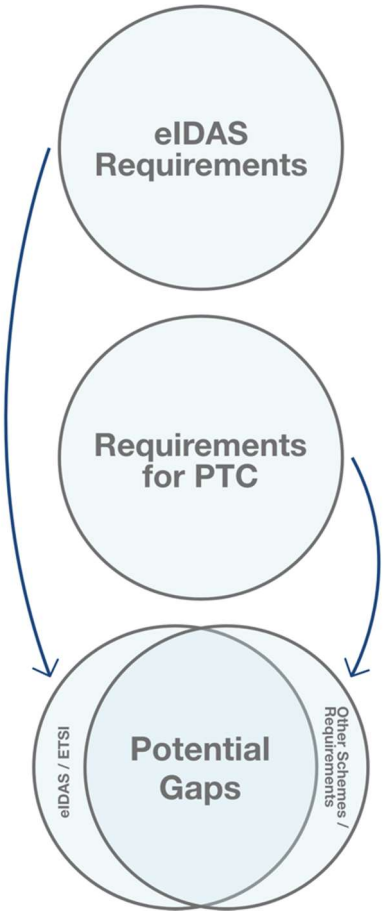

Figure 2: Determining gaps between eIDAS and other schemes

2. eIDAS Regulatory Framework

The eIDAS Regulation[1] repeals the 1999 Directive concerning electronic signatures by providing a new legal framework for "electronic identification and trust services for electronic transactions in the internal market". Whereas the former Directive focused solely on electronic signatures, the eIDAS Regulation extends the concept of trust services to other services such as electronic seals and time stamps, registered mail and website authentication.

To enhance the trust of enterprises and consumers in the internal market and to promote the use of trust services and products, the eIDAS Regulation introduces the notion of qualified to electronic trust services as well as to the providers themselves (i.e. QTS and QTSPs). It aims to identify requirements and obligations that ensure a high level of security for whatever qualified trust service or product is used or provided.

Since this study primarily concerns certificates for website authentication, the discussion hereinafter focuses on what are broadly referred to as QWACs, which play a critical role in the security of online transactions. Prior to the rollout of eIDAS, non-qualified[2] SSL/TLS certificates had long been used in website authentication and network traffic encryption services. For more information, ENISA has previously published a number of relevant studies which concern a range of topics concerning QWACs, including the emergence and growth of a European market for QWACs.

QWACs present a particular case among the newly introduced trust services in the eIDAS Regulation, since they are entering an already mature, global and unregulated (from the point of view of state governance) market for SSL/TLS certificates. For a successful introduction, it will be necessary to stimulate demand for QWACs by properly communicating to consumers their benefits, while at the same time supporting providers to ensure sufficient supply.

As this emergent market matures, becoming more dynamic and transparent, the infrastructure for ensuring the system's trustworthiness will also need to be bolstered with smart, flexible and diverse strategies, especially in light of the stated goal of bringing QWACs and the underlying audit schemes, as accepted by the national authorities, to wider global acceptance, especially to achieve acceptance (i.e. support and visualization) as "Publicly Trusted Certificates" (PTC) [3] by the browser vendors. In other words, the emergence of an ecosystem comprising TSPs, supervisory bodies (SBs), CABs, national accreditation bodies (NABs) and the certificates themselves onto the global stage require cooperation at all levels.

2.1 TSP supervisory scheme

In order to ensure a high-level of security of qualified trust services, the eIDAS Regulation foresees an active supervision scheme of QTSPs and the QTS they provide by a competent national SB that supervises, ex-ante and ex-post, fulfilment of the QTSP/QTS requirements and obligations. Therefore, when a TSP

[1] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[2] The term "non-qualified" is expressly from the point of view of eIDAS and designates all trust services and providers that have not undergone the rigorous certification process set forth by eIDAS since it went into effect in 2016. This includes domain-validated (DV), organization-validated (OV), extended validation (EV) and other certificates for website authentication.
[3] "Publicly Trusted Certificate" is a specific terminology used by the CA/B Forum; all certificates issued to the public are generally considered "publicly-trusted". The term refers to certificates that are issued to the public and the issuing or root CAs are included in the correspondent browser root store.

(without qualified status) intends to begin providing qualified trust services, it submits to the SB a notification of their intention, together with a CAR issued by a CAB accredited under a conformity assessment scheme recognised by the national supervisory body (SB). NABs contribute to the quality assurance of the whole process by being responsible for accrediting and supervising CABs, which perform the conformity assessment audits of the TSPs.

The eIDAS Regulation introduces a clear separation of duties and tasks between CABs and SBs: while the CAB is the body responsible for confirming the compliance of the TSP, according to eIDAS, the SB is the body responsible for actually granting the qualified status. More precisely, Article 17 (4) of the eIDAS Regulation states that the tasks of the supervisory body shall include in particular:

- to analyse the conformity assessment reports (Articles 20(1) and 21(1))
- to carry out audits or request a CAB to perform a conformity assessment of the qualified TSPs (Article 20(2)) and
- to grant qualified status to TSPs and to the services they provide and to withdraw this status (Articles 20 and 21).

The tasks of CABs[4] under the eIDAS Regulation are:

- performing the audit of (qualified) TSPs (Article 20 (1))
- reporting the audit results in written form (a requirement by CAB accreditation)
- making a 'compliance statement' confirming (or disproving) the compliance of a QTSP and its QTS with all the applicable eIDAS requirements (Article 20 (1))
- providing the conformity assessment report (CAR) with the compliance statement to the TSP (Article 20 (1)) and
- usually also directly to Supervisory Body (Article 17 (4) b), Article 20 (2)).

After the successful completion of the audit, the CAB issues a CAR. This report contains all results of the assessment performed and is provided to the TSP, which must in turn provide it to the responsible SB. The compliance statement by a CAB is formally non-binding for the SB for granting or not granting the qualified status to a TSP but represents an important basis for the subsequent decision. Only after a full review of the CAR and any additional requested information will the SB decide whether the TSP and the trust services it provides are in fact compliant with eIDAS requirements. After a maximum of three months following the submission of the conformity assessment report, the SB notifies the TSP of its decision.

If positive, the TSP and the audited trust services will be granted the "qualified" status and will be added to the national trusted list (if it is not already within). In the case that a QTSP and its QTS no longer meet the requirements, the SB then withdraws the qualified status (in the case of a new TSP/TS, it will not grant the qualified status) and informs the body responsible for the national trusted list about its decision. As stated by Article 20 of the eIDAS Regulation, once the qualified status is granted, a QTSP will have to provide a new CAR to the responsible SB every 24 months (or whenever requested by the SB) in order to maintain their qualified status.

Figure 3 provides an overview of dependencies between various stakeholders in the TSP assessment scheme under the eIDAS Regulation.

[4] A current list of accredited CABs is accessed at https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation.

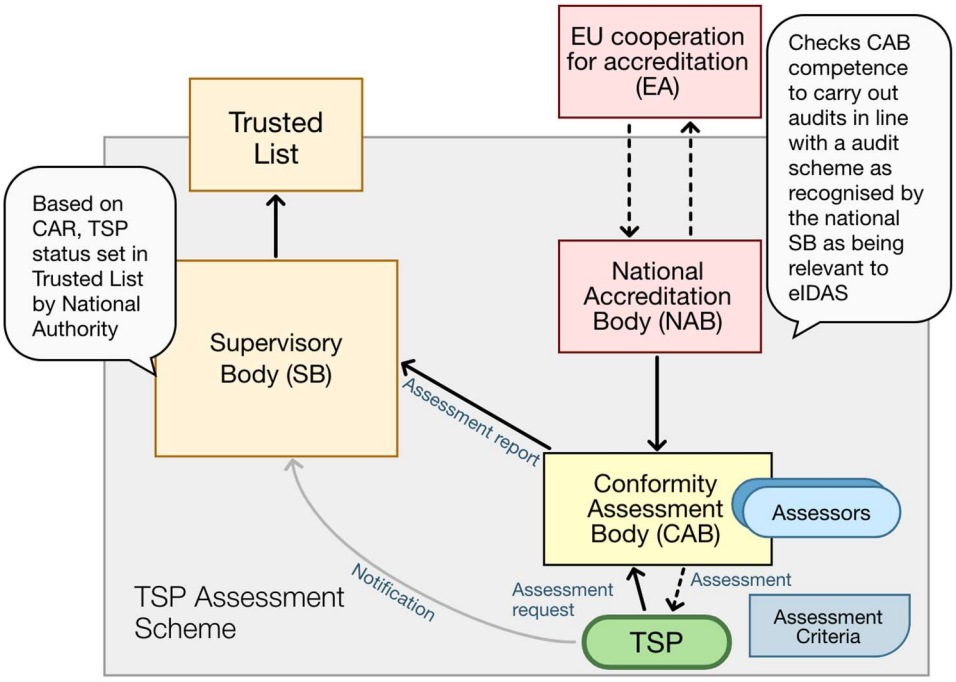

Figure 3: TSP assessment scheme (courtesy of ETSI/ESI)

The European Accreditation (EA) is the body recognised under the EC Regulation No 765/2008 that organises the peer evaluation scheme among the NABs from the EU Member States and other European Countries. Each NAB determines the fundamental ability of a CAB for conducting conformity assessments in accordance with (specific) accreditation criteria. To this day, there is no implementing act, but instead the decision as to whether a scheme meets the requirements of eIDAS and expects appropriate competencies for trust service audit is left to the supervisory body. For the accreditation of a CAB to operate in the eIDAS scheme and, consequentially, for it to undertake certification of TSPs, ETSI, in collaboration with the EA and with representatives of the interested parties, has developed a specific standard (ETSI EN 319 403) for the accreditation of CABs assessing trust service providers and the services they provide. The ETSI EN 319 403 defines an accreditation scheme that:

- requires the accreditation of CABs based on ISO/IEC 17065, and
- supplements ISO/IEC 17065 by defining additional requirements for a CAB's capabilities for performing conformity assessment (certification) of TSPs and the trust services they provide against specific criteria based on standards (such as the ETSI standards for TSPs), publicly available specifications (such as the CA/B Forum baseline or extended validation guidelines) or regulatory requirements (such as the eIDAS Regulation).

2.2 Conformity assessment scheme, criteria and standards

The general approach for CABs assessing the conformity of TSPs and the services they provide is presented in ETSI EN 319 403. For each step of the audit, all the general requirements for evaluating TSPs against the requirements are described in the text of the eIDAS Regulation itself. As mentioned above, however, there is currently no implementing act for this; it is left up to the supervisory body to verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in eIDAS Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide. EN 319 does not include the specific criteria for the type of trust

service to be assessed. This is covered by the relevant regulatory requirements or standards aimed at the type of trust service being assessed.

The audit process, based on ISO 17065 and implemented in ETSI EN 319 403, is divided into different parts:

- General preparation – to agree on the terms of the audit (time, location, scope, etc.)
- Documentation review – to review the documentation regarding the TSPs and TS provided
- On-site audit – to validate the preliminary findings and complete the audit against the predefined assessment criteria

At the end of the process, a conformity assessment report (CAR) containing all the results of the audit will be issued by the CAB to the TSP.

After analysing the list of CABs accredited against the requirements of the eIDAS Regulation, as maintained by the European Commission[5], it is concluded that the EA has widely promoted the accreditation framework of ISO 17065 completed by the certification scheme defined in ETSI EN 319 403. The EA has promoted ETSI EN 319 403 as a channel to demonstrate conformity with relevant requirements laid out in the eIDAS Regulation through assessment by CABs. In fact, 21 of the 22 currently eIDAS accredited CABs follow this EA framework.

Conformity assessment schemes based on standards such as EN 319 403 can be adopted by CABs to certify conformance of QTSPs, and the QTS it provides, with the eIDAS regulation (Article 20.2) as well as best practice standards such as the CA/B Forum guidelines and/or ETSI standards defining policy requirements for particular trust services. However, there does not exist a fully comprehensive list of requirements that has to be used by all CABs for conducting a conformity assessment (Article 20 (4)). Consequently, there is no guarantee that the audit is carried out by a CAB with the competencies and procedures appropriate to the trust services it is assessing. Also, if an audit is carried out just against the requirements of the eIDAS Regulation, there is no guarantee that the policies and practices are or will be in line with accepted best practices standards.

Moreover, the final decision regarding the qualification of the TSP and its trust services is made by the responsible SB that verifies compliance with the requirements laid down in eIDAS Regulation (Article 21(2)). However, the SBs in Member States lack a set of defined and harmonised requirements or criteria related to the compliance (or lack of compliance) of a TSP to the requirements laid down in the eIDAS regulation.

2.3 Identified gap: Harmonization

One of the major shortcomings of the conformity assessment scheme and the assessment criteria used under the eIDAS Regulation appears to be the absence of standardization for the conformity assessment process (certification).

While the accreditation of almost all CABs listed is according to ETSI EN 319 403 (based on ISO 17065), it may happen that different CABs of different Member States will use different criteria by which a TSP will be audited.

Specifically, the eIDAS Regulation itself lends few words to the topic of the CAR. The rigor of presentation (measured generally by the level of detail) is, however, not specified, even though it may be crucial to

[5] The most recent version of this list is accessed at https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation.

enabling the SB to decide on the qualified status of the TSP. The form of presentation is additionally not specified; it is assumed that the CAR might follow the structure of each single requirement from the applied assessment criteria e.g. directly from eIDAS itself, or like-wise from EN 319 401, EN 319 411-1 and -2 and EN 319 421. From the above it is also derived that it is also not regulated according to which criteria the SBs measure whether a TSP has reached the status of "qualified" or not.

This may result in incongruences in the qualification of TSPs in different countries as well as their qualified trust services. This may lead to a non-harmonized trust service market and give rise to doubts about the quality of QTS, which may include QWACs. In this case, harmonization (or the lack there-of) refers to a mandated, detailed or specific set of norms describing the process of producing a CAR for a certification under the eIDAS scheme; it is currently an ongoing topic of discussion at the lever of the Forum of European Supervisory Authorities (FESA).

It is also of interest that the CAR provided to the SBs is not considered a public document, meaning that most TSPs have not published a detailed CAR that is provided to the SB. In fact, they only publish the “certificate”, which provides evidence for the successful completion of the audit. This is an important point from the perspective of (different) browsers, who require documents and reports that can be made publicly available. Some browsers may be more amenable to the confidentiality of these CAR documents and others may not.

The absence of a standardized CAR constitutes a challenge, but also offers an opportunity forward. CABs that have different interpretations of the actual scope of audits and/or the content of audit reports might be better aligned with the publication and enforcement of implementation acts for the accreditation of CABs across borders.

To avoid inconsistent qualification of TSPs and their qualified services, it is necessary to:

- harmonize the conformity assessment scheme against which the CABs are accredited
- harmonize the level of detail and structure of the Conformity Assessment Report issued by CABs and the conformity assessment requirements during the TSP auditing
- harmonize the procedures followed by the national Supervisory Bodies used to verify whether the TSP and the trust services provided comply with the requirements laid down in the eIDAS Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide
- integrate the requirements from external bodies like the CA/B Forum to ensure that the audit follows proper form and adheres to the requirements of the international community
- agree on the criteria to be used for assessment, in particular, whether this is just at the level of the regulation or if it also includes best practice standards such as CA/B Forum guidelines or ETSI standards.

3. Overview of Trust Frameworks

"Trust" may be defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" (Rousseauo, 1998). In the online environment, required positive expectations to reach the state of trust may differ from application to application, such as making an online payment, sending an e-mail or signing a business contract. To serve the needs of this sensitive and differentiated digital ecosystem, several trust frameworks have been established, each attempting to lay the groundwork for trust and enhance the confidence that users can have in all of their digital transactions.

This chapter considers prominent existing trust frameworks in order to discover the similarities and differences between them and analyse these findings in order to derive fundamental structural requirements for such trust frameworks. The aim of this chapter is to identify gaps between coverage in the trust frameworks and assess the directions our recommendations, based on the technical analysis, will lead to some recommendations in the final chapter of this report. Since, in effect, the field is a "moving goalpost", the nature of this study at present is intended to be dynamic and responsive to impending changes to the trust service landscape.

3.1 Key concepts and terminology

In terms of key concepts and terminology (cf. (Sel, 2015)), this report follows the structure of (Hamaguchi 2016), which presents the similarities and differences of several trust models. In most if not all instances where trust in electronic transactions is established, the following four types of trust components are involved: computational trust components (such as hard mathematical problems like the Discrete Logarithm Problem or finding points along an elliptical curve), technology components (such as CA servers, hardware security modules (HSMs) and online certificate status protocol (OCSP) responders), operating procedures (such as face-to-face registration of an applicant who wants to subscribe to a TSP's services) and compliance components. An appropriate combination of these components will yield legal effect.

There are many competing definitions and vocabularies for trust, indicating the concept's importance in many different scenarios and for different stakeholders. In the context of the present study, we use the following model terms:

- Trust framework: a model of multiparty interactions that aims at facilitating a Relying Party's decision on the basis of metadata and services
- Trust ecosystem: collection of trust frameworks
- Mechanism: the apparatus, system or process used to bind the participants within the frame-work
- Actors:
  - Initiator: the actor that took the initiative to create the trust framework
  - Governor/oversight keeper: the actor that governs the trust framework and/or over-sees it
  - Operator: the actor responsible for the operation of the framework
  - Assessor: an actor that provides claims about participants
  - Participants: actors that accept to be bound through the mechanism, this includes:
    - TSPs: actors providing trust services such as authentication, signature creation, validation, long term preservation, registered electronic delivery, time stamping etc. In such a context, the TSP can also be referred to as the trustee, the entity that is potentially trusted
    - Subscribers: actors that subscribe to services offered by TSPs
    - Relying parties: actors that rely on services offered by TSPs.

- Metadata: data provided about the services and data used within a trust framework

Audit schemes by both ETSI and WebTrust are well known to major browser vendors and TSPs issuing website authentication certificates because these two frameworks are adopted by the trusted root CA programs of major browser vendors such as Google, Mozilla and Microsoft (CA/Browser Forum, 2017). Website authentication (SSL/TLS) certificates are electronic certificates for managing the secure connection between the web server and the end user's computer through the browser. SSL/TLS certificates are used for other services that require TLS authentication, as well.

3.2 Conformity assessment scheme and audit requirements for TSPs based on ETSI standards

Certification in accordance with ETSI standards is performed by CABs, which are accredited by NABs within each respective Member State. Harmonization of accreditation processes among accreditation bodies is coordinated through by the EA. Figure 4 shows the trust framework of ETSI certification for the browsers' root program for TSPs.

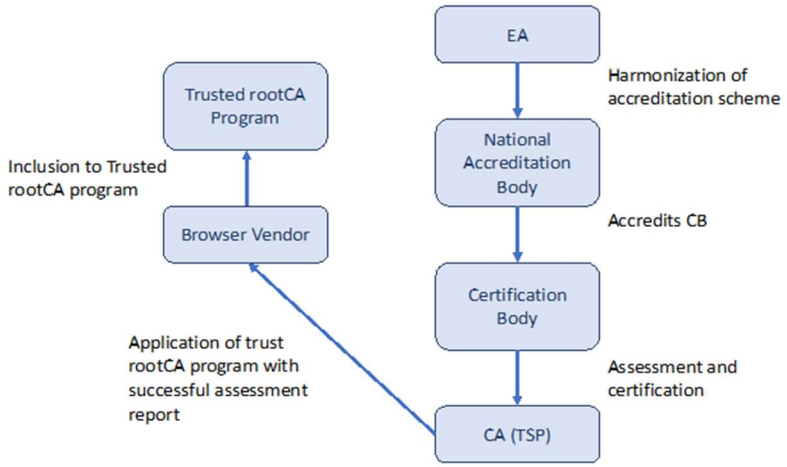

Figure 4: The trust framework of ETSI certification for root CA program (based on (Hamaguchi, 2016))

ETSI EN 319 401 specifies general requirements for TSPs; however, this is not audited independently. When auditing against EN 319 411-1 or -2 (or any other eIDAS trust service), there exist requirements in these documents which reference EN 319 401. This is to say, checks against relevant EN 319 401 requirements are carried out when conducting an EN 319 411-1 and/or -2 audit.

EN 319 411-1 specifies generally applicable policy and security requirements for TSPs issuing public key certificates, including trusted website authentication certificates. It provides guidance to the TSP to develop, implement, enforce and update the Certification Practise Statement (CPS) (which describes the practices and procedures used to address all the requirements identified for the applicable TSP's policy) and the Certificate Policy (CP) (which refers to the CPS to indicate how the TSP implements the policy requirements for the selected CP). EN 319 411-2 specifies policy and security requirements for the issuance, maintenance and life-cycle management of EU qualified certificates as defined in eIDAS Regulation. This builds on the requirements of EN 319 411-1 and a TSP can support both technical requirements of PTC certificate policies and eIDAS QWACs.

Moreover, ETSI has recently published TS 119 403-2, which defines additional requirements for CABs auditing TSPs that issue publicly-trusted certificates (PTC), and it is expected soon to publish the ETSI TS 119 403-3, where requirements for CABs assessing QTSPs against eIDAS will be defined. In order to clarify the difference between TS 119 403-2 and -3, it should be noted that TS 119 403-2 is aimed at meeting the audit requirements of issuers of PTCs as described by CA/B Forum and address specific root store requirements. It includes requirements concerning the audit frequency and audit attestation and defines subsequent audits that examine the history of any events that occurred over the period leading to the last audit. TS 119 403-3, however, aims to provide additional requirements on the certification scheme used by CABs assessing the QTSPs and the QTS they provide in order to demonstrate compliance against the requirements laid down by eIDAS. Both TS 119 403-2 and TS 119 403-3 also require the audit to be carried out in conformance with EN 319 403.

Table 1: Relevant ETSI standards to eIDAS conformity assessment for TSPs[6]

CERTIFICATION POLICY FOR TSPs		
ETSI EN 319 401	*General policy requirements for trust service providers*	This document specifies policy requirements for TSPs that are independent of the type of TSP whether certificate issuer (qualified or otherwise), timestamp issuer, signature verifier, e-delivery provider or other form of trust service provider. It defines policy requirements on the operation and management practices of TSPs.
ETSI EN 319 411	*Policy and security requirements for trust service providers issuing certificates*	This multi-part document specifies policy and security requirements for TSPs issuing certificates. It references EN 319 401 for generic requirements. Both parts provide informative annexes with a check list of the policy requirements that can be used by the TSP to prepare an assessment of its practices against the document and/or by the assessor when conducting the assessment for confirming that a TSP meets those requirements. It also includes the following topics:
ETSI EN 319 411-1	*General requirements for trust service providers issuing certificates*	This part specifies generally applicable policy and security requirements for TSPs issuing public key certificates, including trusted website certificates. The policy and security requirements are defined in terms of requirements for certificates. These policy and security requirements support a number of reference CPs (LCP, NCP, NCP+, EVCP, OVCP, DVCP).
ETSI EN 319 411-2	*Requirements for trust service providers issuing EU qualified certificates*	This part specifies the policy and security requirements for TSPs issuing qualified certificates as defined in the eIDAS Regulation. These policy and security requirements support reference CPs (QCP-1, QCP-n, QCP-1-qscd, QCP-n-qscd, QCP-w) for the issuance, maintenance and life-cycle management of qualified certificates issued to natural persons (including natural persons associated with a legal person), to legal persons and websites.

[6] Visit https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx for more information about recent, current and ongoing ETSI activities.

Table 2: Relevant ETSI standards for eIDAS conformity assessment for CABs[7]

REQUIREMENTS FOR CABs		
ETSI EN 319 403	*Trust service provider conformity assessment – Requirements for conformity assessment bodies assessing trust service providers*	This document is based on ISO 17065 and contains requirements for the competence, consistent operation and impartiality of conformity assessment bodies assessing conformity of trust service providers to standardized criteria for the provision of trust services. Requirements and guidance set out in this document are independent of the class of trust service provided. As reaction to the browser requirements, in spring of 2018, ETSI published TS 119 403-2, *Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates*, which is intended to bring about audit reports that are more compliant with the browser requirements.
ETSI TS 119 403-2	*Additional requirements for conformity assessment bodies auditing trust service providers that issue publicly-trusted certificates*	This document provides additional requirements for CABs auditing TSPs that issue PTC.
ETSI TS 119 403-3	*Additional requirements for conformity assessment bodies assessing qualified trust service providers against the eIDAS requirements*	This document provides additional requirements for CABs assessing qualified TSPs against the eIDAS Regulation requirements.

3.2.1 Analysis of CAB requirements and EN 319 403 / ISO/IEC 17065

The auditing scheme based on ETSI standards can be regarded as a certification scheme, meaning it comprises an examination of whether a TSP's system, product or process faithfully implements the requirements as laid out in the described ETSI documents. Concluding the assessment process, if the TSP meets the criteria described in the applicable standards, the output is a certificate. As a TSP may have a contractual obligation to meet the criteria within three months in order to receive a positive decision on its certification request, this TSP may have to take corrective measures on issues identified, as permitted and requested by CAB. Specifically, a TSP audit may be passed with pending nonconformities provided that these do not impact the ability of the TSP to meet the intended service. This certification decision is conditional upon to the implementation of corrective actions within 3 months after conclusion of the audit (depending on the type and criticality of the correction(s)). Moreover, the CAB assessing the TSP must meet the specific requirements of EN 319 403, for which reporting requirements are specific to the certification scheme and may be adjusted as necessary – for example, according to the requirements under the forthcoming ETSI TS 119 403-3.

The assessment criteria from EN 319 403 (and, ISO/IEC 17065) set out the requirements that the CAB must examine during the assessment of a TSP, the first of which is to indicate that CABs do not perform (or accept contracts for) audits of TSPs for which they have less than the required competence

The contents of the audit report are expected to contain a list of the standards and publicly-available specifications and/or regulatory requirements against which the assessment is carried out, an account of

[7] Visit https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx for more information about recent, current and ongoing ETSI activities.

the TSP's internal risk analysis, the time it took to conduct the assessment, detailed to the review of documentation, on-site assessment and reporting, as well as additional audit enquiries followed, rationale for their selection and the methodology employed, including any additional methodologies for sampling, were that to be the case of the audit. The results contained within the audit report are expected to provide "sufficient detail to facilitate and support a certification decision", the details of which are laid out in EN 319 403 section 7.4.4.1 *Report contents*.

Problems or other discrepant issues discovered during the assessment are defined as non-conformities. For these instances, the TSP is expected to report pending or performed changes according to the conformity issue during the documentation phase of the assessment. Non-conformities may be resolved with the suspension or termination of the certification or under the auspices of a contractual commitment to corrective actions that would return the TSP to within the scope of conformity to the applicable standards. In consideration of this, the TSP may be conferred one of three designations after the assessment process has concluded: certified, non-certified or passed with pending non-conformities. To be clear, if a TSP does not receive a certification, no additional status called "non-certified" is awarded.

As described in EN 319 403 7.10 *Changes affecting certification*, the changes that may affect certification include (but are not limited to) major changes in TSP documentation (during the first stage of the audit), changes to the TSP's policies, objectives or procedures that affect the trust service(s) offered, relevant security changes to networks and trustworthy systems or new sites providing relevant trust services. In these cases, the TSP must undergo a full re-assessment to determine if it (still) adheres to conformance to the requirements laid out in the respective, appropriate standards and requirements. Responses to any of these non-conformances are described accordingly in ISO/IEC 17065 section 8.10 *Termination, reduction, suspension or withdrawal of certification*. This standard also includes provisions for the reduction of the risk of non-conformities in 9.6 *Internal audits*, 9.7 *Corrective actions* and 9.8 *Preventative actions*, which list (non-explicit) strategies and actions relevant to the identification and remediation of such risks.

One point of interest regarding the ongoing industry discussion about non-conformities (and the necessity of responses thereto) considers the absence of specification for the terms "major" and "minor" as they relate to non-conformities. The definition of a nonconformity (from ISO/IEC 17021) is, generally, "the non-fulfilment of a requirement". A nonconformity could be classified as major under two circumstances: "if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements" or if "a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure…". The functional difference between major and minor, by definition, is its ability to "affect the capability of the management system to achieve its intended results". It is assumed within the wider auditing/audited community that TSPs found exhibiting "minor" non-conformities can be awarded a provisional certification whereas any present "major" non-conformities are grounds for termination of certification pending remedial actions and a renewed full assessment. However, these terms have been debated along descriptive lines: disagreements have arisen between e.g. CABs and browser vendors have no existing avenue for mediation except that which is based on the interpretation of whoever is holding the report. Though both sides of these ongoing large-scale arguments have merits, they can also be seen through the lens of political posturing, and could potentially be resolved in part by clearer, or more granular, distinctions between types (and the severity levels) of specific non-conformities and appropriate responses in the certification process.

Moreover, there is a number of requirements for the training and competence of the audit teams according to EN 319 403, which includes provisions for demonstrated knowledge in technical, regulatory, business, risk, policy and control areas, according to section 6.1 *Conformity Assessment Body personnel* (6.1.2.2 *Training of audit teams*). The competences must be derived according to the general requirements

as described in ISO/IEC 17065 section 6.1 *Certification body personnel*. This includes that the certification body, here interpreted as the CAB, needs to define the scope of competence, training and certification of its auditors and provide for such training, performance testing and monitoring as necessary. As discussed before, however, since ETSI (and by extension ISO) standards often do not expressly cite specific controls or give specific examples for the fulfilment of the standards and requirements, no further explicit directions or documentation are given for the practical training of auditors, harmonised across all CABs in the EU (and beyond).

3.3 WebTrust for CAs assurance audit

WebTrust (Figure 5) is another well-known commercial audit scheme for TSPs and browser vendors. WebTrust assessments are performed by independent accountant firms which are recognized by Chartered Professional Accountants (CPA) Canada. As a rule-based assurance audit, the WebTrust scheme aims to review the implementation and operational effectiveness of controls over a period of time in the past (to make sure the systems have been adequately operating, with the assumption that they will continue to do so). The functional philosophy behind WebTrust is the provision of assurance that a TSP's services have, until the point of time the assessment is conducted, verifiably met a rigorous set of defined criteria. The operation assumption here is that fulfilling a checklist of objectives is the same as fulfilling the obligations to security for which TSPs are responsible in their operations.

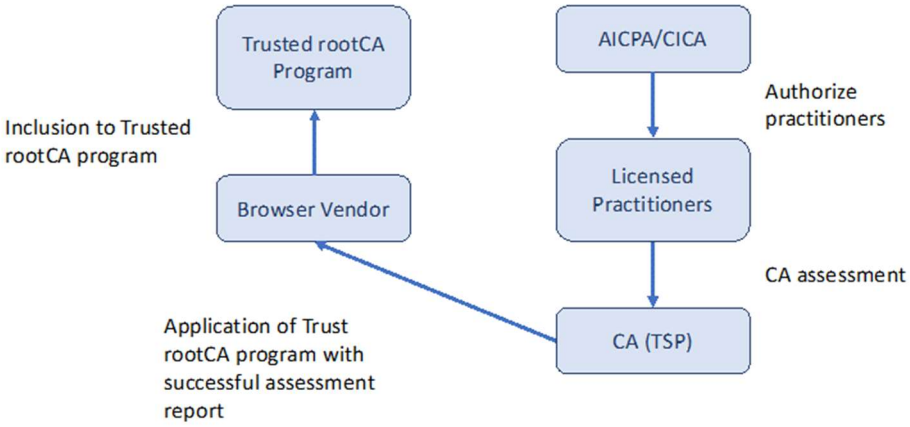

Figure 5: The trust framework of WebTrust for root CA program (based on (Hamaguchi, 2016))

It should be made clear that the WebTrust scheme does not actually meet the requirements of eIDAS conformity assessment bodies in Article 3 (18)[8], "which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides". A CAB, as defined in point 13 of Article 2 of Regulation (EC) No 765/2008 is "a body that performs conformity assessment activities…", according to "a system of accreditation which functions by reference to binding rules, [helping to] strengthen mutual confidence between Member States as regards the competence of CABs and consequently the certificates and test reports issued by them." Additionally, the reference to the term "qualified" as it relates to the TSP and the trust services it provides,

[8] 'Conformity assessment body' is defined in point 13 of Article 2 of Regulation (EC) No 765/2008 as "a body that performs conformity assessment activities including calibration, testing, certification and inspection"

indicates a principal reason for why WebTrust does not align with eIDAS requirements; because there is no current provision for the proper assessment of conformity with the existing standard for QTSPs issuing e.g. QWACs.

3.4 ISO/IEC 27000 series

The ISO/IEC 27000 series represents the information security family of standards, which provides best practices recommendations for the management of information security and covers a wide range of general network and information security concerns. Table 3 outlines the preliminary set of documents in this series.

ISO/IEC 27001 stipulates "the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization". It also encompasses requirements for "the assessment and treatment of information security risks tailored to the needs of the organization. The requirements are generic and are intended to be applicable to all organizations, regardless of type, size or nature".[9] This document requires that management systematically examine security risks inherent to the business in question. Not unlike the ETSI protocols for certification, ISO/IEC 27001 also focuses on the design and implementation of controls to this effect, and the adoption of an overarching management process.

Table 3: ISO 27000 series relevant to this study

STANDARD NO.	TITLE	MOST RECENT
ISO/IEC 27000	Overview and vocabulary	2018
ISO/IEC 27001	Information security management systems - Requirements	2015 (under development)
ISO/IEC 27002	Code of practice for information security controls	2015
ISO/IEC 27003	Guidance	2017
ISO/IEC 27004	Monitoring, measurement, analysis and evaluation	2016
ISO/IEC 27005	Information security risk management	2018
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems	2015
ISO/IEC 27007	Guidelines for information security management systems auditing	2017
ISO/IEC PDTS 27008	Guidelines for the assessment of information security controls	(under development)
ISO/IEC TR 27008	Guidelines for auditors on information security controls	2011

Whereas ISO/IEC 27000 and ISO/IEC 27001 outline foundational elements of ISMSs, ISO/IEC 27002 can be read like a CP concerning a TSPs information security controls. Also important to this study are the recommendations laid out in ISO/IEC 27006, ISO/IEC 27007 and ISO/IEC 27008, which comprise guidelines

[9] cf. www.iso.org

for auditing a TSP's management system and security controls. However, the trust scheme of ISO is very similar and comparable to ETSI certification framework, as is shown in Figure 6.

Figure 6: The ISO trust framework (based on description of accreditation and certification process of the International Accreditation Forum)

It should be made clear, however, that certification against ISO/IEC 27001 plus ISO/IEC 27006 does not require that the CAB has competencies relating to trust services and does not require an assessment that considers if the TSP follows any recognised best practices for the provision of trust services.

3.4.1 New work item (ISO/IEC JTC 1/SC 27)

While there is currently no dedicated ISO standard for PKI, practices and corresponding policy frameworks,[10] ISO is currently in discussion about such a standard as a new work item (ISO/IEC JTC 1/SC 27), tentatively entitled, "Information Technology – Security techniques - Public key infrastructure - Practices and policy framework" (ISO SC 27/2WG4). This new work item proposal on information technology, security techniques, PKI, practices and policy frameworks are, at the time of this draft, presently under development.

The scope of this proposed work item includes the development of a framework of requirements to manage information security for PKI TSPs through CPs, CPSs and, where applicable, their internal underpinning by an ISMS. This requirements framework aims to include the assessment and management of information security risks, which will be tailored to meet the agreed service requirements of its users, as specified through the Certificate Policy. It also aims to help TSPs support multiple CPs. It intends to address the life-cycle of public key certificates, but it is not intended to address authentication methods, non-repudiation requirements or key management protocols based on the use of public key certificates.

Moreover, the new work item will make use of concepts and requirements of an ISMS, as defined in ISO/IEC 27000 and ISO/IEC 27001, respectively. It will also use the code of practice for information security controls, as defined in ISO/IEC 27002. Specific PKI requirements (e.g. certificate content, identity proofing, certificate revocation handling) will, however, not be addressed directly by a generic ISMS; it will in fact depend on the scope of the audit chosen at the beginning of the process. The use of a generic ISMS is extended through the application of PKI service requirements specified in the CP as described in the

[10] A standard does exist, however, which is targeted at the financial sector in ISO 21188.

present document. The planned ISO norm distinguishes between PKI systems used in closed, open and contractual environments. It facilitates the implementation of "operational, baseline controls and practices in a contractual environment". Application of the norm to open or closed environments is not specifically precluded.

3.5 Federal PKI

In contrast to the Trusted List framework of the eIDAS regulation, the US Federal PKI is a bridge CA framework. Central to this trust framework is the Federal Bridge CA (FBCA), which acts as a trust hub for disparate PKI domains (cf. (FPKI, 2015), (FPKI, 2012)). The Federal Policy Management Authority (FPKI Management Authority) is the organization that operates and maintains the FBCA on behalf of the U.S. Government, U.S. Federal PKI Policy Authority (FPKIPA). Figure 7 shows the trust framework of FPKI.

The FBCA is not an autonomous service as such, but rather consists of a framework of specific norms and standards to determine the reliability of CAs, based on a standardized methodology for assessing compliance with these norms and standards, and a cross-certification platform allowing CAs to cross-certify with the US Federal PKI Architecture at seven pre-defined assurance levels. The FBCA functions as a non-hierarchical hub allowing relying parties to create certificate trust paths from their PKI domains back to the PKI domain of the cross-certified CAs, so that the levels of assurance honoured by disparate CAs can be more easily reconciled. The FBCA itself operates under the FBCA CP, which specifies seven different levels of assurance.

All CAs have to demonstrate their compliance with the predefined assurance levels, by regular independent audits in accordance with the published procedure.[11] When a CA cross-certifies with the FPKI architecture, and is an affiliate in good standing, a relying party operating an online application that utilizes digital certificates for electronic identity authentication may choose to trust that PKI's digital certificates at the Level(s) of Assurance asserted by those certificates. The purpose of the FBCA is to ensure that no other trust requirements are needed for the relying party to make that determination. While designed specifically with the benefit to US federal government services, the cross-certification approach is not inherently restricted to any sector, application or domain. In fact, there are additional sectors using the same approach and requesting the same conditions (e.g. SAFE Bio-pharma, etc.).

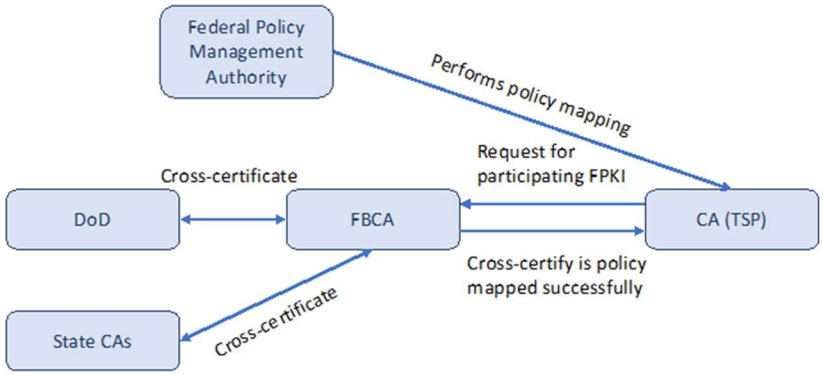

Figure 7: The trust framework of FPKI

Cross-certification with FBCA can demonstrate that the TSP operation and its security level is equivalent to what the US government requires for their PKI system, which warrants harmonization. However, one

[11] For more information, see https://www.idmanagement.gov/fpki-cas-audit-info/

notable problem with the system, as it currently stands, is that it is not updated very often and sometimes includes TSPs that are trusted, although motivation to this level of trust may not be obvious.

3.6 Comparison of CA/B Forum guidelines, ETSI standards and WebTrust audit scheme

The standards that are employed by ETSI are developed by experts from different industries and all requirements from the CA/B Forum and are included in the latest standards (ETSI, 2016a), (ETSI, 2016b), (ETSI, 2016c).[12] We refer to the ETSI approach as distributed because it makes use of a body of individual standards. Some critics of this system cite the “disconnected” nature of the ETSI framework as a downside, citing potential confusion from a reliance on so many external references (the scheme is not self-contained like WebTrust) (Timmerman, 2004). Its distributed nature, however, suggests that the policy is flexible enough to incorporate updated standards at a fairly granular level as ETSI produces them to reflect the needs of the time. In particular, it draws particular focus to the democratic structure of how European norms are drafted and implemented, placing high value on input and consensus from many actors rather than favouring the few.

The criteria in the ETSI standards are also aligned with those of the CA/B Forum guidelines to facilitate conformance to both best practices. Conformance to the requirements described in ETSI standards can therefore demonstrate that the TSP fulfils the required assurance level in order to be trusted by browser vendors and their users, as a product of the work of stakeholders across most or all pertinent industries. This is the primary, generic use case for ETSI standards: to be valid inside the European community for different levels of CPs. An EN 319 403-based conformity assessment scheme, for example, can be used to assess conformance to the CA/B Forum guidelines as well as the ETSI standards. Inclusion in the browsers’ trusted root stores is an additional feature of ETSI certification.

Regarding the frequency of assessment, the ETSI audit cycle is two years, meaning that full assessments are performed every second year, while annual surveillance assessments are performed in between. Ultimately, the ETSI audit may result in a certification that legitimizes a TSP to perform certain activities in the future by assessing if the body is capable and ready to perform those activities. For PTC, the CA/B Forum requires annual audits, whereas in the context of eIDAS, the audit cycle is biennial.

One important aspect and defining feature of the ETSI scheme is the reliance it puts on the competence and autonomy of individual auditors, and the extent to which he or she is afforded the flexibility to make judgments during the audit process, and for its conclusion. On the one hand, more flexibility and trust in the individual auditor reveals a "human weakness" in the trust chain (Timmerman, 2004); a TSP with and overlooked security flaw could go “into the wild” and impact the ecosystem, as with the major breaches of the past. However, this grim prognosis delivers an opportunity for narrowing on and addressing the individual points of weakness along the chain. Specifically, this means that part of the solution to a more dynamic, powerful system lies in the judgment of the auditors themselves and at least a second person (certifier) who reviews the whole process and every single judgement done by the auditor in the certification stage. To this end, more should be done to educate and support these actors. This point is introduced more narrowly in chapter 6 as a pathway to systems improvement and improved global acceptance of eIDAS audits.

Similar to the ETSI scheme (EN 319 403 requires the observation of the past period of time to the previous audit), WebTrust is inherently interested in past performance, meaning that the ETSI certification gives the

[12] It should be noted that whereas the eIDAS Regulation issues legal requirements, ETSI CP are norms (e.g. how to conduct audits via EN 319 403) and are not mandatory for audits pertaining to QWACs under eIDAS. However, the ETSI requirements are mandated by the CA/B Forum.

TSP one or two years in advance to keep going while WebTrust certifies what the TSP did last year (AIM-BEUC Joint Initiative, 2012). It should be considered what a WebTrust auditor does when he or she identifies a fundamental misconduct of the TSP when performing a review of past activities (e.g. ten months ago). It is not entirely clear what happens with the TSP's approval, from a retroactive perspective. In cases such as these, ETSI has been cited as a more advanced system, in which changes to the operations are always considered to the CAB before they are allowed to be implemented and taken into operation.

The trust framework for WebTrust is, at least in hierarchy, comparable with ETSI: Figure 5 lays out the simplified structure for the trust framework, which can be compared with Figure 4 describing the ETSI trust framework. One major difference in the system's organization is in the absence of a "harmonization body". Originally developed by the AICPA and CICA, "the WebTrust program is now managed by the Chartered Professional Accountants of Canada". Public accounting firms and practitioners, who are specifically licensed by CPA Canada, can provide assurance services to evaluate and test whether the services provided by a particular Certification Authority meet these principles and criteria."[13] Since there are no other accreditation bodies responsible for this scheme which could possibly interpret requirements in a different way, harmonization across audits is automatically guaranteed.

Although the WebTrust and ETSI audit schemes are intended to achieve the same objectives, namely to obtain (root and issuing) TSPs' recognition and inclusion by browsers, there are a number of important differences both in the practice of implementing the structure as well as important differences pertaining to the theoretical underpinning of both trust frameworks. WebTrust is a nearly self-contained document that hardly contains any external references, as opposed to ETSI, which refers to an expanding and evolving body of external standards. This allows WebTrust auditors a somewhat more straightforward process by which to conduct the assessment, but critics have, in the past, pointed out that it lacks the durability and flexibility of consensus-based standards which reflect the needs of a larger sample of industry stakeholders. However, recently, WebTrust has surveyed TSPs and browsers for their opinions about possibilities for improving and updating their audit program. In this case, we see some convergence forming between WebTrust and ETSI.

In practice, WebTrust generally employs a comprehensive set of illustrative controls, describing in detail the stated objectives and how a TSP might meet those objectives, often (though not always) in more specific terms than the ETSI audit. More specifically, WebTrust mirrors the exact requirements set forth by the CA/B Forum, adding detailed instructions about how the control objectives might be reached, since this is a primary focus of the audit. This is designed to reduce the probability of human error and to bring added efficiency to the assessment of control objectives. The case can be made, however, that this focus on rules and illustrative controls removes a large degree of the autonomy of the independent auditor to issue an assessment based on his or her professional judgment, a point which will emerge later in this report as a feature of the proposed roadmap towards global acceptance of the eIDAS audits. This study regards the education and capability of individual auditors as integral to the system as a whole; the checkbox approach inadvertently disarms auditors, who should be educated and empowered to think critically and make decisions, as opposed to fulfilling the obligation of making sure a discrete list of illustrative controls is aligned.

Like the ETSI scheme, the WebTrust audit criteria include all defined requirements from CA/B Forum (CPA, 2014)(CPA, 2016). Therefore, conformance to the WebTrust framework can also demonstrate that the TSP fulfils the required assurance level in order to be trusted by browser vendors and their users.

[13] WebTrust: www.webtrust.org/item64428.aspx

3.7 Visual guide to the trust frameworks criteria

Table 4: Comparison between the trust frameworks (based on (Hamaguchi, 2016))

	ETSI	WEBTRUST	eIDAS	FPKI	ISO 27000
Law	Supports eIDAS Regulation	N/A	eIDAS Regulation	e-Government Act of 2002	N/A
Objective	Technical interoperability and trusted third party assessment	Technical interoperability and trusted third party assessment	Legal recognition of electronic trust services	Identity management and trust across organizational, operational, physical and network boundaries	Information security
Governor	ETSI Board	N/A	EU Committee	CIO Council	
Harmonization Body	ETSI ESI	PKI Assurance Task Force	FESA	N/A	
Accreditation Body	National Accreditation Bodies	CPA Canada	NAB	FPKI Policy Authority	National Accreditation Bodies
Conformity Assessment Body	CAB accredited to EN 319 403	Same as above	Conformity Assessment Body	FPKI Certificate Policy Working Group	Conformity Assessment Body
Supporting Technical Standards	ETSI Standards, CA/B Forum: BRG, EVCG + NetSec	WebTrust Criteria	ETSI Standards, CEN Standards	NIST SPs, FIPS 201, FPKIPA Documents	
Assurance to be achieved	Best Practices and Legal Compliance	Best Practices	Legal Compliance	Technical Compliance, Interoperability with FPKI system	Technical Compliance to Management Requirements

4. Comparison of Auditing Standards for TSPs

As discussed in chapter 2, there is no implementing act for the assessment criteria for the conducting of a conformity assessment by accredited CABs (Article 20 (4) in the eIDAS Regulation). However, for cases of assessing QTSPs for QWACs, the usage of ETSI EN 319 401, ETSI EN 319 411-2, supported by ETSI EN 319 411-1 and connected standards, should be expected. A reasonable next step would be to examine these standards and compare them with other mentioned standards, especially with WebTrust as a leading competing audit scheme. This was performed by means of a comparison of the criteria of the mentioned ETSI and WebTrust standards.

A common discussion is about the level of detail of the criteria as they are described in the standards. If requirements are more detailed, the possibility for different assessors to reach the same results would be higher. However, detailed requirements may deter the free interpretation about the fulfilment of the requirements.

Hence, in this report, each of the criteria has been assessed on level of detail. This assessment yields an overview of the level of detail of the above-mentioned ETSI standards and give indication of the degrees of freedom that auditors may be able to interpret differently. It is especially when norms, or the criteria supporting those norms, are not explicit or very detailed, that the auditor will be asked to use his professional judgment for assessing criteria and ultimately making judgments about the control objectives and management systems.

This chapter presents a tabulated assessment that includes the level of detail of the controls of the examined standards, which are qualitatively categorized in one of the three levels, based on (Timmerman, 2004), s indicated below:

- High: The control criteria or evaluation guidance provided is detailed or includes tangible bench-marks. In other words, how a control objective is achieved is considered in addition to what that objective comprises. For example, “Physical barriers are in place (e.g. solid walls that extend from real floor to real ceiling) to prevent unauthorized entry and environmental contamination to the CA’s certificate manufacturing facility.”
- Medium: The qualitative criteria are provided at a relatively high level of detail. How those objectives are achieved, however, is generally less concrete. For example, “Physical protection shall be achieved through the creation of clearly defined security perimeters.”
- Low: Only the control objectives are provided. Commonly, what the control objective is, but not how it is to be or should be achieved. For example, “The integrity and authenticity of the status information shall be protected.”

Although WebTrust contains many illustrative guidance controls in addition to the high-level control objectives, they do not necessarily yield non-compliance when not adhered to, but they do provide a higher level of detail for interpreting the control objective. These controls were, therefore, taken into consideration when evaluating the level of detail of the control objective. Evidently, they provide meaningful tips and guidelines for both the manager implementing a system, and the auditor assessing the (management) system, thereby framing the professional judgment of the auditor. It is for that reason that, even though illustrative controls have no mandatory status, these controls are included in the comparisons throughout this report.

4.1 ETSI requirements

We start with the examination of the level of detail of ETSI standards which could/should be used by a CAB for a conformity assessment of a TSP. The level of detail of the ETSI standards which could/should be used by a CAB for a conformity assessment of a TSP (i.e. the controls of ETSI EN 319 401, ETSI EN 319 411-1 and -2) are listed in the checklist contained in ETSI TR 119 411-4.[14] This checklist provides all requirements identifiers in such a way that it can be used by the TSP itself to prepare for an assessment of its practices against the current standards (i.e. to serve as a basis for a self-declaration) and/or by the assessor when conducting the assessment, for the sake of facility for both the assessor and the TSP being assessed. We use here the expression “detail” exactly as it is used in (Timmerman, 2004) and follow the methodology of (Timmerman, 2004).

Table 5 is a sample (high-order) extract of TR 119 411-4 to help give an idea about the content of the full list. In this sample, the column “CA/B Forum Requirement” is omitted, since it is not relevant to any technical requirement. The column “CA/B Forum Requirement” provides the reference from where the technical requirement originates, when relevant. To indicate the severity of the requirement:

- the term "shall" indicates requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted;
- the term "should" indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

To summarize, the examined ETSI requirements in general are principle-based. Control objectives are stated at the beginning of each section, frequently broken down into more detailed control objectives and enriched with guidelines on what elements should be controlled to cover the objective. However, not all elements are illustrated by measurable controls to validate effectiveness of the control objective. This is also reflected in the fact that level of detail of the majority of these requirements received a score of Medium.

[14] This checklist can be found at https://www.etsi.org/deliver/etsi_tr/119400_119499/11941104/01.01.01_60/

Table 5: High-order extract of checklist ETSI TR 119 411-4

DOCUMENT REFERENCE	REQUIREMENT REFERENCE	SEVERITY	MAIN SECTION	SUBSECTION	LEVEL OF DETAIL
[ETSI 319 411-1]	OVR-5.1-03	should	General provisions on Certification Practice Statement and Certificate Policies	General requirements	High
[ETSI 319 411-2]	OVR-5.1-03	shall	General provisions on Certification Practice Statement and Certificate Policies	General requirements	High
[ETSI 319 411-2]	OVR-5.1-04	shall	General provisions on Certification Practice Statement and Certificate Policies	General requirements	High
[ETSI 319 411-2]	OVR-5.1-05	shall	General provisions on Certification Practice Statement and Certificate Policies	General requirements	High
[ETSI 319 401]	REQ-5-01	shall	Risk Assessment	Risk Assessment	Low
[ETSI 319 401]	REQ-5-02	shall	Risk Assessment	Risk Assessment	Low
[ETSI 319 401]	REQ-5-03	shall	Risk Assessment	Risk Assessment	Low
[ETSI 319 401]	REQ-5-04	shall	Risk Assessment	Risk Assessment	Low
[ETSI 319 411-1]	OVR-5.1-03	should	General provisions on Certification Practice Statement and Certificate Policies	General requirements	High
[ETSI 319 411-2]	OVR-5.1-03	shall	General provisions on Certification Practice Statement and Certificate Policies	General requirements	High
[ETSI 319 411-2]	OVR-5.1-04	shall	General provisions on Certification Practice Statement and Certificate Policies	General requirements	High

4.2 Requirements of WebTrust for CAs

In this section, we examine the level of detail of the criteria in WebTrust[15]. Once again we use the expression "detail" exactly as it is used in (Timmerman, 2004). Table 6 analyses the level of detail concerning the "WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL" (WebTrust EV SSL) (CPA, 2014), and Table 7 analyses the "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security" (CPA, 2016) (WebTrust Principles and Criteria for CAs). The analysis is based on the analysis of the authors following the methodology of (Timmerman, 2004).

Table 6 : Level of detail of checklist for WebTrust principles and criteria for CAs (based on (CPA, 2016))

CRITERION		LEVEL OF DETAIL
1.1	Certification Practice Statement (CPS)	Medium
1.2	Certificate Policy (CP) (if applicable)	Medium
2.1	Certification Practice Statement (CPS) Management	Medium
2.2	Certificate Policy (CP) Management (if applicable)	Medium
2.3	CP and CPS Consistency (if applicable)	Medium
3.1	Security Management	High
3.2	Asset Classification and Management	Medium
3.3	Personnel Security	High
3.4	Physical and Environmental Security	High
3.5	Operations Management	Medium
3.6	System Access Management	High
3.7	Systems Development, Maintenance, and Change Management	High
3.8	Disaster Recovery, Backups, and Business Continuity Management	High
3.9	Monitoring and Compliance	Medium
3.10	Audit Logging	High
4.1	CA Key Generation	High
4.2	CA Key Storage, Backup, and Recovery	High
4.3	CA Public Key Distribution	High
4.4	CA Key Usage	High

[15] Principles and Criteria, http://www.webtrust.org/principles-and-criteria/item83172.aspx

4.5	CA Key Archival	High
4.6	CA Key Destruction	High
4.7	CA Key Compromise	High
4.8	CA Cryptographic Hardware Life Cycle Management	Low
4.9	CA Key Escrow (if applicable)	High
4.10	CA Key Transportation (if applicable)	High
4.11	CA Key Migration (if applicable)	High
5.1	CA-Provided Subscriber Key Generation Services (if supported)	High
5.2	CA-Provided Subscriber Key Storage and Recovery Services (if supported)	High
5.3	Integrated Circuit Card (ICC) Lifecycle Management (if supported)	High
5.4	Requirements for Subscriber Key Management	High
6.1	Subscriber Registration	High
6.2	Certificate Renewal (if supported)	High
6.3	Certificate Rekey	High
6.4	Certificate Issuance	High
6.5	Certificate Distribution	High
6.6	Certificate Revocation	Medium
6.7	Certificate Suspension (if supported)	High
6.8	Certificate Validation	High
7.1	Subordinate CA Certificate and Cross Certificate Lifecycle Management	Not relevant for QTSP

Table 7: Level of detail of checklist for WebTrust EV SSL (based on (CPA, 2014))

CRITERION	LEVEL OF DETAIL
Business practices - Disclosure	Medium
Key generation ceremonies	High
EV SSL subscriber and certificate content profiles	High
EV SSL certificate request requirements	High

Information verification requirements	High
Certificate revocation and status checking	High
Employees and third parties	Medium
Data records	High
Audit and legal	Medium

4.3 Gap analysis: A comparison of ETSI and WebTrust

Finally, we directly compared the analysis of checklist of ETSI TR 119 411-4 with "WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security" (CPA, 2016) combined with (CPA, 2014). Here, rather than a mapping and comparison of the hundreds of individual requirements in detail, we were interested in whether there may be significant differences in the level of detail between the standards that could influence acceptance. The results of this comparison survey can be found below in Table 8. If the level of detail is not equal, then the name of Webtrust or ETSI is indicated in Table 8.

Table 8: High-order comparison of the level of detail of ETSI and WebTrust requirements

MAIN TOPICS COVERED BY WEBTRUST	CORRESPONDING TOPICS COVERED BY ETSI	DETAIL LEVEL
Certification Practice Statement (CPS)	General provisions on Certification Practice Statement and Certificate Policies General requirements Certification Practice Statement Requirements Certificate Policy name and identification PKI Participants Certification authority Subscriber and subject Others Certificate Usage	Equal
Certificate Policy (CP) (if applicable)		Equal
Certification Practice Statement (CPS) Management		Equal
Certificate Policy (CP) Management (if applicable)		Equal
CP and CPS Consistency (if applicable)		Equal
Security Management	Security Management, Risk Assessment, Information Security Policy	WebTrust
Asset Classification and Management	Asset management	Equal
Personnel Security	Human Resources	Equal
Physical and Environmental Security	Physical and environmental security	Equal
Operations Management	Operation Security, Management and Operation	ETSI
System Access Management	Access Control, Physical security controls,	Equal
Systems Development, Maintenance, and Change Management	Operation Security, Management and Operation	Equal

Disaster Recovery, Backups, and Business Continuity Management	Facility, management, and operational controls, Business Continuity Management, Compromise and disaster recovery	Equal
Monitoring and Compliance	Compliance	Equal
Audit Logging	Facility, management, and operational controls, Audit logging procedures	Equal
CA Key Generation	Technical security controls, Key pair generation and installation	Equal
Key generation ceremonies	Technical security controls, Key pair generation and installation	Equal
CA Key Storage, Backup, and Recovery	Technical security controls, Private key protection and cryptographic module engineering controls	Equal
CA Public Key Distribution	Technical security controls	Equal
CA Key Usage	Technical security controls	Equal
CA Key Archival	Technical security controls	Equal
CA Key Destruction	Technical security controls	Equal
CA Key Compromise	Technical security controls	Equal
CA Cryptographic Hardware Life Cycle Management	Technical security controls	ETSI
CA Key Escrow (if applicable)	Technical security controls	Equal
CA Key Transportation (if applicable)	Technical security controls	Equal
CA Key Migration (if applicable)	Technical security controls	Equal
CA-Provided Subscriber Key Generation Services (if supported)	Certificate Life-Cycle operational requirements	Equal
CA-Provided Subscriber Key Storage and Recovery Services (if supported)	Certificate Life-Cycle operational requirements	Equal
Integrated Circuit Card (ICC) Lifecycle Management (if supported)	Certificate Life-Cycle operational requirements	Equal
Requirements for Subscriber Key Management	Certificate Life-Cycle operational requirements	Equal
Subscriber Registration	Identification and Authentication	Equal
Certificate Renewal (if supported)	Certificate Life-Cycle operational requirements	Equal
Certificate Rekey	Certificate Life-Cycle operational requirements	Equal

Certificate Issuance	Certificate Life-Cycle operational requirements	Equal
Certificate Distribution	Certificate Life-Cycle operational requirements	Equal
Certificate Revocation	Certificate Life-Cycle operational requirements	Equal
Certificate Suspension (if supported)	Certificate Life-Cycle operational requirements	Equal
Certificate Validation	Certificate Life-Cycle operational requirements, Facility, management, and operational controls	Equal
Subordinate CA Certificate and Cross Certificate Lifecycle Management	Certification Practice Statement requirements, Certification Authority,	WebTrust
Employees and third parties	Human Resources, Internal organization	Equal

From the point of view of a TSP, WebTrust Principles and Criteria for CAs (CPA, 2016) is more or less equivalent to ETSI EN 319 401 and WebTrust Principles and Criteria for CAs – SSL Baseline with Network Security combined with WebTrust Principles and Criteria for CAs (CPA, 2016) is more or less equivalent to ETSI EN 319 411-1. By and large, the requirements from the ETSI standards under consideration can be found in the world of WebTrust and vice versa.

The CA/B Forum[16], as a voluntary organization comprising major browser vendors and TSPs, has specified guidelines for TSPs: Extended Validation Guidelines (CA/Browser Forum, 2012), Baseline Requirements (CA/Browser Forum, 2017) and Network and Certificate System Security Guidelines (CA/Browser Forum, 2013). These guidelines are for the TSPs to know what they have to do, but they are not necessarily requirements for achieving inclusion in the browsers' root stores. That is to say, it is not sufficient as a stand-alone audit, but indirectly, via ETSI or WebTrust, the TSP must fulfill all of the requirements. The browsers have policies and procedures that the TSPs must comply with in order to be included; in the various root store policies is stated that the TSP must be compliant with them in order to achieve inclusion.

The ETSI standards include requirements from the above three guidelines, which are covered in the EN 319 4xx series documents. Moreover, WebTrust has adjusted its requirements and specifically has adopted the (CPA, 2011) and (CPA, 2014) to meet the CA/Browser Forum Baseline SSL requirements.

According to both the in-depth technical analysis of this and other studies, as well as the judgment from industry experts, the WebTrust audit scheme is more or less equivalent to the ETSI audit scheme in purpose and outcome. By and large, the requirements from the ETSI standards under consideration for the assessment of TSPs can be found in the world of WebTrust and vice versa. Likewise, the degree of detail in the ETSI standards considered above and for WebTrust are also comparable. Therefore, from the generalised point of view, there is no reason to prefer ETSI or WebTrust.

WebTrust assessments are performed by independent accountant firms, which are recognized by CPA Canada. That is to say, if the WebTrust scheme is compared with the ETSI scheme, CPA Canada can generally be regarded in parallel as an accreditation body. On the other hand, assessment and certification in accordance with ETSI standards are often performed by a CAB accredited by a NAB (as set out in the previous chapter). This scheme is similar to the ISO certification scheme. Capabilities of CABs are ensured

[16] CA/B Forum web page: https://cabforum.org/

by the NABs, and the NABs are regulated by European Co-operation for Accreditation (EA). In this case, the ETSI scheme stands out as a more regulated environment, with bodies in place to oversee the full length of the trust chain, from the highest level of administration down through each individual TSP. While the two schemes look very similar, ETSI is characterized by this higher level of organization. The ETSI trust framework can also be considered more transparent, a characteristic typically seen as valuable across all levels of the ICT industry, since all rules for the assessment are published and publicly accessible.

The level of detail of the requirements as they are described in the criteria in auditing is more important in an ETSI driven world. If the criteria include more detailed requirements, the reproducibility of the audit result would be high (even among different CABs, which are accredited by NABs within different Member States). This means that the possibility for different assessors to reach the same results would be higher when more detailed requirements are included. It does not mean the ETSI requirements are less complete, effective or comprehensive criteria, but this difference about the detail levels may cause different assessors (CABs) to deliver different decisions when assessing the same TSP according the ETSI standards.

5. QWACs Recognition and Visibility

In today's internet, browsers are necessary for providing access to the world wide web, and to this end, as the gate-keepers of information and the secure transmission thereof, browsers wield significant weight both in how relying parties and end users experience the deployment of certificates, and also internally to the industry.

With this in mind, eIDAS audits, which are foundational to the European trust scheme, require the successful deployment of QWACs into a healthy and developing digital market, here in Europe and abroad in the wider digital world. A most notable area that needs to be addressed in order to facilitate the wide spread and use of the QWACs lies in discussions with major browser vendors, who operate the largest public-facing vehicle for website authentication certificate usage and European counterparts, i.e. in ETSI, ACAB'c and other boards and agencies that exist to protect and strengthen the interests of the EU in the global community.

This assessment views the promotion of QWACs at a high level; standards themselves can be written to bridge technical gaps (an important point that will be covered in the roadmap), but if the system for trust supersedes the a priori value of the (auditing) system in question, the marginal utility of QWACs will in fact decrease. It is the task of all stakeholders of this effort to engage in the promotion of QWACs at the same time that the audit scheme is tightened in language and in scope of the utility and value TSPs and browsers place in it.

5.1 Visualization and visibility

It is no exaggeration to say that, without the help of various tools like indicators on the browser user interface (UI), the average (i.e. technically inexperienced) internet user would not be able to determine whether or not a website is secured by a corresponding valid QWAC. For example, the verification step in which the TSP issuing a website authentication certificate was granted the "qualified" status requires that the TSP be identified by reading and understanding the certificate, followed by a check that this status is included in the trusted list of the EU Member State in which the TSP is located. It is by no means self-explanatory for the average end-user to know about, let alone to locate, peruse and interpret this list. Moreover, trusted lists are primarily machine-processable documents (in XML); the legal entities "behind the scenes" are often hidden behind trade names. In the current configuration of the trust service environment (not only in Europe, but in the rest of the world), users will find it difficult to mark the distinction between qualified and non-qualified trust services that any one single qualified TSP may provide.

Web browsers have a special and important role to play here. Evidence from a number of studies demonstrates that the average user has been educated (through the use of various web browsers active on the market) in recent years in such a way that he or she has come to expect to see various indicators (e.g. a URL with "https", a green bar or padlock symbol, etc.) guaranteeing (by means of a certificate) the security of the website currently open. More informed users may also note the difference in the web browser UI when a webpage is secured by an Extended Validation (EV) certificate (as opposed to e.g. a Domain Validated (DV) certificate). Until very recently, it appears that one could assume that this has more or less become established, and browser providers would continue to handle security visibility in this way. However, during the drafting of this study, the landscape has already changed with the latest versions of Chrome and iOS, Apple's mobile operating system. It appears that some browsers will change their UI and

not indicate the use of EV certificates anymore. This is one area to keep a close eye on over time and is the basis for a strong set of recommendations in the following chapter.

5.1.1 What we have now: No industry consensus on standards for UI security indicators

Figure 8 gives a sample of the ways in which security is denoted by different browsers in different contexts. While there is generally a hierarchy for UI marking (in so far as DV and EV certificates generally use different indicators), there are different approaches between the browsers and between individual browsers' approaches to the UI that the argument has surfaced at trust service conferences and workshops[17] in the past several years in favour of unifying the browser iconography of security. The lack of consistency among browser UI is and has long been a persistent challenge, and often appears as granular indications of four states of security: unencrypted, Domain Validated (DV), Organization validated (OV) and Extended Validation (EV). This can be problematic for several reasons, namely that criminal threats can easily hide behind a DV certificate and because DV certificates have exploded into popularity, accounting for a majority of website encryption, a problem eIDAS both sought to and has the capacity to address. However, individual browsers have frequently changed their own UI, and it has been claimed that users cannot keep up. Most mobile devices do not even show a symbol for encryption and, as a result, users can be confused about how to read the browser UI and determine the safety of their online behaviour.

To date, however, despite lengthy industry discussion, no streamlining of these images or texts has taken any public shape or direction.

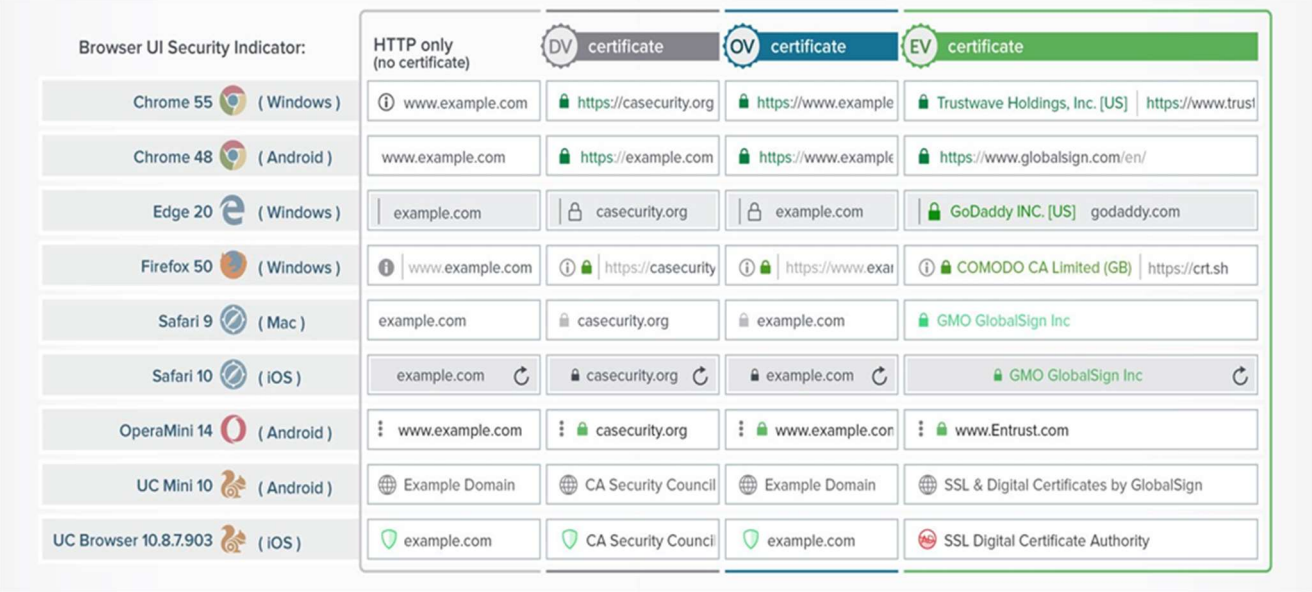

Figure 8: Examples of browser UI for SSL/TLS encryption across device (Source: Security Council (CASC) May 2017 CA)

5.1.2 The future of browser security UI

Google has chosen to follow a different path with the Chrome browser. While aggressively promoting HTTPS web encryption in the last few years, the Google Chrome security team has come to distrust CAs and other "trusted third-parties". In October 2017, in fact, Google began transitioning to a mandatory policy of "Certificate Transparency" (CT), opening the way for an online community of open certificate logs, monitors and auditors to provide near real-time validation of certificates. This push away (Fiedler, 2014)

[17] E.g. CA Day Berlin 2017 & 2018, CA/B Forum meeting (Taipei), etc.

from the certificate authority-based infrastructure relies on disintermediated – so-called "qualified" – certificate logs[18] for SSL/TLS end-entity certificates. Under the rules of this new "public" trust framework, if a TSP does not include a certificate in the CT log server, it will not be trusted by Chrome or, recently, by Apple's Safari browser. As a logical consequence, Google has since banned the green bar in the Chrome UI that use to indicate the deployment of an EV certificate (though Chrome 70 still has an EV indicator by displaying the company name on the left-hand side of the URL bar). The TSP community and representatives from other leading browsers have been public and vocal against this latest measure to distrust trusted third parties and, especially, to simplify the UI in such a way that they claim undermines long-vetted and practiced public understanding of web security features like the padlock and green URL bar.

The Chrome browser has certainly introduced a number of radical changes to the web and user interaction with the internet, and the Chrome security team is considering yet another controversial initiative: fundamentally rethinking URLs and showing information in the address bar. While the Chrome security team does not presently believe that URLs work well conveying website identity, Google plans to move "toward a place where web identity is understandable by everyone – they know who they're talking to when they're using a website and they can reason about whether they can trust them." However, this will mean substantial changes in how and when Chrome displays a URL.

It is therefore by no means clear what web browsers will show in their UI in the coming months, let alone in the coming years. While in a world of different certificates (e.g. EV certificates and QWACs), it seems from the plurality of industry voices both reasonable and preferable to be able to recognize these differences when visiting a web page secured by a certificate; today there does not seem to be any activity by browser vendors that supports this conviction. Instead there are grounds to assume that browser vendors, especially Google, are likely to define, on their own, which websites they choose and refuse to render.

5.1.3 Difficulties inherent to a separate QWAC UI

One could argue that because browsers are extendable, it should be possible to develop extensions that indicate on the browser UI whether a website is secured (and, specifically, by a QWAC) or not. The modern extension frameworks of Firefox and Chrome – and therefore also Opera, Edge and Vivaldi, which mimic Google Chrome's extension architecture (at least at the time of this writing) – allow the display of buttons and/or icons on the browser UI. This could be, for example, a green or red button on the right-hand side of the address panel or even to open a new small browser window that displays some explanatory information. However, extensions are not able to assume control of the normal behaviour of the browser, a rule defined by the browser vendors. If the browser indicates that a user should not trust an SSL/TLS connection because the corresponding SSL/TLS certificate cannot be found in so called "qualified" certificate transparency (CT) logs for SSL/TLS end-entity certificates, this cannot be changed by modern extensions. In the case of a QWAC that cannot be found in the CT logs, this would trigger trust concerns for users, even if the extension shows that the website uses a QWAC. Moreover, if the browser should refuse to render websites in which the corresponding SSL/TLS-certificate cannot be found in so called "qualified" CT logs for SSL/TLS end-entity certificates, then the proposed extensions will either be useless or need to open a second window, which would then render the previously-refused website. Unfortunately, it is difficult to imagine the scenario in which any customer would put much trust in such a solution.

Moreover, both on desktops and mobile devices, there is currently no way to directly provide information about a given SSL/TLS connection to extensions based solely on modern extension frameworks. This

[18] The term "qualified" in reference to Google CT must not be conflated or confused with eIDAS "qualified".

implies that the evaluation of the corresponding certificates and the validation of QWACS must be implemented outside such an extension, i.e. by so called native messaging (s.(Mozilla, 2018)), which leads to additional security questions.

5.1.4 The EU trust mark as a possible branding tool

Visualizing whether a website is secured by a QWAC is only one side of the coin. The visibility of the eIDAS framework and of QTSPs and confidence in websites using QWACs is another. The confidence of the average user to trust a website (e.g. the websites of European banks) can be based on the use of QWACs.

One of several building blocks of the EU to support the visibility of eIDAS system of QTS in the market is the introduction of the EU trust mark (EU Commission, 2015) and its direct linking to the trusted lists. The rules for the use of trust mark, as well as the specifications relating to the form of the EU trust mark for qualified trust services are set in the eIDAS Regulation (EU Commission, 2014) and the above-mentioned implementing regulation (EU Commission, 2015). The trust mark is intended to give reassurance to customers about the confidence they can have in a certain TSP and, by extension, the area of the web they are visiting, should it be secured with a QWAC. Once a TSP is granted the qualified status (and such status being indicated in the trusted list), it may use the EU trust mark to indicate in a simple, recognisable and clear manner the QTS they provide. When using the trust mark for QTS, QTSPs need to ensure that a link to the relevant trusted list is made available on their website.

5.2 Getting browsers on board

The following section summarises key assertions presented in a paper entitled “Trust Service Provider Technical Best Practices Considering the EU eIDAS Regulation (910/2014)”, which was developed in mid-2017 by representatives from the leading browsers: Apple, Google, Microsoft and Mozilla.

A major point leading the report focuses on the need to look beyond the scope of what European national or supranational governments can accomplish. While regulatory options do exist for the management of planned activities and institutionalized learning behaviours, the eIDAS regulation expressly stipulates that industry-led initiatives are not only an appropriate strategy, but a desirable one as well. In specific the regulation stipulates that “Recognizing that ‘best practices in the field’ change over time, Recital 67 in the Regulation considers industry-led initiatives to define appropriate best practices”. This is, in effect, because the field of ICT has a propensity towards significant and frequent change. This point suggests the significance of its own influence on the recommendations that this study makes towards meeting its goal (see Chapter 6 for the road map).

While the legislative course might not be a match in speed for developments in technology, market tools (broadly speaking, companies and specialist industry groups that comprise said digital ecosystem) might be successfully interlinked to maintain the demand for cryptographic products and strategies, for the purpose of combating cybercrime as well as to modernize government and civil applications. It also supports the idea that key industry players like the browser vendors have a significant role to play.

This report provides an example for convergence or overlap between eIDAS and industry efforts to make available TSP security across-the-board. This is achieved by means of best practices which are themselves not necessarily addressed in Implementing Acts on electronic trust services.

While there are a number of representative requirements for each major trust framework, there still exist discrepancies between the standards set out for PTC and those for QWACs under eIDAS. Figure 9 shows the relevant gaps that exist between requirements for CA/B Forum PTC certificates and those for QWACs.

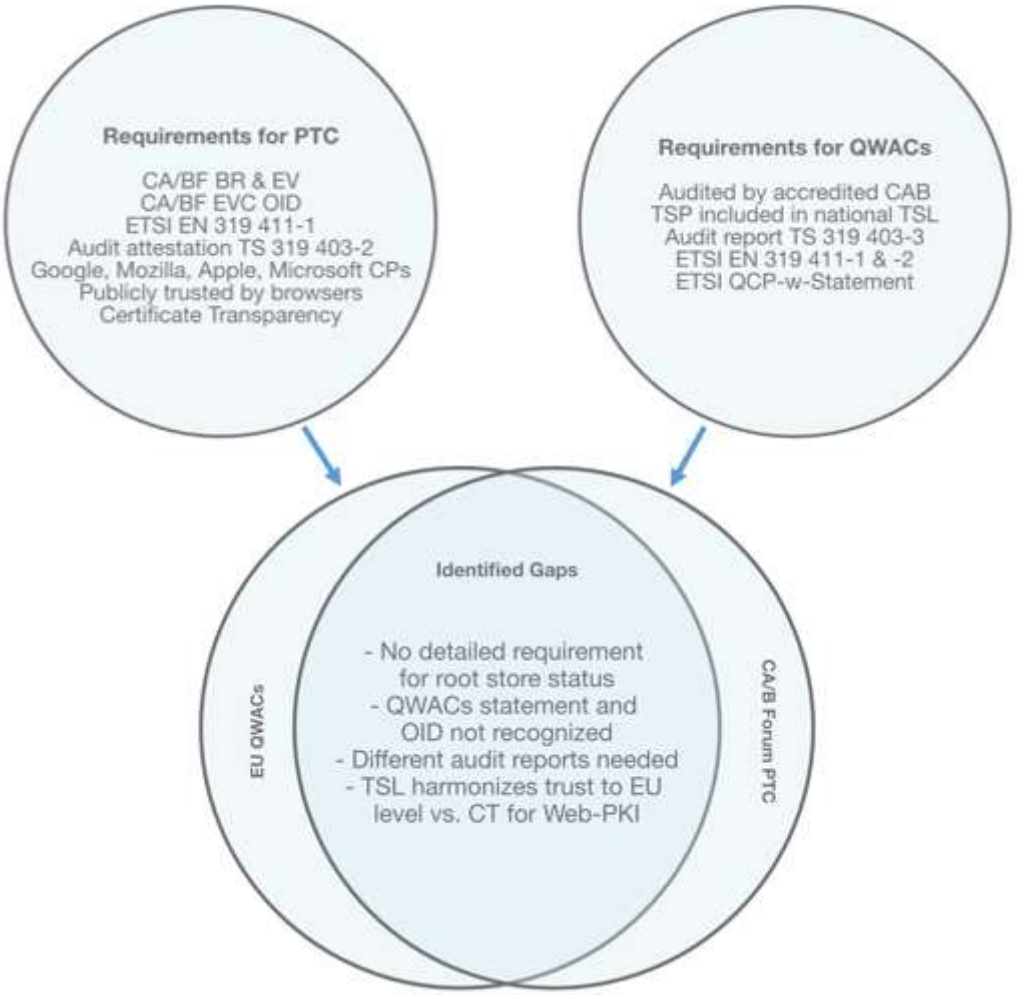

Figure 9: Requirements for PTC and QWAC (and identified gaps)

The TSP best practice report also describes what defines an "incident", and lays out the steps necessary or industry-accepted standards for appropriate response behaviour to such deviations in accepted normal operations by TSPs:[19] “An incident is any event, situation, or circumstance that has, could have, or might cause the TSP to operate outside the requirements laid down by the Certification Authorities/Browsers (CA/B) Forum Baseline Requirements or Extended Validation (EV) Guidelines, Root Store Policies, Audit Requirements, or other security relevant obligation”. This definition helps to establish a baseline for what "acceptable" or "normal" TSP operational behaviour looks like, in order for incidents to be identified and appropriately addressed.

Although little is written in the current draft of the report about the mechanics of incident handling, it is expressed in no uncertain terms how important incident-reporting is, as well as establishing intelligible

[19] It should be noted that these guidelines or recommendations for security best practices can be observed without specific reference to any technology to lead the way. This point is meant to suggest that, while, for example, Google can be part of the contributors to these sets of guidelines for TSPs, trying to force an industry conversion to certificate transparency (CT) has no real bearing on e.g. certificate lifecycles and etc., or the reporting requirement for TSPs that experience an incident.

protocols for following up.[20] It appears that incident-reporting is one of the best ways that the system itself can maintain a consistent level of ecological security; unfortunately, it is a reactive, rather than a preventative response to security threats. It also seeks to minimize damage from breaches and other attacks with e.g. a 72-hour maximum requirement for reporting and response, it does not offer a way to prevent damage from occurring.

There is also a variety of agents to whom the TSP needs to report (and thus, have an appropriate communications plan for reporting), including auditors and supervisory bodies, but especially to the root store operators, a point which diverges somewhat from the overall hierarchical trust framework currently employed within the eIDAS environment.

Another notable message from this study is the advice from the browser community that TSPs undergo audits with a frequency of no less than one per year, which indicates a convergence with the WebTrust requirement of an annual auditing requirement. In 2015, ETSI changed the audit cycles from three to two years (see ETSI EN 319 403). The best practices study makes specific reference to this ETSI audits cycle of two years, based on the eIDAS Regulation, which stipulates that a full conformance audit, rather than a surveillance audit, would be necessary to constitute the successful completion of an annual audit in this case. This presents an opportunity for both ETSI and eIDAS to close a gap that currently exists in strong audit requirements as perceived by the browser community.

Furthermore, "if an Auditor finds non-compliance with Audit Criteria, the Auditor should provide a qualified report that indicates the controls that failed. If there are any changes in the certification status of a TSP, the TSP should notify Root Store Operators immediately". This statement indicates a divergence in stated policy from e.g. ETSI audit standards, and the best practices set forth by the lead browser community. The fundamental difference is in the inroads of communication through which the root store operators are involved in the audit process. In this case, deficiencies in an audit report are suggested to be notified by the TSP to the root store operator in addition to the requirement that they advise the supervisory body (as required in eIDAS Article 19). A point-in-time audit statement may be used to address a TSP that has rectified said deficiencies, but this only validates a TSP's practices on that particular date. Indeed, it seems that regular audits, supplemented with these spot checks for interim inadequacies, are a good way to manage the ecosystem.

As reaction to browser requirements, in July 2018, ETSI also published technical specification TS 119 403-2 (Additional Requirements for Conformity Assessment Bodies Auditing Trust Service Providers that issue Publicly-Trusted Certificates), with the expectation that it would lead to the preparation of audit reports that are more compliant with the browser requirements, although the reports are not required to report publicly about any details of instances of non-compliance. Section 4.2 Audit Frequency states both that, “a full-surveillance audit shall be conducted no less frequently than annually” and that, “updated audit information shall be provided no less frequently than annually” (see ETSI EN 319 403, clause 7.4.6). In addition, a current CA/B Forum ballot is under preparation to make the requirements from TS 119 403 mandatory for all ETSI audits for PTC.

Incidentally, and in consideration of appropriate management systems, the study in question also suggests that “the CA's Certificate Policy (CP) and Certificate Practice Statement (CPS) must provide enough detail to allow third parties to assess how TSPs enforce imposed requirements”. This is a particularly important point, which specifically addresses the intelligibility of the CP and CPS of a TSP to third parties. A CP or CPS

[20] This comment may be updated after 14 October 2018, after which the latest approved ballot will take effect.

which only states that it meets CA/B Forum's Baseline Requirements (an industry "open secret" that many, if not most, CPs today are a copied verbatim from the BR) is not sufficiently detailed enough.

Lastly, for the purposes of this study, an interesting point was made concerning liability: the "inability to update software due to insufficient engineering resources, contractual barriers, reprioritization, or other delay is not a valid reason for non-compliance". This presents an interesting economic approach to the security ecosystem problem. It is worth discussing this statement as a theoretical end game in economic terms e.g. what happens if it becomes too financially onerous for a large company providing certificates to perform critical updates. Whereas small holes in the TSP infrastructure can be mended quickly by other TSPs issuing cross-over certificates, security measures should be in place to deal with a hypothetical end-of-days event, should a "too big to fail" TSP cease to offer continuity. To illustrate, before the 2008 global financial collapse, the collapse of large, global financial institutions was unthinkable. It is perhaps worth exploring the possibility of ecosystem-wide failure scenarios and draft a body of documents which can help identify and reduce such risks. A robust audit scheme will help curb the possibility of these kinds of events.

It should be noted that there has been criticism on the report from industry experts, which includes the focus on root store operators – as bodies which see themselves as responsible for policing the operation of TSPs – rather than a closer focus on the role of eIDAS regulatory requirements. Secondly is the section about Certificate Transparency, which suggests that all PTC should be published to a public domain, a point which avoids taking into account any restrictions which might apply under the rules of the European General Data Protection Regulation (GDPR), which went into effect in May 2018. As a final note, some experts have agreed that all the security requirements addressed in this study can be comfortably covered by the current version of ETSI EN 319 411-1.

However, it appears that the recommendations issued by the browser community in this study have regardless made some compelling suggestions about convergences and divergences between audit requirements on the books and best industry practices, a number of which this study moulds into the language of recommendations in the roadmap in Chapter 6.

6. Conclusions and Recommendations (Road Map)

From our preliminary conclusions and based on the comparative analysis specifically between the eIDAS regulatory framework and the ETSI and WebTrust audit schemes, we can offer the following recommendations as a way forward for the eventual, enhanced global acceptance of an audit scheme under the eIDAS Regulation. The recommendations can be separated into three basic categories of action: 1) making improvements to the existing scheme based on ETSI EN 319 4xx, 2) creating a branding and public usage strategy for QWACs usage, in part by creating value for the EU trust mark and enforcing it by law and 3) continuing to foster relationships and cooperating closely with browser vendors for better acceptance.

Annex A includes diagrams to visualize the predicted effort required to carry out actions in each of the recommended direction as a result from the assessment made by experts in the context of this report.

6.1 Improving the audits, top down

6.1.1 Harmonization of the conformity assessment scheme

As already discussed, the eIDAS Regulation does not place any restrictions on the conformity assessment scheme beyond its fit into the general regulatory framework of conformity assessment in Regulation (EC) No 765/2008. It is up to the supervisory body to specify any requirements for CAB accreditation against any specific audit scheme. Nearly all supervisory bodies have adopted the use of EN 319 403. Without the adoption of a scheme aimed specifically at trust services, this is may be no assurance that the CAB has the appropriate procedures and competencies for the audit of trust services. The eIDAS Regulation does not impose any conformity assessment criteria beyond the requirements of the Regulation. There is no requirement for assessment against recognised best practices for trust services.

Some of the publicly-available eIDAS audit attestations do not contain the minimum-required information, which are required to assess the trust status of a TSP. In fact, many appear untrustworthy and cannot be downloaded from a QWAC-secured website. In comparison with the WebTrust audit scheme, these particular deficiencies of the eIDAS audit come into focus. According to interviewed experts, a comparison of several audit reports from different European TSPs and CABs reveals notable dissonance.

Moreover, the decision regarding the qualification of the TSP and its trust services is made by the SB that verifies compliance with the requirements laid down in eIDAS Regulation. However, the decision regarding the specific practices used for qualification of the TSP is made by the SB. There are no defined requirements on the use of best practice standards across the EU. This may result in inconsistencies in the qualification of TSPs in different countries and may lead to a non-harmonised trust service market, facilitating the rise of doubts about the quality of QTSP and the provided QTS, hence also the QWACs.

Therefore, there is need to define a harmonised conformity assessment scheme against which CABs would be accredited and the QTSP/QTS certified in order to verify conformance to the eIDAS Regulation requirements. This harmonised conformity assessment scheme would ensure that the eIDAS requirements are satisfied, while at the same time meeting the requirements of other communities like the CA/Browser Forum, browser vendors and application providers. This process would involve the Supervisory Bodies of the MS as key contributors towards the specification of this conformity assessment scheme.

There is need to agree upon and define a harmonised conformity assessment scheme against which CABs would be accredited and the QTSP/QTS assessed in order to verify conformance to the eIDAS Regulation requirements. Such a process would involve all the stakeholders – EA, ETSI, EC, ENISA, SBs – which would participate from the specification till the enforcement of such a scheme.

One possible way forward is to map the ETSI audit scheme with the ISO 27000 series. However, used alone, this does not include best practice for trust services and does not ensure that the auditor has the necessary competencies to evaluate the specifics of trust services. ISO/SC27/WG4 has started a new work item, entitled "Public key infrastructure – Practices and policy framework". To integrate the set of ETSI documents into the ISO framework can help eIDAS achieve better acceptance, but the quality of the ISO audit practice in the field is not (yet) defined appropriately.

The current list of accredited CABs in the EU is not frequently updated,[21] potentially causing some confusion. It is proposed as a relatively simple step to keep a centralised list of all accredited CABs, where it will be clearly indicated whether a CAB has been accredited under ETSI EN 319 403 by a NAB and whether it has been accredited in line with the ETSI standards concerning the certification scheme in order to be recognised also by the CA/B forum and the browsers. This list should be regularly updated and provide a higher level of confidence. A list with all international licenced auditors is maintained by WebTrust website.[22]

A centralised list of all accredited CABs should be maintained (by the European Commission) and regularly updated, where it will be clearly indicated whether a CAB has been accredited under ETSI EN 319 403 by a NAB and whether it has been accredited in line with the ETSI standards concerning the certification scheme in order to be recognised also by the CA/B Forum and the browsers.

6.1.2 Standardisation of auditor requirements

This study regards the skills and competences of individual auditors as integral to the system as a whole; the auditing scheme lies in the judgement of the auditors themselves and, their ability to make decisions. While ETSI EN 319 403 is widely adopted, it is not universally done so as no single conformity assessment scheme is required. eIDAS Regulation is fundamentally technology-neutral, the requirements for the use of state-of-the-art technology to achieve control objectives, defined according to ETSI EN 319 411, are not equally recognized or even known to all accredited CABs. In principle, since NABs interpret the implementation of the eIDAS Regulation, possible complications may arise for the maintenance of broader ecosystem-wide security and also the market accessibility of TSPs.

Moreover, there is a number of requirements for the training and competence of the audit teams according to EN 319 403, which includes provisions for demonstrated knowledge in technical, regulatory, business, risk, policy and control areas, according to section 6.1 *Conformity Assessment Body personnel* (6.1.2.2 *Training of audit teams*). The competences must be derived according to the general requirements as described in ISO/IEC 17065 section 6.1 *Certification body personnel*. This includes that the certification body, here interpreted as the CAB, needs to define the scope of competence, training and certification of its auditors and provide for such training, performance testing and monitoring as necessary. As discussed

[21] The most recent version of this list can be accessed at https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation.
[22] http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx

since ETSI (and by extension ISO) standards often do not expressly cite specific controls or give specific examples for the fulfilment of the standards and requirements, directions should be given for standardisation of auditor requirements across all CABs in the EU (and beyond). These issues continue to be a challenge because of the lack of requirements for adopting consistent best practices.

Therefore, providing specific auditors requirements would help to eliminate some degree of human error and to bring added efficiency to the verification of the control objectives as well as facilitate the exchange of experience and practical examples from the field.

It is recommended that ENISA, in cooperation with ETSI and CEN, develop and publish a comprehensive set of auditors' requirements together with best practice examples from the field.

6.1.3 Further optimization of ETSI standards

The ETSI Certification Policies 319 411 have developed into good frameworks over the past 15 years and have been well-suited to both eIDAS "qualified" and "publicly trusted" requirements according to the CA/B Forum. In direct comparison to WebTrust, only major deficiencies in the detailing of the requirements for TSP procedures and audit best practice to "set up New Roots" and "CA Key Generation" can be recognized. To this end, further specifications should be made by ETSI ESI.

It is recommended that ETSI ESI provide further specifications in the detailing of the requirements for TSP procedures and audit best practice to "set up New Roots" and "CA Key Generation.

Another recommendation is to tighten up management of the TSL. Currently, the 3-month maximum for any changes made is a long period. While incident reports are requested within 24-72 hours, the updating of the TSL can take up to 3 months in some countries.

The management of the TSL needs to be updated continually to maintain the fidelity of the system and to develop the TSL system as an alternative to the hierarchical trust approach using root stores.

6.2 Branding QWACs, rolling them out for public consumption

6.2.1 Improved visibility of the EU trust mark for qualified trust services

The Commission Implementing Regulation (EU) 2015/806 lays down specifications relating to the form of the EU Trust Mark for qualified trust services. This trademark-protected EU branding tool for qualified trust services should signal to the users the trustworthiness of eIDAS-compliant, audited, trust services. Only TSPs that have been audited and confirmed by a national supervisory body can advertise their products and services with the EU trust mark for qualified trust services. Until now, this logo has been to a large extent unknown and has rarely been used. The WebTrust logo, in contrast, is used by a number of international TSPs for promotional and marketing purposes and is considered trust-worthy.

The difference here is that, currently, the WebTrust logo usually links the user to a webpage with all the desired information and is managed by WebTrust itself. In fact, there are three different logos, depending on the audit a TSP has passed. In comparison, there exists only one EU trust mark, and its meaning currently only really reflects that the QTSP is entitled to use it, not which from the list of applicable qualified trust services is offered by a QTSP. Access to the EU List of the Lists through an EC browser tool currently exists, which can help users search and discover important information about TSPs based on different criteria like country of origin or trust service type.

Increasing the global visibility of the EU trust mark as a trusted logo for qualified trust services would in turn strengthen the acceptance of the audits. In a preceding ENISA study[23], it was determined that to display the logo in the browser URL/address bar is, in the current state of the web environment, too difficult to be effectively implemented. While it is perhaps not technically difficult to do, there is currently no intention for browsers to integrate it.

There is need to further analyse, test and review how the EU trust mark can be displayed on websites in a tamper-proof manner in order to increase the global visibility of the EU trust mark as a trusted logo for qualified trust services, which would in turn strengthen the acceptance of the audits. This could be done by the European Commission or by ENISA.

6.2.2 A logotype certificate with CA/B Forum (development of a QWAC-specific UI)

In 2004, RFC 3709 defined logotypes in X.509 certificates. Logotype certificates can help make brands or trust marks visible in a trustworthy manner. Many issuers may use a community logotype to co-brand with a global community in order to gain global recognition of its local service provision, a type of community branding that is very common e.g. in the credit card business, where local independent card issuers include a globally recognized brand (such as VISA and MasterCard).

The development of a QWAC-specific UI can be an alternative for the green bar and padlock in the browser URL field and it will also need consent from the browser or application vendor to show the content of the certificate.

6.2.3 Mandate EU trust mark usage, beginning with European banks

One concrete idea to complement the previous recommendation about improving the visibility of the EU trust mark is the possibility of mandating its use in test cases and expanding its reach in an already trusted environment. After PSD2, since it is now obligatory for European banks to deploy QWACs, it may be possible to obligate banks to engineer some sort of visual indicator of their deployment. This seal could be displayed in the browser for websites that deploy QWACs, beginning first with banks and then later extending to other areas such as healthcare, etc. It should be made clear here that this strategy needs to be one that is unified. The EU trust mark embodies an image at the heart of the European trust iconography and is ready to be deployed more publicly.

Since "banks are taking part in educating customers by offering browser plug-ins for enhanced security and peripheral education" (Timmerman, 2004), a foreseeable next step is the full pan-European usage of the trust mark on bank websites that fall under the purview of PSD2 rules. This agenda might also be extended to the TSL integration for all operating systems and browser vendors operating in the European Union as part of a wider rollout of the trust mark and its potential close association with QWACs.

[23] QWACs Plugin, January 2018, https://www.enisa.europa.eu/publications/qwacs-plugin.

6.3 Relationships with the browsers

6.3.1 Face-time with the browsers, meetings planned for CA/B Forum

A critical step forward is going to be convincing the browsers and OS vendors to include the TSL in their respective root stores. Before they even consider including the TSL in the browser list, they need to gain reassurance that the audit schemes meet their expectations and that the criteria used meet their requirements as represented in the CA/B Forum documents. ETSI has gone a long way in achieving this by the inclusion of ETSI standards for audit (EN 319 403) and the policy criteria (EN 319 411-1) in their documents. However, there still remains some resistance to their adoption. That being said, however, ETSI has enjoyed substantial success with CA/B Forum concerning the adoption of ETSI standards that are based on eIDAS requirements (e.g. EN 319 403 and EN 319 411-1) as basic fulfilment of the requirements of CA/B Forum's Baseline and EV Guidelines.

The value of QWACs, outside the EU, will diminish as the browser vendors (after 2018, Google and Apple) deprecate the use of EV certificates as they promote a system for which website security comes without additional information on the certificates. Since the publication of a number of studies in which the EV certificates no longer benefit from their previous utility leading up to the rollout of CT, unless a way forward is fostered with these vendors, it will be challenging to grow the value of QWACs outside the EU Digital Single Market.

In part, this argument is why individual, face-to-face meetings are being arranged with the browsers at the CA/B Forum meeting in Shanghai in late 2018 and in Cupertino in 2019.

It will be challenging to grow the value of QWACs outside the EU Digital Single Market by convincing the browsers and OS vendors to include the TSL in their respective root stores. Towards this goal face-to-face meetings should be arranged by the European Commission with the browsers also in the context of CA/B Forum meetings.

6.3.2 EU browser

Because website certificate services are dependent on the willingness of browsers to recognize Trusted List status, and because no browsers currently recognize the Trusted List by default, an alternative, if not short- and medium-term, way forward is the cooperation with a European-based browser vendor as a test case for Trusted List root store acceptance. Previously a partnership with the Vivaldi browser from Norway has been floated in various EU ICT forums and workshops.

An alternative way forward is the cooperation with a European-based browser vendor as a test case for Trusted List root store acceptance. The terms of this agreement would include e.g. mandatory use of QWACs in e-Government and financial services for a Digital Single Gateway.

6.3.3 European Certificate Transparency

Certificate Transparency (RFC 6962) was described by Google some years ago in 2013 at the IETF as an open framework for the monitoring of the SSL / TLS certificate system and the auditing of specific SSL/TLS certificates. Since then, Google has implemented this RFC by requiring its use in Chrome for all EV certificates issued after 1 Feb 2015. By the end of 2018, both Google and Apple will require CT for all issued SSL certificates (otherwise Chrome and Safari will classify affected websites as insecure).

Using its substantial market power, with this CT initiative, Google is considerably influencing the future of the SSL/TLS ecosystem. At the European level, it is important to play an active role in the context of CT and to represent European concerns and enforce them in cooperation with politics and administration.

To support the visibility of eIDAS and to place the aspects of eIDAS in the context of CT, European players should develop and operate European components for CT i.e. a European (qualified) certificate log and European certificate monitoring and auditing services. It is anticipated that this would offer great political leverage in the relationship between the EU concerns and major browser vendors.

7. Bibliography/References

(AIM-BEUC Joint Initiative, 2014)	AIM-BEUC Joint Initiative, *Smarter Logos, better informed consumers*, February 2014 http://www.aim.be/uploads/news_documents/Brochure_smarter_logos%2C_better_informed_consumers%2C_e-version.pdf. Retrieved September 2018
(CA/Browser Forum. 2012)	CA/Browser Forum, *Guidelines for The Issuance and Management of Extended Validation Certificates*, V1.4, CA/Browser Forum, effective on 29 May 2012
(CA/Browser Forum. 2013)	CA/Browser Forum, *Network and Certificate System Security Requirements*, V1.0, CA/Browser Forum, effective on 1/1/2013
(CA/Browser Forum. 2017)	CA/Browser Forum, *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates*, Version 1.4.2, January 2017.
(CPA, 2014)	CPA Canada, *WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5*, April 2014.
(CPA, 2016)	CPA Canada, *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.1*, November 2016.
(CPA, 2011)	CPA Canada, *WebTrust for Certification Authorities - Version 2.0*, March 2011.
(EU Commission, 2014)	EU Commission, *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*.
(EU Commission, 2015)	EU Commission, *Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services*. OJ, L 128:13–15, 2015. Available from https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0806.
(ETSI, 2016a)	European Telecommunication Standards Institute, *ETSI EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*, February 2016.
(ETSI, 2016b)	European Telecommunication Standards Institute, E*TSI EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*, February 2016.

(ETSI, 2016c) European Telecommunication Standards Institute, *ETSI EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*, February 2016.

(FPKI, 2012) FPKI Federal Public Key Infrastructure Policy Authority, *Federal Public Key Infrastructure (FPKI) Concept of Operation (ConOps)*, Version 1.0.0, January 2012.

(FPKI, 2015) FPKI Federal PKI Management Authority, *Federal PKI Trust Infrastructure Overview*, V1.0, September 2015.

(Fiedler, 2014) Fiedler, A., Thiel, C., *The need of European White Knights for the TLS/SSL Certificate System*. ISSE 2014: 170-174

(Hamaguchi, 2016) Hamaguchi, S., Kinoshita, T. and Tezuka, S, *An Analysis of Trust Models of Public Key Infrastructure*, International Journal of Control Theory and Applications, International Science Press, Volume 9 • Number 43 • 2016

(Mozilla, 2018) Mozilla Org, *Native Messaging*, https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Native_messaging, Retrieved 2018-10-6

(RFC 6962) RFC 6962, *Certificate Transparency, Experimental Request for Comments*

(Rousseauo, 1998) Rousseauo, D. M., *Not so different after all: A cross-discipline view of trust*, Academy of Management Review 1998, Vol. 23 No. 3, 393-404.

(Sel, 2015) Sel, M., *A Comparison of Trust Models*, ISSE 2015 pp 206-215.

(Timmerman, 2004) Timmerman, T., R., *Certificate Authority Criteria in User Perspective*, Master Thesis, University Amsterdam Faculty of Economics and Business Administration, 2004

Annex A: Predicted effort required to carry out actions in each of the recommended directions

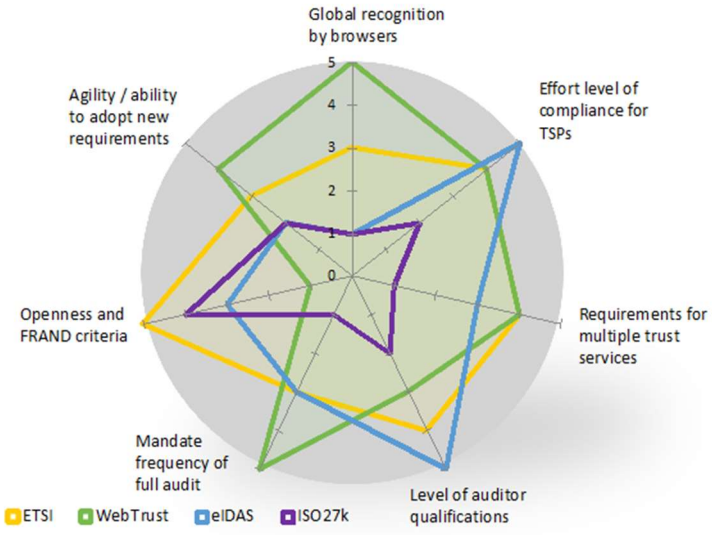

Figure 10 Comparison of audit schemes by factor (based on industry discussions and expert interviews)

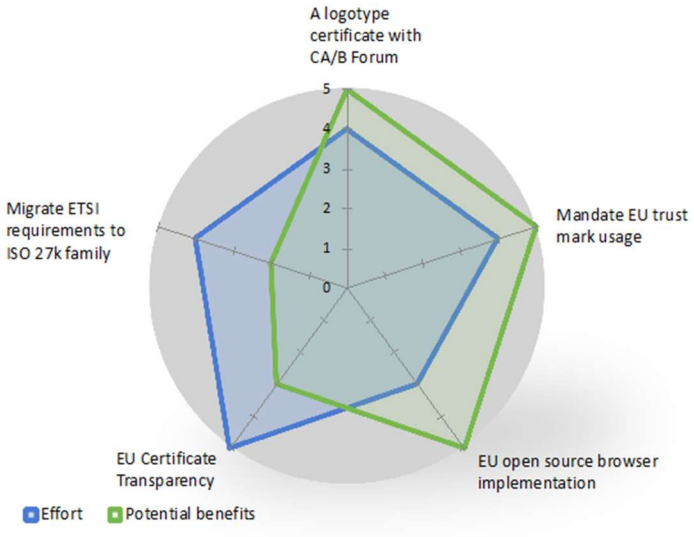

Figure 11: Strategic measures/recommendations evaluated by effort and benefits (based on industry discussions and expert interviews)

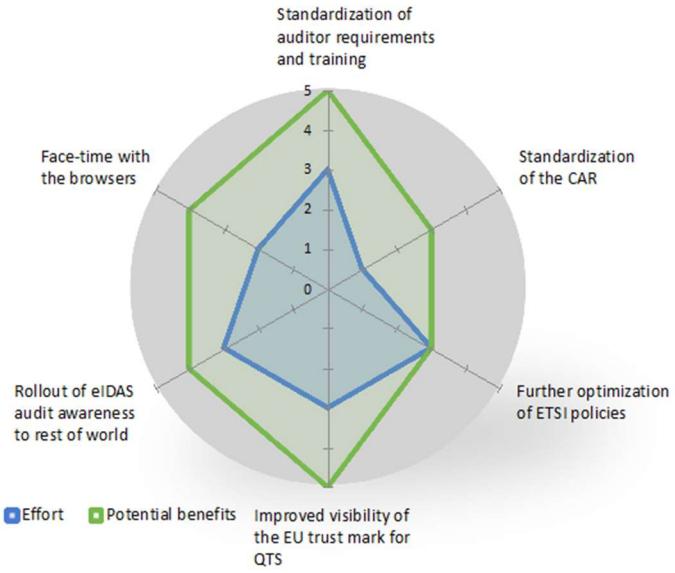

Figure 12: Tactical measures/recommendations evaluated by effort and benefits (based on industry discussions and expert interviews)

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-02-19-005-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: 978-92-9204-255-4
DOI: 10.2824/74012