Qualified Website Authentication Certificates

Promoting consumer trust in the website authentication market

DECEMBER 2015

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 Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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.

Author(s)

This report was elaborated by a group of experts: **Arno Fiedler** (Nimbus Technologieberatung), **Jon Shamah** (EJ Consultants), **Inigo Barreira** (Izenpe), **Wanko Clemens** (TÜViT), **Arthur Miękina** (PWPW), **Slawomir Gorniak** (ENISA), **Clara Galan Manso** (ENISA).

Editor(s)

European Union Agency for Network and Information Security
ENISA responsible officer: **Clara Galan Manso**.
For contacting the authors please use isdp@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to express our gratitude to the following individuals for providing valuable comments as external reviewers of the report:

Marco Fernandez Gonzalez (European Commission), **Ben Wilson** (Digicert), **Lionel Antunes** (Centre des technologies de l'information de l'État, Luxembourg), **Marcin Fijalkowski** (Ministry of Economy, Poland), **Herbert Leitold** (Secure Information Technology Centre, Austria) and **Tanel Kuusk** (Certification Centre, Estonia).

Acknowledgement should also be given to ENISA colleagues who helped in this project, in particular: **Prokopios Drogkaris** and **Evangelos Rekleitis**.

Legal notice

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

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

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

Copyright Notice

ISBN 978-92-9204-152-6, DOI 10.2824/464966

Table of Contents

List of tables

List of figures

List of abbreviations

CA	Certification Authority
DV	Domain Validated
EFF	Electronic Frontier Foundation
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
EVCP	Extended Validation Certificate Policy
HTTPS	Hypertext Transfer Protocol Secure
MS	Member State
NIS	Network and Information Security
OV	Organization Validated
QTSP	Qualified Trusted Services Provider
QWAC	Qualified Website Authentication
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSP	Trust Service Provider

Executive Summary

Context for the study

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market[1] (eIDAS Regulation), adopted on 23 July 2014, extended the scope of the Directive 1999/93/EC on a Community framework for electronic signatures[2] (eSignatures Directive), by introducing in the legal framework provisions for new types of trust services. Additionally to services related to electronic signatures, the new trust services covered in the eIDAS Regulation are those related to electronic seals, electronic time stamps, electronic registered delivery services and certificates for website authentication.

The eSignatures Directive introduced as well in the EU market a clarified regulatory context for electronic signatures by setting in place the qualification scheme. The eIDAS Regulation also broadens the scope of this framework, by establishing the possibility to become qualified for the new types of trust services. In this respect, the aim of the Regulation is to enhance consumer's trust in the digital environment and to improve the trust services market's transparency by introducing a clarified and comprehensive legal framework.

The eIDAS Regulation provisions for trust services will enter into force on July 2016. To support its successful introduction in the market, this study focuses on one of the newly introduced services, qualified certificates for website authentication. Certificates for website authentication, widely known as SSL/TLS certificates, play a critical role in the security of online transactions and have been long employed by websites (it is estimated that currently 64.5% use presently some kind of certificates[3]). This number has grown sharply in the last years driven by business needs rather than any regulatory framework, and the market has evolved to be highly concentrated in a small number of players, mostly from outside Europe.

Based on these features, qualified certificates for website authentication (QWAC certificates) present a particular case among the new trust services defined in the eIDAS Regulation. They will need to enter in an already mature, global and unregulated market. For their successful introduction, it will be necessary to create a demand by properly communicating to consumers their benefits, while at the same time supporting providers to ensure enough supply.

In this context, the objective of this report, carried out under ENISA Work Programme 2015[4], is to make recommendations on strategies for the successful introduction in the European market of qualified certificates for website authentication.

Structure of the report

Chapter 1 introduces the main concepts around website authentication certificates: the role they play in the security of internet, the different types of certificates available in the market, and the existing industry level harmonization activities.

[1] EUR-Lex, European Union, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

[2] EUR-Lex, European Union, "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

[3] W3TECH report on the usage of SSL certificate authorities for websites (data retrieved on November 2015), http://w3techs.com/technologies/overview/ssl_certificate/all

[4] ENISA Work Programme 2015, https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2015

Chapter 2 describes the framework for trust services in the eIDAS Regulation. It analyses the main requirements set for all trust services providers established in the EU, both for non-qualified and qualified providers, and the more strict requirements set for the later.

Chapter 3 explains the main concepts around qualified website authentication certificates, both in the context of the eIDAS Regulation and in the existing market for website authentication certificates.

Chapter 4 presents an analysis of the website authentication certificates market, with the aim of determining the most noteworthy market features.

Chapter 5 introduces a brief characterization of qualified trust services providers market and their presence in the website authentication market introduced.

Chapter 6 proposes a SWOT analysis for the introduction of qualified website authentication certificates in the market. The analysis aims to identify internal and external factors that can impact positively and negatively the growth of the adoption of this new kind of trust services in Europe and the development of the related market.

Chapter 7 presents the final outcome of the study, a collection of short-term, medium-term and long-term strategies and recommended actions aimed to ensure transparency of the European market by introducing qualified website authentication certificates in Europe.

Annex A presents additional figures in the analysis of the website authentication certificates market (in terms of types of certificates, market players, geographical distribution, etc.).

Proposed strategies and recommended actions

Based on the findings of the report, this report proposes six strategies and twelve recommended actions as an escalated approach that targets the most important aspects detected to be critical for (i) improving the website authentication market in Europe and (ii) successfully introducing qualified website authentication certificates as a means to increase transparency in this market.

Short-term Strategies

I. Increase the number of websites using website authentication certificates in Europe

1. EU governments and web browsers developers should increase efforts to help end users understand the key role website authentication certificates play in protecting their personal information and their online transactions.
2. EU governments and trust service providers should undertake initiatives to communicate to website owners the importance of using website authentication certificates to protect themselves from fraud.
3. All stakeholders involved should try to communicate more clearly to users the differences types of website authentication certificates and their distinct assurance level.

II. Establish a market for qualified website authentication certificates

4. Public administrations at all EU levels should lead the way in the adoption of qualified website authentication certificates.
5. Qualified providers should consider to provide a full range of trust services to seize more business opportunities.

III. Align existing regulatory and industry led initiatives

6. EU regulators should take into account existing good practices from industry led initiatives during the implementation of the eIDAS Regulation.

Medium-term Strategies

IV. Increase recognition of qualified website authentication certificates by end users

7. EU Regulators and qualified trust service providers should promote the acceptance of qualified website authentication certificates by browsers, as an equivalent to Extended Validation certificates or with their own distinctive feature.
8. EU Member States should support the recognition of the EU trust mark through nationwide promotions as part of NIS and cybersecurity campaigns.

V. Strengthen the market position of QTSPs

9. Qualified providers should cooperate to strengthen their position in the website authentication certificate market.
10. EU institutions and governments should incentivize qualified providers to expand beyond their national market.

VI. Substantially increase the market share of qualified website authentication certificates

11. EU institutions and governments should communicate to businesses the benefits the clarified legal framework that qualified website authentication certificates will offer them.
12. EU institutions and governments should promote the use of qualified website authentication certificates by targeting specific critical sectors such as health and finance.

Long-term Strategy

VII. Make qualified website authentication certificates the reference for high quality website authentication certificates globally

13. EU Institutions should promote the recognition of qualified website authentication certificates outside of the EU as a high-quality product.

1. Website authentication certificates

1.1 Introduction

The digital society is transforming the way that individuals and companies are interacting, by improving communication and extending the distance over which trading can occur. With the lack of face-to-face contact within transactions, trust is growing as one of the key elements that facilitates those interactions. This transformation is similar to the postal mail-order companies that grew up in the mid-twentieth century, when brand confidence fed success and growth.

With internet transactions increasing in numbers, and the ability to interact with anyone capable of presenting what appears to be a legitimate web store front, it is hard to distinguish and place trust. Organizations have grown to become more distributed and their supply chains grow longer, while becoming more dependent on trust infrastructures. Similarly, government agencies are stepping up their efforts trying hard to reach out digitally to their citizens in an attempt to increase efficiency, transparency and reduce fraud.

Add to this revolution in communication, the coming to terms by criminals that this is an opportunity to defraud millions of people by posing as legitimate businesses, or even, by using these false web-sites to intercept communications and steal personal details and passwords for illegal use. Furthermore, organisations can be made vulnerable if commercially sensitive information or false reporting is introduced, causing loss of revenue and reputation alike.

A typical example is certificate seal abuse. Because trust seals normally demonstrate compliance with standards, business identify verification, or website security, they are likely to be misused due to the trust they instill to the vendor image and due to the functional benefit the pose for the attacker. There are two main types of abuse: phishing sites copying the seal from the target's real login pages, and counterfeit sites where the fraudster uses the benefits of the trust seal to increase conversions. Some legitimate sites also include a trust seal they are not permitted to use.

A solution to these problems was the creation of website authentication certificates. These electronic certificates are cryptographically secured tokens, which are deployed in webservers, and which identify uniquely and confidently a webserver or a domain as being genuine. Many of these certificates are recognised by browsers, through cryptographic validation, as being legitimate, and this recognition is used to promote the trust to the individual. In the case of server-to-server communication, without that recognition, communication is programmatically blocked.

However, as with any system, there are no absolutes and website authentication certificates are no different. There are many types of website authentication certificates, which depend on similar qualities of cryptographic processes, but importantly, are differentiated by the procedures in establishing the true identity of the organisation or individual that is applying to purchase them. Their value is only as good as the trust in the verification of the identity.

This leads to a market with varying features and types of website authentication certificates. Low quality certificates, from trust service providers that are issued against weak or no-existent identity checks, have been used by fraudsters to run phishing sites with a trusted certificate, and to perform attacks and assist fraudulent causes; e.g. man-in-the-middle or code injection.

From a governance point of view, website authentication certificates need to be created by a trusted authority and follow strict rules and certificate practices, otherwise they will be valueless, and even used to misrepresent webserver identities. Technically anyone with sufficient access to authentication technology, can create an untrusted website authentication certificate by him/herself, this is why a strict hierarchy or chain of trust is needed. This trust chain is upheld by web browsers through the certificates, and therefore issuers, they recognise.

1.2 Stakeholders in the market for website authentication certificates

To understand the website authentication certificates domain, it is important to start by identifying the various stakeholders that participate in it. Ultimately, certificates are meant to protect the communication between an end user and a website owner, by providing an assured link between the cryptographic keys used to secure the transaction and the entity to whom the keys belong. But there are four essential participants in the chain; that is trust service providers, website owners, web browsers, and end-users themselves.

Each participant plays an important role:

- Trust services providers as producers of certificates, which attest the legitimacy of the owner of the domain and the security properties of the certificate.
- Website owners as direct consumers of certificates, who purchase certificates from trust service providers in order to show the legitimate nature of the domain (and in some cases, of the organization owning the domain) and the fact that the connection with the server will be secured.
- End users as the indirect consumer of certificates, who place confidence in the legitimacy of a website and the security of connection based on the displayed certificate.
- Browsers as third party validators of the certificates, which act as a middle agent between the end user and the website, by performing checks on the legitimacy and the security of the certificate.

Trust service providers

Trust service providers (TSPs) issuing website authentication certificates, commonly known as Certificate Authorities (CAs), provide essential services in the electronic trust services ecosystem, including monitoring and verifying various kinds of certificates. Essentially, the signatures that they put in the certificate serves to authenticate the legitimacy of a certificate holder's identity and establish trust in online data transfers. The global market consists of a handful of large TSPs and a few hundred of other much smaller organizations, with a similar ability for their certificates to be verified along the certificate chain of trust between browsers and servers.

This is important for two reasons: (a) the entire HTTPS ecosystem is built upon trust in the integrity and of the ability of TSPs (especially the larger ones) to make security-critical decisions, and (b) just about anyone can become a TSP relatively easily. These two conditions together are an odd function of the market for website authentication certificates, and result in a number of systemic problems within the HTTPS ecosystem, which will be touched upon in the following sections.

Website owners

The owners of websites play a critical role in the market for website authentication certificates as primary consumers. These include a range of actors, from governments and universities, to businesses and private citizens. These institutions or individuals must decide the level of security they deem appropriate for their content and the services that their sites provide to end-users.

The decision to deploy one or more website authentication certificates depends on a range of factors, and in fact, some owners choose not to use certificates to protect their websites. Indeed, despite the value of website authentication certificates and their obvious advantages to electronic transactions, their deployment has still room to increase as a percentage of all websites. It has been reported that 35.5% of all websites do not have any authentication certificates at all[5]. This means that over one third of all websites do not consider that there is a need for website authentication certificates or do not monitor their validity or use when they are installed.

Web browsers

Web browsers also perform critical tasks in the chain of trust that website authentication certificates create between users and online content. They help determine the trustworthiness of trust service providers. The five most widely used web browsers all contain strictly moderated and monitored lists of root TSPs, which must follow a set of guidelines in order to prove the identity of intermediary TSPs and certificates they authorise and to ensure security is maintained within the system. After a root TSP is designated trustworthy, browsers can automate a number of security decisions, while at the same time indicating the level of security to users via their interface[6], with visual cues such as a green padlock icon.

In the past several years, worldwide usage of individual browsers has changed substantially, as illustrated in Figure 1. According to W3 analysis, Google Chrome has taken the number one place worldwide, as well as in Europe (Mozilla Firefox is still first over Chrome in Germany, though barely so). Although the exact data on browser use vary depending of the specific report, this is an important trend to observe because their root stores and the rules that govern those help dictate standards for security deliverable by trust services providers. With the help of other international level regulatory measures, overall security can be boosted through cooperative efforts with leading web browsers.

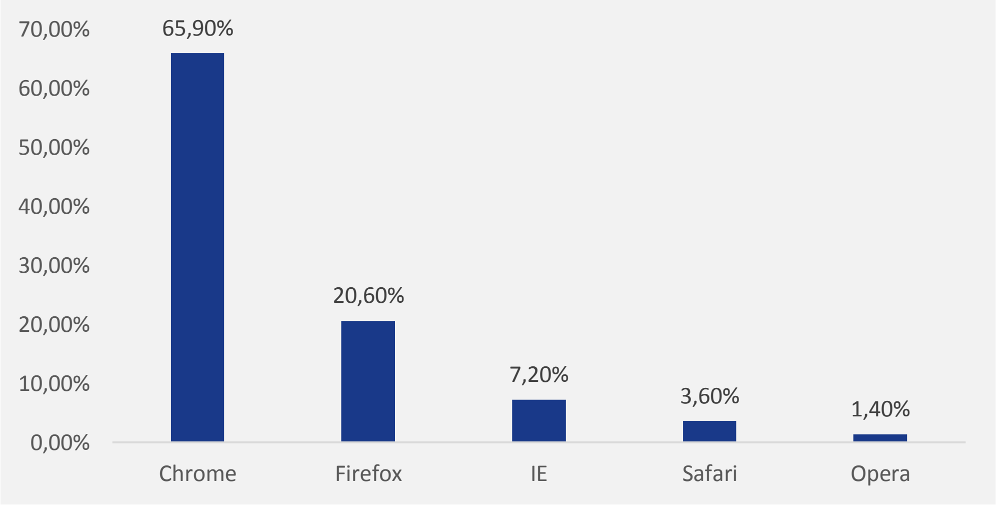

Figure 1 Major browser user statistics (September 2015)[7]

End-users

The term ‘end-user’ refers to natural persons (including citizens, residents and consumers), and legal entities (including businesses, non-profit organizations, and governmental agencies and institutions) that access an online service which employs a website authentication certificate. Often it is these individuals who have the

[5] W3TECH report on the usage of SSL certificate authorities for websites (data retrieved on November 2015), http://w3techs.com/technologies/overview/ssl_certificate/all

[6] Jeremy Clark and Paul C. van Oorschot, “SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements“, 2013, http://users.encs.concordia.ca/~clark/papers/2013_sp.pdf

[7] w3schools report on browser usage statistics (data retrieved on September 2015), http://www.w3schools.com/browsers/browsers_stats.asp

least knowledge about and control over the security or lack thereof in their online dealings, though they often have the most to lose from security breaches involving personal information and other sensitive data.

Back in 2007, a study had shown that over 90% of users were unfamiliar with or just ignored security indicators and were still willing to transmit personal information or sensitive data over unsecured websites[8]. These user "mental models of HTTPS"[6] were considered a challenge for the long-term projection for adoption and success of the HTTPS model. However, a recent study by the CA Security Council discovered this trend had all but reversed, with only about 2 percent of users proceeding beyond an "untrusted connection" warning and 3 percent giving out credit card details on forms without the padlock icon[9].

1.3 Existing types of website authentication certificates in the market

So far we have introduced the concept of website authentication certificates and their overall role in the security of the internet. However, website authentication certificates are not homogeneous. There are a number of different types of website authentication certificates, which vary depending on the quality (technical and/or procedural) of the production process, their purpose of use, their Certificate Policy, their Certification Practice Statement and their general terms and conditions. Two main classifications can be established regarding types of commercial certificates, based (i) on the verification procedure of the applicant's data and (ii) on the number of domains/servers the certificate is intended to secure.

Classification according to the data validation level

When a trust service provider issues a website authentication certificate, it is acting as an independent trusted third party; performing the authentication of the applicant, as well as the verification of the certificate data. The effort taken for the proper authentication and data verification usually is reflected in the quality level of the certificate (as well as in the price for the customer). According to this parameter, a common terminology has been adopted in the market to differentiate the types of website authentication certificates:

Domain Validated (DV): This is an entry-level type certificate with a low level of trust. The only procedural check that is made by the issuing TSP is that the prospective owner of the certificate actually owns the domain that it will authenticate. DV certificates are available nowadays at a very low price or even for free. There are no checks that the owner organisation is a valid business entity or any other validation of the owner organisation.

Organization Validated (OV): Also called 'subject identity validated' or 'fully authenticated'. This certificate has detailed validation checks performed by the issuing TSP that the prospective owner of the certificate is a registered legal entity, registration is valid, it is the owner of the domain, which it will authenticate, and indeed that the applicant has the authority to apply for such a certificate.

Extended Validation (EV): This certificate includes additional information on the owner of the certificate, and additional checks are made by the issuing TSP to ensure that the owner of the domain which it will authenticate, is validated, and that the applicant has indeed the authority to apply for such a certificate. Overall, these aspects are validated:

- The legal, physical and operational existence of the entity
- The identity of the entity matches official records
- The entity has exclusive right to use the domain specified in the EV certificate

[8] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer, "The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies", 2007, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4223213

[9] CA Security Council Consumer Trust Survey Report, 2015, https://casecurity.org/2015/04/13/ca-security-council-report/

- The entity has properly authorized the issuance of the EV certificate

When consumers visit a website secured with an Extended Validation certificate, the address bar at the top of the browser becomes green and details of the genuine owner of the website and the certificate provider are shown. This works on many of the commonly available browsers.

Finally, it should be noted that some certificates, meant to be used internally within private networks, are not issued by publicly trusted third party providers. These self-signed website authentication certificates are created and signed internally by an organisation and are not trusted outside of that organisation network. They do not hold the same weight as a publicly trusted certificate created by a trust service provider, and may or may not conform to some form of certificate policy. Self-signed certificates are not meant to be used publicly, as there is no third party who can attest to the veracity of the information contained in the certificate, therefore they should be created for strict internal use only.

Classification according to the number of domains secured

Another distinction that can be made among types of website authentication certificates relates to the number of domains that are secured by the certificate:

Single domain: Single domain certificates are used to secure a single domain. They are the most adequate for small organizations. Single domain certificates are available as Domain Validated, Organization Validated or as Extended Validation.

Wildcard: Wildcard certificates (e.g. issued to *.example.com) are used to secure an unlimited number of first level subdomains in a single domain. Subdomains added subsequently will automatically be secured. This adds flexibility to customers, however it can introduce some security risks. Wildcard certificates are available as Domain Validated or as Organization Validated, but not as Extended Validation.

Multi Domain: Multi Domain certificates are used to secure multiple domain names or servers across multiple domains in one certificate. They are the most adequate for large organizations and usually allow typically up to 100 domains to be included in one certificate. Multi domain certificates are available as Domain Validated, Organization Validated or as Extended Validation.

Figure 2 shows a cross-classification of possible combinations of commercial types of certificates based on both attributes, identity validation and number of domains.

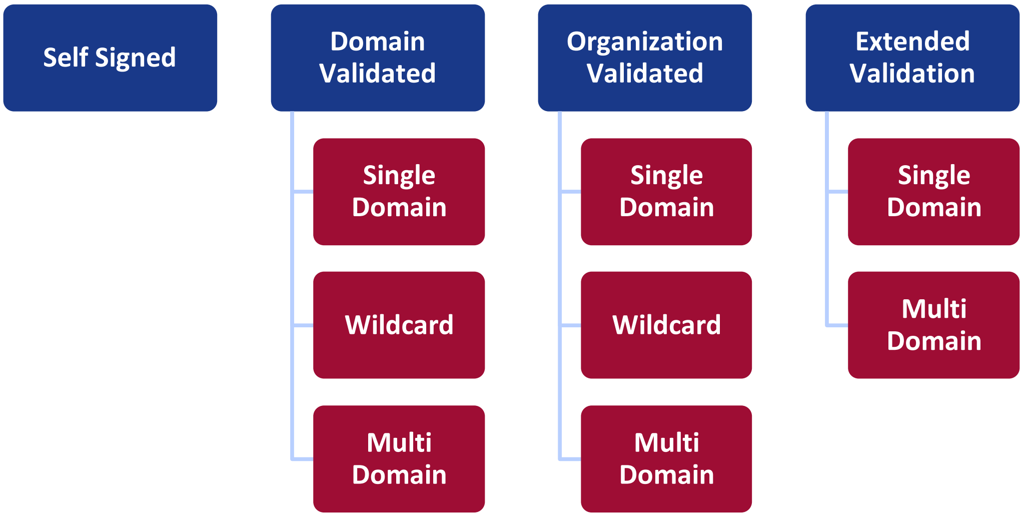

Figure 2 Cross classification of existing types of commercial website authentication certificates

1.4 Existing industry led harmonization activities

CA/Browser Forum

The most relevant, market-led, harmonization activities in the area of website authentication certificates have been conducted by the CA/Browser Forum[10], a voluntary consortium which groups more than fifty TSPs and browsers, among them the largest market players. The CA/Browser Forum was created in 2005 as part of an effort among TSPs and browser software vendors to provide greater assurance to Internet users about the web sites they visit by leveraging the capabilities of SSL/TLS certificates.

At that time, several trust problems were present in the SSL/TLS certificates ecosystem:

- There were no generally-accepted standards for validating the identity of the certificate requester, which is a critical point in the chain of trust of website authentication certificates.
- There was a degree of uncertainty in users' over the significance of the padlock icon.
- URLs that commonly appeared in browser address bars had become obscure and users could no longer use them to ensure that they were transacting with the web site that they expected.
- Some breaches involving TSPs caused by a lack of quality in the procedures created a sense of mistrust among customers on the overall quality of the website authentication certificate market.
- Phishing web sites that used counterfeit content to trick users into providing login credentials were a concern.

The CA/Browser Forum identified the need for better security indications to increase users confidence on the legitimacy of the web sites they were visiting, and to perform this in a way that clearly indicated to users the identity of the business entity with whom they were doing business. A solution was put forward with the creation of a new type of certificate, the Extended Validation certificate. The CA/Browser Forum first published the EV SSL/TLS Certificate Guidelines[11], a voluntary standard that defines a set of requirements for the issuing of Extended Validation certificates, in June 2007.

As described in the previous section, Extended Validation certificates offer the highest quality in terms of assurance of the identity of a certificate owner among exiting types of certificate in the market. Since then, EV certificates have been adopted by major TSPs, due to a continuous increase in security threats such as data theft and identity theft (e.g. through phishing), which has created the need for organizations to adopt advanced security solutions. Growing incidents of email hacking and password theft are driving companies to adopt EV certificates[12].

At the same time, some browser suppliers developed user interface standards for displaying that information to emphasize its trustworthiness. Internet browser software displays enhanced indication of that identity by changing the appearance of its display (i.e. colors, icons, animation, and/or additional website information). Currently, most desktop browsers will indicate that you are on an EV website by giving a distinctive indication in the "chrome" of the browser. The chrome is anywhere in the browser that is outside the part in which your website is usually displayed, – e.g. in the colored frame or address bar of the browser. Typically the use of an EV certificate is indicated by a green color – but this varies by browser.

The CA/Browser Forum undertook in 2012 also the publication of the baseline requirements for the issuance and management of publicly trusted certificates[13]. These requirements serve as a voluntary standard for any organization issuing publicly trusted website authentication certificates.

[10] CA/Browser Forum, https://cabforum.org/

[11] EV SSL Certificate Guidelines, https://cabforum.org/extended-validation/

[12] http://finance.yahoo.com/news/global-ev-SSL/TLS-certification-market-215900160.html

[13] CA/Browser Forum Baseline Requirements Documents, https://cabforum.org/baseline-requirements-documents/

2. Trust services in the eIDAS Regulation

2.1 Introduction

The eIDAS Regulation[14] enables the use of electronic identification and trust services by citizens, businesses and public administrations, to access online services or manage electronic transactions. It supersedes Directive 1999/93/EC[15], which introduced in the legal framework the concept of electronic signatures, and determined that an electronic signature may not be refused as evidence in legal proceedings solely because it is in electronic form.

This clarified legal framework introduced by the eSignatures Directive stimulated the European market of electronic certificates, and providers started to issue certificates for electronic signatures that could be used by EU citizens. Subsequently, electronic signatures became an essential building block in citizens' interactions with public administrations, and are nowadays used in multiple sectors for online transactions.

However, the Directive only covered a subset of the trust service universe, which in actual implementations expands beyond electronic signatures. But these other trust services, that were often associated or combined with electronic signatures, did not enjoy the same legal recognition. To tackle this issue, and with the aim of extending the clarified regulatory context to other trust services used in electronic transactions, the eIDAS Regulation has defined five types of trust services within the legal scope.

Trust services are defined as electronic services, normally provided for remuneration, by Trust Service Providers (TSPs), which consist of:

- **Electronic signatures** (creation, verification, validation and preservation of electronic signatures and certificates related to them)
- **Electronic seals** (creation, verification, validation and preservation of electronic seals and certificates related to them)
- **Electronic time stamps** (creation, verification and validation of electronic time stamps and certificates related to them)
- **Electronic registered delivery services** (creation, verification and validation of electronic registered delivery services and certificates related to them)
- **Website authentication** (creation, verification and validation of certificates related to them)

The eSignatures Directive introduced also the concept of qualification of electronic signatures. The main objective of the qualification scheme was to establish a certain set of requirements for an electronic signature that, when conforming to them, would make the signature *"satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based"* and *"admissible as evidence in legal proceedings"*. These requirements concerned aspects related to (i) the security of the signature creation device, (ii) the format certificate itself and (iii) the policies of the provider of the service.

The eIDAS Regulation enhances and extends the qualification scheme to all trust services within the scope of the legal framework. From the date of entry into force of the provisions for trust services in July 2016, TSPs will be able to issue certificates for all five types of trust services as qualified. Qualified trust services (electronic

[14] EUR-Lex, European Union, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

[15] 15 EUR-Lex, European Union, "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

signatures, electronic seals, electronic time stamps, electronic registered delivery services and website authentication certificates) are based on qualified certificates. A qualified certificate is defined as a certificate that (i) meets the format requirements set in the Regulation and that (ii) is issued by a Qualified Trust Service Provider (QTSP). For providers to be granted the qualified status by a supervisory body, they would need to conform to a set of provisions established in the eIDAS Regulation, which are described in detail in Section 2.3.

Lastly, an important feature the eIDAS Regulation is the internal market principle, namely, that trust service providers can freely offer their services in any member state of the European Union regardless of the state where they are established. The framework established under the eSignatures Directive led to market fragmentation and national silos due to different national implementations that were not always legally and technically interoperable. This limited the possibility for citizens of member states to use their electronic signature certificates in other member states, and also restricted providers to operate in national markets.

In essence, the eIDAS Regulation provides a framework to promote:

- Transparency and accountability: well-defined minimal obligations for TSPs and liability;
- Guarantee of trustworthiness of the services together with security requirements for TSPs;
- Technological neutrality: avoiding requirements which could only be met by a specific technology;
- Market rules and standardization certainty.

The eIDAS regulatory framework, standards and technologies will influence international dialogues and trade negotiations, thus broadening the economies of scale for eIDAS services and increasing the global competitiveness of European businesses and private sector. This will be accompanied by the necessary policy, standardisation and communication activities at the national, European and International levels to ensure understanding and a positive environment for the acceptance and wide uptake of the new legislative framework.

With the objective of understanding the framework for qualified website authentication certificates, and in order to produce relevant recommendations for their introduction in the market, the following sections provide an insight of the main provisions of the eIDAS Regulation regarding trust services, by describing the requirements that will need to be fulfilled by qualified and non-qualified providers, in order to analyse later how they differentiate from the current market practices.

2.2 General requirements for trust service providers

The eIDAS Regulation includes different provisions for qualified and non-qualified trust service providers and trust services. For all trust service providers, the Regulation establishes a set of minimum obligations to fulfil (i.e. data protection and access to persons with disabilities) with a view to ensure a level playing field for market operators. Likewise, the Regulation foresees obligations for risk management, appropriate security requirements and breach notifications which are applicable to all providers.

The following lines cover the most relevant requirements of the eIDAS Regulation for all trust services providers, and the differences within them for qualified and non-qualified providers.

Liability and burden of proof

All trust services providers established in the EU are liable for damage caused by failure to comply with the applicable provisions of the eIDAS Regulation. However, qualified trust service providers (QTSPs) have to prove the absence of intention or negligence, namely that reversal of the burden of the proof is applied, due to the expected high level of security and trust of the services they offer. For non-QTSPs, no reversal of the burden of the proof applies; customers have to make their own risk assessment when selecting a trust service. Since non-QTSPs are not required, a priori, to be providing a high level security service, it would be disproportionate to reverse the burden of the proof.

Security requirements and breach notifications

Concerning security measures and breach notifications, the eIDAS Regulation introduces a full life cycle approach under article 19, both for QTSPs and non-QTSPs. For all providers, there is a risk management obligation (i.e. following a risk assessment, adopting security measures commensurate to the identified risks), that will help to mitigate and early detect any possible breaches (taking into account technical solutions and economic model). Additionally, there is an obligation for notification of such significant security breaches or losses of integrity in a time frame of 24 hours after being aware of it. This obligation is not only very relevant from a customer protection perspective, but will also help to identify the remaining gaps in the system set up by the trust service provider, who will have to update and configure its system accordingly (leading to improving the state of the art in data security and technical expertise).

Supervision

Regarding the level of supervision, there is a distinction between full supervision for QTPs and light-touch ex post monitoring for non-QTSPs, which strikes the balance between the need to ensure an average security playing field for all eIDAS market operators and the resources of supervisory bodies. In this regard, QTSPs are subject to a very strict supervision system that goes together with the level of security and trust they intend to provide. Non-QTSPs are not required to demonstrate this high security level. Nevertheless, in order to anticipate possible drawbacks to the security of the market, the Regulation establishes baseline obligations for all providers as well as possible controls by the supervisory body, for example in the case of a security breach.

Table 1 in the next page provides a summary of (i) common requirements for all TSPs and (ii) specific differences applicable within each requirement for QTSPs and non-QSTPs.

Requirement	Provisions for QTSPs	Provisions for non-QTSPs
Liability	Trust service providers shall be **liable for damage** caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.	
	The **intention or negligence** of a qualified **trust service provider shall be presumed** unless that qualified trust service provider proves that the damage occurred without its intention or negligence.	The **burden** of proving intention or negligence of a non-qualified trust service provider shall lie with the **natural or legal person** claiming the damage.
Risk assessment and security measures	Qualified and non-qualified trust service providers shall take **appropriate technical and organizational measures to manage the risks** posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.	
Security breach notification	Qualified and non-qualified trust service providers shall, without undue delay but in any event **within 24 hours** after having become aware of it, notify the supervisory body of **any breach of security or loss of integrity** that has a significant impact on the trust service provided or on the personal data maintained therein.	
Level of supervision	Subject to **ex ante** and ex post supervisory activities	Subject to **ex post** supervisory activities

Table 1 Requirements in the eIDAS Regulation for QTPs and non-QTSPs

2.3 Requirements for qualified trust service providers

Article 24 on QSTPs

Further to the baseline requirements that any TSP established in the EU must comply with, the eIDAS Regulation provides a detailed set of stringent requirements (as well as procedures) that QSTPs must fulfil in order to ensure the highest possible security level of the services provided. Essentially, the criteria for a qualified trust service provider are indicated in article 24 of the Regulation, which sets the following controls for QTSPs:

- Inform the supervisory body of any change on the provision of the services.
- Inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions.
- Employ staff who possess the necessary expertise, regarding security and personal data protection rules.
- Bear the risk of liability for damage, maintaining sufficient financial resources and/or obtaining appropriate liability insurance.
- Use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, to store data provided to it and take appropriate measures against forgery and theft of data.
- Record for an appropriate period of time all relevant information concerning data issued and received, particularly for the purpose of providing evidence in legal proceedings.

- Provide to any relying party information on the validity or revocation status of qualified certificates issued by them, register any certificate revocation in its certificate database and publish the revocation status within 24 hours after the receipt of the request.
- Have an updated termination plan to ensure continuity of service.
- Ensure lawful processing of personal data in accordance with European regulations.
- Establish and keep an updated database of certificates.

Supervision requirements

Additionally to requirements set in Article 24, another important provision specific to QTSPs is the ex-ante (in advance) supervision. National designated supervisory bodies will be responsible for granting the qualified status to and for the supervision of qualified trust service providers established in their member state. As a first step to apply for the qualified status, a trust service provider will be required to provide the supervisory body with a conformity assessment report carried out by a conformity assessment body (article 21).

As a consequence of such a process, the trust service provider and the trust service it provides will be indicated in the national trusted list as qualified. The trusted list is the constitutive tool that makes that a trust service provider and its services are qualified ones. When listed, the qualified trust service provider will be allowed to make use of the EU trust mark for qualified trust services (art.23). The latter will be of great help to promote high level security services as well as for helping consumers to distinguish between qualified and non-qualified services.

As a further step, once the status is granted, qualified trust service providers will be subject to audits on a regular basis to confirm that they keep on fulfilling the qualifying requirements. The supervisory body may at any time audit a qualified trust service provider to confirm the compliance with the requirements set out in the proposed rules. In the case of non-compliance, the supervisory body would have the power to issue binding instructions aimed at remedying the failure to fulfil the requirements. If the qualified service does not remedy the failure, it could lose its qualified status.

In brief, qualified trust service providers shall be assessed at their own expense:

- Before initiating to provide qualified trust services.
- At least every 24 months by a conformity assessment body.
- At any time by the supervisory body (or by a conformity assessment body in its behalf).

3. Qualified website authentication certificates

3.1 QWAC certificates in the eIDAS Regulation

As described in the previous section, website authentication certificates are one of the five trust service defined in the eIDAS Regulation. A certificate for website authentication is defined in the Regulation as *"an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued"*. They provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website.

According to the Regulation, this service contributes to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. With this authentication of both the website and the person (natural or legal) owning it, it becomes more complicated to falsify websites, thus online fraud is reduced.

As with the other trust services, the eIDAS Regulation sets requirements for qualified certificates for website authentication, which will be recognised and accepted in all Member States. It should be noted that the Regulation adopted an outcome based approach; it sets the requirements to fulfil but does not establish how it must technically and operationally be implemented by trust service providers. In light of the above, the minimum requirements for QWAC certificates are defined in Article 45 and annex IV of the Regulation.

Article 45 sets the requirement for trust service providers issuing qualified website authentication certificates of being qualified, which implies that all requirements for QSTPs described in the previous section will be applicable.

Annex IV defines the content of qualified certificates for website authentication:

1. An indication that the certificate has been issued as a **qualified certificate for website authentication**
2. A set of data unambiguously representing the **qualified trust service provider issuing the qualified certificates** including **Member State** in which that provider is established and adequately to the situation
    a. for a legal person: the name and, where applicable, registration number as stated in the official records,
    b. for a natural person: the person's name;
3. **For natural persons**: at least the **name of the person** to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated

   For legal persons: at least the **name of the legal person** to whom the certificate is issued and, where applicable, the **registration number** as stated in the official records
4. **Elements of the address**, including at least **city and State**, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;
5. **The domain name(s)** operated by the natural or legal person to whom the certificate is issued
6. Certificate's period of validity
7. **The certificate identity code**, which must be unique for the qualified trust service provider;
8. The advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider
9. The location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point 8 is available free of charge
10. The location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.

Finally, another relevant aspect to take into account is that qualified website authentication certificates are meant to be deployed in public systems facing the internet, and as such they need to follow the web public key infrastructure domain already deployed. Indeed, website authentication certificates, which are one new type of the commonly known as SSL/TLS certificates, are used in the so-called Web Public Key Infrastructure Trust Model[16] as it is currently implemented.

This trust model supports communications between the subscriber of the certificate and the client browser. The web PKI trust model also refers to the current processing behaviour of the different crypto libraries, the browsers support, and is related to the communication protocol between the web server and the browser client. This implies that qualified website authentication certificates do not need only to fulfil to the eIDAS Regulation, but also to be fully compatible with the trust model that is already built in the internet.

3.2 QWAC certificates in the context of existing types of certificates

Qualified website authentication certificates are entering an established market with its own industrial standardization efforts, and the eIDAS Regulation has taken this end into account. The objective is not to create a disruption with existing initiatives and to optimize the effort for qualified providers to align both with the EU regulations and with the existing market standards.

In this sense, the eIDAS Regulation states in its recital 67 that “this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union”.

When we try to compare to the different types of certificates, the rationales is that QWAC certificates are meant to be high quality certificates, and therefore should have comparable requirements to high quality types. As described in section 1.3, the most relevant criterion for the classification of website authentication certificates concerns the level of validation of identity of the certificate requester.

It is paramount to mention that the eIDAS Regulation provides with strict rules regarding the identification of the requester of a qualified certificate. Indeed, according to article 24:

"When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

(a) by the physical presence of the natural person or of an authorised representative of the legal person; or

(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’; or

(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

[16] Trust models of the Web PKI (draft-ietf-wpkops-trustmodel-04): https://datatracker.ietf.org/doc/draft-ietf-wpkops-trustmodel/

> **(d)** by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body."

The above is key to ensure trust in qualified certificates for website authentication and avoid, as far as possible, fraud and unauthorised use of such certificates.

In the website authentication commercial market, the strictest requirements are set for Extended Validation certificates, in the CA/Browser Forum EV guidelines. This document describes in detail the required level of validation and the acceptable methods to validate the identity of the certificate requester. However, the eIDAS Regulation, as a high level legal text, does not go into such a level of detail on this matter.

This issue is already being addressed by European standardization bodies, which are preparing a series of standards to facilitate compliance of QTSPs with the eIDAS Regulation. These standards are following an approach of achieving compatibility of QWAC certificates with EV certificates, easing for QTSPs to be compliant with both schemes. At the moment of publication of this study, ETSI has released four public drafts of standards relevant to QWAC certificates, which are under the process of approval[17]:

- EN 319 401 General Policy Requirements for Trust Service Providers[18]
- EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements[19]
- EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. Note: Extends requirements in part 1 with specific requirements for EU qualified certificates[20]
- EN 319 412-4: Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations.[21]

The standard EN 319 411-2, which sets requirements for trust service providers issuing EU qualified certificates, states as its objective, in what concerns qualified website authentication certificates, to define *"A policy for EU qualified web certificate offering the level of quality defined in Regulation (EU) N° 910/2014 for EU qualified certificates (requiring or not the use of a secure cryptographic device) used in support of web authentication. The requirements for this certificate policy include all the Extended Validation certificate policy (EVCP) requirements, plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) N° 910/2014."*

The Extended Validation Certificate Policy (mentioned as a base for the qualified website authentication certificate policy), is defined the standard EN 319 411-1, which concerns all TSPs issuing public certificates. The EVCP is a policy for *"TLS/SSL/TLS certificates offering the level of assurance required by CA/Browser Forum for EVC. The requirements for this certificate policy are built on the normalized policy requirements for the issuance and management of Normalized Certificate Policy certificates, enhanced to refer to requirements from Extended Validation guidelines."*

[17] ETSI Certification Authorities and other Trust Service Providers portal: https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx

[18] EN 319 401 v2.0.0 (under EN approval procedure when retrieved in October 2015): http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.00.00_20/en_319401v020000a.pdf

[19] EN 319 411-1 v1.0.0 (under EN approval procedure when retrieved in October 2015): http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.00.00_20/

[20] EN 319 411-2 v2.0.6 (under EN approval procedure when retrieved in October 2015): http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.00.06_20/

[21] EN 319 412-4 v1.0.0 (under EN approval procedure when retrieved in October 2015): http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.00.00_20/en_31941204v010000a.pdf

Thanks to this integrated approach, issuers of QWAC certificates that comply with the ETSI standard EN 319 411-2, will also be compliant with EV guidelines requirements. This includes the strict requirements for validation of identity of the certificate requester. On top of this, QWAC certificates providers will need to fulfil the additional provisions of the eIDAS Regulation that are not foreseen in the EV guidelines, among them being the most notable:

- Be under the continuous supervision of a national supervisory body, which will grant the qualified status for both itself and the qualified website authentication certificates it intends to issue.
- Submit the audit results to the supervisory body, which may also audit the TSP at any point.
- Be audited by a conformity assessment which is accredited according to EU regulations.
- Notify all security breaches and losses of integrity to the supervisory authority and to the individuals, when they might be adversely affected.
- Be under the EU data protection regulatory framework.

4. The current market of website authentication certificates

4.1 Introduction

Issuing of QWAC certificates is expected to start in July 2016, with the entry into force of the provisions affecting trust services in the eIDAS Regulation. From this moment on, QWAC certificates will need to integrate in an already mature, but still growing, commercial website authentication market. In order to make relevant recommendations for a successful market uptake, it is important to understand the current market's main characteristics and features. The following sections of this document present an analysis of the main website authentication market traits, the risks and barriers within the current market and the possible ways to move ahead to overcome these barriers. A more detailed description of the market, in terms of market size, geographical distribution, and distribution based on existing types of certificates is presented in Annex A of this document.

At first glance, the market for website authentication certificates is structured similarly to other conventional goods or services markets, with actors occupying the supply- and demand-side economic curves, and with regulators intervening at various places along the value chain to facilitate a fair, optimal and competitive environment. The very concept of this market, however, needs to be defined in broad strokes, given its strongly heterogeneous and relatively fragmented nature. Providers of website authentication certification services span a wide variety of offerings, some of which occupy narrowly defined niche markets focusing on specific regions or product types, and others acting as one-stop-shops with many differentiated product bundles.

The website authentication market is a dynamic economic space, which has shown sustained growth of between 6 and 12 per cent in average compound annual growth between 2008 and 2013. The total operating revenue as well as the average margin for profit are growing steadily across the board, and while EU-specific statistics are not currently available, eGovernment and eInvoicing services appear to be entering EU national and cross-border markets.

While the market for electronic trust services is large and varied, this particular section focuses on the specific market for HTTPS services, namely for website authentication trusted certificates. The primary players in the website authentication certificate market are server system and/or website owners and trust service providers. If the owner of a server system or website wishes to use HTTPS services, they would purchase one or more website authentication certificates from a TSP in order to authenticate their server system or their webpage for the user community. Unlike conventional goods or services markets, however, the HTTPS market ecosystem looks significantly different and exhibits notable features with great current and potential future impacts on the market for website authentication certificates and overall security in the HTTPS environment.

4.2 Noteworthy market features

With only three or four companies dominating the market for website authentication certificates, one might expect to observe a few particular conditions: a general lack of availability of a similar product offering anywhere else, few other competitors marked by steep barriers to market entry for newcomers and smaller companies, and high prices offered across the board. However, this particular market opposes conventional economic assumptions about how markets behave in a number of important ways, all with interesting implications for the future of website authentication certificates.

Market concentration

The impact of market concentration has an effect on the price of goods and services within a given market, with monopolistic or oligopolistic markets demanding higher prices for goods or services (especially those which are without substitute and also deemed necessary). Conversely, more competitive markets tend to drive the cost of these goods or services down.

The Herfindahl-Hirschman Index (HHI) is a relatively simple calculation and is widely used, among others, for competition law and anti-trust oversight as an indicator for competition by comparing firm size in terms of market share against the whole of the industry. It is based in the theoretical notion in economics that as concentration increases, that is, that output is concentrated in fewer companies, competition within the market will be weak. On the other hand, if market share is more equally distributed across the industry, competition within the market will tend to be strong.[22]

The most complete data set for website authentication certificate market share publicly available, in 2013, show an HHI of between 2220 (using data from Durumeric et al.) and 2250 (using data from Netcraft), indicating a moderate to relatively high market concentration per the generally accepted guidelines (over 2500 being the signal for high concentration). By 2015, the HHI has grown to over 2600 (using data from W3Techs) applying even the most generous parameters for calculation, indicating a substantial increase in market concentration over the course of the past few years. Given that in the present year only 8 companies (from a group of hundreds) command about 98% of the market, one would expect near monopolistic pricing strategies to be in effect. However, as can be seen, this assumption generally does not hold true.

Table 2 shows the market distribution among main players in the website authentication certificate market.

EV CERTIFICATE ISSUER	OVERALL MARKET SHARE[23]
Comodo	40%
Symantec	29%
GoDaddy	30%
GlobalSign	7%
DigiCert	3%
StartCom	2 %
Entrust	0.8%
Verizon Enterprise	0.6%

Table 2 Current approx. (2015) SSL/TLS market leaders

It may be of particular value to adopt regulations in the coming months and years which set a standard for trustworthiness to increase competitiveness in the website authentication certificate market, but which also encourages or facilitates standard adoption by new TSPs. The potential benefits are twofold. Not only would increasing competition drive long-term prices down for consumers (i.e. website and server systems owners), but could also help strengthen developed security standards as more TSPs improve themselves in order to meet officially recognized trust standards, especially for qualified website authentication certificates.

[22] Stephen A. Rhoades, The Herfindahl-Hirschman index, Federal Reserve Bulletin, 1993, issue Mar, pages 188-189, http://EconPapers.repec.org/RePEc:fip:fedgrb:y:1993:i:mar:p:188-189:n:v.79no.3

[23] W3TECH report on the usage of SSL certificate authorities for websites (data retrieved on November 2015), http://w3techs.com/technologies/overview/ssl_certificate/all

Low price competition

To get a more accurate sense of the economic climate within the market for website authentication certificates, a few additional pieces of information need to be considered including the degree of technical or actual difference between the product being offered and the variation thereof in price charged by each issuing company. One may expect to observe, in a market populated with hundreds of competitors offering perfectly substitutable products, a 'race to the bottom' of prices approaching marginal cost. However, the empirical data seem to suggest otherwise.

The market for DV certificates, exhibits the most normal price distribution. Though they offer lower standards of security, the lower cost of these certificates is one indication for their large share of the overall market. OV and EV markets, on the other hand, are characterized by a lower-weighted average price with extreme outliers towards the top of the price scale. Price competition is also highly varied among smaller vendors. For example, TSPs operating in countries such as Russia, Hungary, Poland, Turkey and the UAE, each holding less than a tenth of a per cent global market share, offer OV certificates at a price between €90 and €300 while the current leader offers the same certificate for about €115.

A direct comparison of asking prices also illustrates a fairly large variability in the market for Extended Validation certificates, supporting the notion of weak price competition in the market. This wide differential in prices would generally prompt the assumption that there exist substantial differences in quality or function between product offerings, and yet the certificates, within their own category of verification, are perfect substitutes.[24]

It would therefore appear that the market is driven by the influence of number of other 'non-essential' factors. Since buyers often cannot tell the difference between technical security features from one certificate to another (or between the security levels of their respective issuers), it would appear that the market for website authentication certificates is predicated on the commercial appeal of additional, bundled security, or certificate management services, warranties, and perhaps most consequentially, the perception of trust and an expectation of continuity by the larger competitors during the case of security failures.[25] Strategies to address these issues at the European Union and international policy level are underway, building off of successful implementation of regulatory devices in other trust services markets.

Brand trustworthiness versus information asymmetries

One particular place in which the market leaders excel is in the perceived trustworthiness of their brand. Even if website owners are aware of the fact that large TSPs have all fallen victim to successful attacks in recent years (and it has been the case in the past that security breaches have gone un-notified o with delayed notification[26][27]), having a leading brand adds a cover of safety that has little to do with the technical security of website authentication certificates or the HTTPS ecosystem as a whole.

[24] Arnbak, Axel and Asghari, Hadi and van Eeten, Michel and van Eijk, Nico, Security Collapse in the HTTPS Market, Com. of the ACM, Vol. 57(10), Oct. 2014, p. 47-55, http://ssrn.com/abstract=2537568

[25] ibid.

[26] Report of the investigation into the DigiNotar Certificate Authority breach: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf

[27] Adam Langley, Maintaining digital certificate security, Google online security blog, https://googleonlinesecurity.blogspot.gr/2015/03/maintaining-digital-certificate-security.html

Industry leaders have been instrumental in creating a more transparent and secure system, however, since the more notable breaches. Major browsers have developed stronger policies for the maintenance of their root stores and publication of revoked certificates. Furthermore, Google announced in late 2014, in its goal to bring “HTTPS everywhere”, that the use of a secure connection would begin serving as a website ranking signal, boosting SEO visibility and helping to build user trust in HTTPS services. Responsibility for observing better security practices has, in the past few years, been co-developed by market players, standardisation bodies such as ETSI, CEN, ISO and in informal working groups through the CA/B Forum, which aim to develop effective cross-border standards for operability and enforce conformity to these standards.

Quality of website authentication certificates

The electronic trust services market is built on just that: trust. Consumers, including individuals, enterprises and governments, need to have confidence that the system for website authentication is robust and that their private data remains secure. Website authentication certificates play an incredibly important role in this trust-based system. They need not only to employ highly advanced technological features, but they also need to inspire trust in the system as a whole. In particular, this means the creation of a single digital European market with uniform standards for data and consumer protection. With around 400 million EU citizens using the Internet, there is room for the development of value as well as impact in this area.

The policies that are currently under development at the EU level, in connection with the best practices that have been developed by website authentication certificate market players themselves, are the next step in generating value and trust, and moving forward. More specifically, the eIDAS Regulation was adopted by co-legislators in July 2014 and entered into force in September the same year. This and subsequently expected implementing legislation has facilitated the development of a better legal framework, in addition to technical guidelines and parameters, in consideration of markets for electronic identification and trust services.

4.3 Risks and barriers within the market

A number of issues arise from the systemic vulnerabilities within the HTTPS ecosystem and are impacted by a general lack of transparency in the market. These vulnerabilities illustrate where the system as a whole has needed help, and give rise to opportunities for the creation and implementation of better-defined standards in support of a healthier HTTPS ecosystem and a long-term strategy for improved security across the web.

Weakest link

All trusted root TSPs can issue a certificate for any domain, meaning attackers can target the weakest TSP for an attack. One single TSP can therefore compromise the security of the entire system. Because security is predicated on the success or failure of the weakest TSP, if any of the hundreds of them fails, the whole system suffers. This phenomenon is problematic for a number of reasons, and is perhaps an element that can help account for the reliance of certificate issuing organizations on emphasizing additional features while excluding technical information about certificates at the point of sale. Smart buyers and users understand that the market is based on a weakest-link system and that certificates are of comparable value and cannot guarantee total security. Regardless of this information and ongoing threats, the system is carried forward by necessity and it has relied on leading TSPs.

This is an important area of opportunity with readily available solutions. To reduce this burden on market leaders and to support higher quality from small TSPs, regulatory and industry wide initiatives are being developed which set standards in important areas such as identity verification, operational requirements and data protection. These measures have the ability to be strict, requiring high levels of commitment to quality and conformity across borders, while also being flexible and allowing local competent supervisory authorities to enforce and industry members to meet these standards in a way that encourages their individual and optimal abilities.

Too big to fail

As previously discussed, the largest trust services providers issuing website authentication certificates occupy a preponderant portion of the market for website authentication certificates. Asghari et al. [28] (2013) explore in depth the idea that the market leaders are in fact for a number of reasons too big to fail. They are able to offer more in depth services to large clients, provide a strong sense of implicit trust and a "liability shield" to those corporate leaders, and they are less likely to be removed from the trusted root stores of major browsers in the event of a security failure because of the system-wide catastrophic effects that would arise upon their disappearance. For government agencies, banking institutions, and other organizations that rely on continuity in their operations, market leading TSPs offer the ability to keep business running smoothly even during the course of a security failure. What is paid for, then, is the continuity of the system and availability of services rather than integrity and security. There is therefore a large incentive on the part of regulators to reduce this effect, especially due to the motivation of browser vendors to keep them in their root stores, even at a high potential cost to the system.

Since the most notable security breaches, however, the major browsers have already taken steps to overhaul internal procedures for the publication of certificate validity or revocation, and to enforce conformity to transparent policies by root (and other) TSPs. Likewise, by supporting all TSPs in their achievement of the framework for European standards, regulations can assist smaller TSPs to assume more of the responsibility for maintaining system-wide trust, which is currently carried by the market leaders.

Lack of breach notification

The consequences associated with instances when TSPs (or others) do not provide a notification of a security failure can be significant. The 2011 DigiNotar breach[29] (among several notable others) is frequently referenced in related studies and articles. Various organizations, including TSPs as well as website owners, have a strong incentive not to publicly disclose security breaches for fairly evident reasons. Breach notification is a largely public action; end-users can react negatively toward publicly untrustworthy organizations, hurting credibility and in some cases the ultimate continuation of operations. As discussed above, steps appear to have been taken by web browsers to reduce instances of negligence in reporting by instituting strict rules for noncompliance. This can be further be supported by mandates to divulge security breaches to proper authorities, and when appropriate, to the public. Transparency in this regard can help reduce the likelihood of security failures while boosting consumer trust in the system as a whole.

Liability dump

Clark & Borscht (2013) make the point that the HTTPS market has allowed for a greater sense spontaneity in achievement of one of the original goals of TLS: "an online world with great convenience."[30] This convenience, however, has not come without its price for the end-users who benefit from it. Browser trust stores catalogue TSPs who trust certificates, allowing users the freedom of using the Internet without themselves needing to make hundreds or thousands of choices on who or what to trust. However, users tend to be uninformed due to strong existing information asymmetries, and also tend to be the most affected by security breaches,

[28] H Asghari, M van Eeten, A Arnbak & N Van Eijk. Security Economics in the HTTPS Value Chain, WEIS 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2277806

[29] DigiNotar was subsequently acquired by VASCO Data Security International, Inc.

[30] Jeremy Clark and Paul C. van Oorschot, "SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements", 2013, http://users.encs.concordia.ca/~clark/papers/2013_sp.pdf

conditions which lead to the end user suffering the consequences of failure on the part of TSPs, website owners or other knowledgeable parties.

This is an opportunity to strengthen the entire system by marketing qualified certificates, increasing public visibility of new security features, and bringing easily accessible information to the table for less technical audiences. End-users have already responded well to security icons such as the URL 'lock' and browser security warnings, similar interactive cues could enjoy similar success, however considering as well that the amount of security information in the user interface needs to be compact to be effective. Bringing more transparency to the certificate chain of trust also stands to help shift the liability for security failures, rather than on the user community, back to their point of origin.

4.4 Outlook on how to handle risks and overcome barriers

The market for website authentication certificates has some unique features that present challenges and opportunities for the future. Competition can make the market healthier, yet the entrenched nature of the largest "too big to fail" trust service providers presents an obstacle to market diffusion.

Warning messages and icons like the padlock have already proven successful in communicating security to end-users without over-saturating user experience and diminishing the lasting power of the cues. Browsers have been systematically building white lists[31] for root authorities and issuing bans to those who do not adhere to strict policies, and there are expanding opportunities for website owners to more fully engage with this technology (correctly and uniformly). Incentives can be further created through policy for international TSPs operating on a regional level, specifically within Europe, to interact with other stakeholders within the HTTPS ecosystem to achieve enhanced security and system integrity as well as connectivity and continuity across the Web.

To date, the collaborative efforts of European policy such as eIDAS Regulation, standards and enforcement bodies such as ETSI and CEN, among others, have built and continue to foster a comprehensive set of recommendations and tools to satisfy the market's need for high standards as well as cross-border interoperability and conformity in matters of data security. These steps have already begun creating clearly high quality trust services, enhancing existing trust in electronic transactions in the market by providing a shared basis for secure electronic interaction between individuals, businesses and public authorities.

Some of the challenges and opportunities for the market that lie ahead include:

- Promoting healthy competition in the market (maintaining strict guidelines for high security while also allowing market entrants and small organizations to compete with fewer barriers),
- Building trust and value in the certificates themselves and in the HTTPS infrastructure, rather than the current commercial push for the bundled extras,
- Writing policy that encourages innovation as well as system-wide cooperation between all actors and stakeholders,
- Encouraging more website owners to participate in the system, and
- Encouraging easy-to-deploy certificates so that it is done uniformly and correctly system-wide.
- Solutions to these challenges will be introduced and discussed in the following sections.

[31] For Trust service Status Lists, see ETSI TS 119 612 Trusted Lists, http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/

5. The market of qualified providers

5.1 Introduction

Studies on the market for qualified trust services market, which, until the entry into force of the trust services provisions of the eIDAS Regulation in July 2016 covers only electronic signatures related services, are not as numerous as those on the website authentication certificate market. However, it is relevant for the study recommendations to take a glimpse of this market features, as already qualified providers of electronic signatures will probably be the first parties undertaking the commercialization of QWAC certificates.

A valuable source for information on the size of the qualified certificates for electronic signatures market are the trusted lists of the MS. The trusted lists, created under the scope of the eSignatures Directive, and which are also foreseen in the eIDAS Regulation, aim to provide reliable information related to the qualified trust service providers for which each MS is responsible, together with information related to the qualified trust services provided by them. Non-qualified trust service providers can voluntarily be included in the list.

The current composition per MS, as of September 2015, of the trusted lists provides detailed information about the number of qualified providers in Europe. Table 3 below shows there are 146 active trust service providers in Europe registered in the Trusted Lists issuing qualified certificates for electronic signatures for individuals.

MEMBER STATE	TSPS IN THE TRUSTED LIST	MEMBER STATE	TSPS IN THE TRUSTED LIST
Austria	3	Italy	30
Belgium	3	Latvia	1
Bulgaria	5	Lithuania	3
Cyprus	0	Luxembourg	1
Croatia	1	Malta	0
Czech Republic	3	Netherlands	8
Denmark	0	Poland	6
Estonia	1	Portugal	8
Finland	1	Romania	5
France	12	Slovakia	5
Germany	11	Slovenia	5
Greece	5	Spain	24
Hungary	3	Sweden	1
Ireland	1	United Kingdom	0

Table 3 Distribution of active TSPs in the Trusted List issuing qualified certificates per MS

The Trusted Lists show an uneven distribution of TSPs among MS, which is not directly related to population or to their presence in their global market. This unequal distribution can be attributed to several factors. For example, countries were qualified electronic certificates have been more widely required for online transactions with public administrations have seen an increase on the demand of this service and consequently the appearance of providers. Inversely, other countries where electronic signatures were required as well have evolved to a single solution for qualified electronic signatures certificates, in some occasions embedded in the national electronic ID card while in others stand alone. This single solution has been either provisioned directly by the government, or done in cooperation with sectors like postal companies or the banking, and no other entities have seen incentives to enter the market.

For countries with a large number of qualified providers, a noteworthy market feature is the strong presence of sectorial TSPs. An example of this are associations that provide services only to individuals from a particular professional domain, such as notaries or lawyers, and they do it as an added value for their associates. Similarly, several ministries and public organizations provide qualified trust services for their employees and systems. It is unlikely that these providers will enter the qualified website authentication certificates market to offer services for the general public.

Another remarkable aspect of the qualified providers market is that they are strongly oriented to their national market. Although some qualified providers offer commercial website authentication certificates in a global scale, a big percentage of them focus exclusively in national markets, offering services that comply with national trust services regulations that were developed after the entry into force of the eSignatures Directive. The introduction of the eIDAS Regulation is expected to have an effect in the strengthening of the single market.

5.2 Presence in the website authentication market

In 2013 ENISA conducted a survey among EU trust services providers, in which 46 participants took part. Its goal was to identify security practices in force at these organisations[32]. The results showed that a majority of the EU providers participating in the survey already issued different types of certificates. While 95% of the respondents reported issuing certificates for electronic signatures, making it the most common type of service, 80% of participants also reported issuing certificates for web site authentication. These figures show that a majority of European TSPs have an objective of providing an integral portfolio of trust services to their customers.

A method to study the current presence of European TSPs in the website authentication certificate market is to analyse their presence in the browsers' trust programs. 48.4% included in the Windows root certificate program are EU based, and this figure stands similarly at 41.5% in the case of Mozilla's program. Some more relevant data can be inferred by going further in this analysis, for example, 36% of TSPs present in the Windows program are also issuing qualified certificates. On the other hand, 12% of EU providers are present in the Windows program but not in the qualification market.

The explanation of the above might be twofold:

1. Firstly, only providers issuing qualified certificates are to be listed in the national trusted lists at the time being. Other services (such as time stamps) are included by some Member States in the trusted lists on a purely voluntary basis. With eIDAS, this is not anymore valid as all qualified trust services, including issuing QWAC certificates are to be listed.

2. The trusted lists established under the service directive are informative tools meaning that they are not granting any specific legal effect while the ones established under eIDAS are constitutive of the qualified status of a trust service provider and of the given trust service it provides (including QWAC certificates).

Despite a large number of TSPs issuing qualified certificates for electronic signatures present in the commercial website authentication certificate market, their market share is reduced. Based on the 2013 SSL/TLS ecosystem study, we can observe that 96.1% of hosts were secured by a website authentication certificate from a provider originating in a country with no qualified providers present, therefore setting a theoretical maximum of 3.9%

[32] For the in-depth description of the study, please refer to ENISA 2013 report "Guidelines for trust service providers - Part 1: Security framework", https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp1-framework

of deployed commercial website authentication certificates issued by TSPs offering also qualified certificates for electronic signatures.

This data shows some relevant facts, for example that the EU electronic certification is much more segmented than in other regions on the world and that EU providers are in general much smaller than their non EU counterparts. A rationale behind this may be that many European TSPs are focused on electronic signature certificates, which is a nationally oriented market, and issue other types of certificates, like commercial website authentication certificates, as an additional product, not as their core business model.

Regarding the presence in the Extended Validation certificates market, 18 out the 46 TSPs members of the CA/Browsers Forum issuing EV certificates are also present in the qualified certificates market. Comparing with data from the browser certificate programs, it can be inferred that only around one third of qualified providers issuing website authentication certificates are commercializing EV certificates. This number is still low if QWAC certificates are going to converge with EV requirements. This could slow down the adoption of qualified website authentication certificates.

6. SWOT analysis for the introduction in the market of QWAC certificates

In previous chapters, this study has explored the new trust services regulatory framework, the characteristics of qualified website authentication certificates, the commercial types of website authentication certificates and the web certification market. The objective of this report is to fully understand the website authentication certificate universe in order to produce recommendations on how to successfully introduce in the market qualified website authentication certificates.

To move further in the process of creating recommendations, the aim of this section is to conduct an analysis on the existing factors, external and internal, affecting the introduction on the market of qualified website authentication certificates. A SWOT analysis, as a strategic tool for evaluating strengths, weaknesses, opportunities, and threats, has been chosen to support the research on the main elements affecting the qualified website authentication certificates market in Europe.

The proposed SWOT analysis aims to identify internal and external factors that can impact positively and negatively the growth of the adoption of this new kind of trust services in Europe and the development of the related market. Strengths and weaknesses are identified as characteristics that give, respectively, an advantage or disadvantage among the internal factors of that market. Opportunities and threats are to be considered as external elements that, respectively, facilitate or hamper development conditions for the qualified website authentication certificates market in Europe.

The SWOT analysis results will serve as input to propose relevant recommendations that build on strengths, overcome weaknesses, seize opportunities and mitigate threats in the market. Figure 3 in the next page summarizes the main findings of the SWOT analysis, which are described in the next sections.

	STRENGTHS	WEAKNESSES
INTERNAL	Clarified legal framework of QWAC certificates	Small size of qualified providers
	Supervision by EU national authorities	National market orientation of qualified providers
	Clear requirement and appropriate methods for the identification of the requester of a QWAC certificate	Compliance cost burden and higher priced certificate costs
	Security breach notifications	
	Liability and damage coverage	
	Subject to EU data protection regulations	
	EU trust mark and trusted lists	
	Same technical security requirements as high quality commercial certificates	
EXTERNAL	OPPORTUNITIES	THREATS
	Growing adoption of electronic ecommerce	Website authentication certificate market dominance by a few players
	Increase in European electronic government services	Lack of browsers' recognition of the qualification model
	Growing security and privacy awareness	Lack of user understanding of the differences between types of website authentication certificates
	The Digital Single Market	Lack of market demand
	eIDAS Regulation – chance for education	Lack of differentiation by browsers
	Acquiring all services from a single provider	Many providers issuing low quality website authentication certificates
	Builds on an existing well known scheme	Lack of appeal for customers outside Europe
	Minimal adaptation for qualified providers	

Figure 3 SWOT analysis - market of qualified website authentication certificates

6.1 Analysis of strengths & opportunities

6.1.1 Strengths

Clear legal framework of QWAC certificates

Although the do not enjoy direct legal effect like other trust services, the clarified legal framework of QWAC certificates defined in the eIDAS Regulation can be an important pillar for its acceptance by website owners and end users. The provisions in the Regulation affect several aspects like liability, indemnities, termination, personal data protection, etc. All these requirements combined result in a unique, and one of the most complete, frameworks in the domain of information security products.

Supervision by EU national authorities

Qualified website authentication certificates can only be issued by qualified providers, which are subject to a strict supervision by designated supervisory authorities in Member States. The qualification model relies in a publicly governed harmonized scheme. This approach can be perceived by many customers as being more transparent, having a clearer governance framework, and providing higher assurance due to a legally mandated active monitoring of the due diligence of the providers.

Security breach notifications

A security breach notification obligation is imposed to all TSPs established in Europe, as an additional protection for the end user. There is a growing concern among end users on the lack of transparency in the internet regarding the protection of our data and whether some incidents involving them go unreported. With this legal obligation, customers will be assured that any breach involving either their cryptographic keys or their personal data will be reported to the supervisory authorities, and, if the certificate holders may be affected in any way, also to them.

Liability and damage coverage

Qualified providers, when faced with a dispute with a customer regarding the security in the provision of their trust services, will need to demonstrate that they were managing the service with the adequate level of security, i.e. the burden of proof will be with the provider. Furthermore, they will also be required to maintain insurance or sufficient funds to cover damage costs. These two provisions, which facilitate dispute settlement, move further into customer protection.

Subject to EU data protection regulations

Privacy concerns are raising among internet users, in the EU and globally. Qualified providers are subject to EU data protection laws and actively supervised by public designated bodies, which will cooperate with Data Protection Authorities in case of any violation of data protection law, assuring end users a proper management of their personal data in accordance with EU data protection regulations. Supervisory bodies will inform data protection authorities on the results of audits of QSTPs, where personal data protection rules appear to have been breached.

EU trust mark and trusted lists

The use of the EU trust mark[33], which QTSPs may use to indicate in a simple, recognisable and clear manner the qualified trust services they provide by providing a link to the relevant trusted list on their website, will give reassurance to customers about the confidence they can have on a certain trust provider. The EU trust mark will be easily recognizable and will visually associate the provider to the EU qualification framework.

Same technical security requirements as extended validation certificates

Technical security requirements for qualified website authentication certificates will be analogous to those of high quality commercial qualified website authentication certificates, such as EV certificates. Their differences lie in what refers to the legal, including the identification of the requester of the QWAC certificates, and supervisory framework, but from a technical security perspective, due to a planned compatibility of both schemes, QWAC certificates and EV certificates are expected to be largely equivalent. This might incentive EU users to acquire QWAC certificates, as they will offer a combination of the highest legal and technical protection available in the market.

6.1.2 Opportunities

Growing adoption of electronic ecommerce

The electronic commerce market (online transactions, shopping, payments, etc.) is still growing at a fast pace and it can be a key driver for qualified website authentication certificates market in the future. Businesses are becoming increasingly aware of the risks associated to online payment and the importance of trustable websites for users. There is also a place for using qualified website authentication certificates as well as steadily increasing online interactions in business-to consumer, business-to-business, and employer-to-employee relationships.

Increase in electronic government services

As with electronic commerce, the percentage of citizens' transactions with public administrations that are conducted online is growing rapidly. Public administrations are already a consumer of website authentication certificates, and they understand the risks associated to website fraud, as they have often been a targeted victim of phishing attacks. Moving to qualified website authentication certificates seems a natural choice for public administrations, as they are involved in the governance, transparency and accountability of the scheme.

Growing security and privacy awareness

The amount of personal data being collected and processed online is growing exponentially. Website authentication certificates are a critical component in the security of the interaction among internet users and online services. They provide assurance of the identity of the online service owner and they are used to encrypt the communication. Qualified website authentication certificates, which will be recognized by the EU trust mark by website owners, can support users' quick and better assessment on the legitimacy and security of an online service.

[33] EU trust mark competition: https://ec.europa.eu/digital-agenda/en/news/e-mark-u-trust-competition-trustmark-design-wanted

The Digital Single Market

The Digital Single Market strategy of the European Union is based on three pillars: better access for consumers and businesses to digital goods and services across Europe; creating the right conditions and a level playing field for digital networks and innovative services to flourish and maximising the growth potential of the digital economy. With trust services being a key building block of the digital market, horizontal actions linked to the Digital Single Market will facilitate the creation of a European single trust service market.

eIDAS Regulation – a chance for education

Thanks to the eIDAS Regulation, there is a chance to educate users on what website authentication certificates are, their role on the security of different platforms, applications, and browsers. This can be achieved by preparing material on website authentication certificates and how to read content of the certificates. It will also help to comprehend features of qualified website authentication certificates.

Acquiring all trust services by a single provider

The possibility for a customer, such as a public organization, to acquire all their certificates from a single trusted source, can facilitate the introduction of qualified website authentication certificates and constitutes an opportunity for providers of qualified certificates for electronic signatures to move into the domain of website authentication.

Builds on an existing well known scheme

The new eIDAS Regulation builds upon a scheme that has successfully been adopted in Europe for years now, i.e. electronic signatures. Qualified certificates for electronic signatures are extensively used in Europe, especially, but not only, in online public services. Thanks to electronic signatures, users already understand the concept of qualification and its implications in terms of guarantees for them. This will facilitate the introduction of other qualified trust services.

Minimal adaptation effort for qualified providers

Once a TSP has undergone all the procedures to become qualified to provide a trust service such as electronic signatures, providing other qualified trust services should not require a large additional effort. This can facilitate the early introduction of qualified website authentication certificates by already qualified providers.

6.2 Analysis of weaknesses & threats

6.2.1 Weaknesses

Small size of qualified providers

Studies show that QTSPs (the most likely providers to start using qualified website authentication certificates) are small players in the commercial website authentication compared to their counterparts from other countries (e.g. 96.1% of certificates are issued from TSPs based on countries with no accredited QTSPs). Competing with large players can be challenging, as within any market, and this can be an important deterrent for the large adoption of qualified website authentication certificates.

National market orientation of qualified providers

So far, qualified trust service providers of electronic signatures certificates have been focusing largely on their national markets, issuing certificates compliant with national legislations adopted pursuing the eSignatures Directive. The eIDAS Regulation comes with a strong spirit of harmonization, however, in so far, qualified certificates are still mostly nationally oriented market, which has reduced the size of their potential market. Furthermore, another disadvantage derived from the national orientation is that in the global market of website authentication certificates brand recognition is important for placing trust and many providers are largely unknown outside of their country.

Compliance cost burden and higher priced certificate costs

Website authentication certificates are a market with a low price competition, sensible to small prices changes. Potential higher cost of qualified website authentication certificates due to stronger requirements can deter clients to purchase them for their websites if the benefits of qualified website authentication certificates are not properly communicated, if clients perceive that the risk does not justify the investment, or if end users don't create demand. Currently, neither website owners nor users are fully aware that the use of less quality certificates with less guarantees can lead to the materialization of threats phishing.

6.2.2 Threats

Market dominance by a few established non-qualified players

The trust services market in Europe is currently polarized, with many small, qualified providers focusing on qualified services for electronic signatures and a few very large players focusing on commercial website authentication certificates, with the later having no presence in the qualified trust services market. The existing market for website authentication certificates is highly concentrated, despite the large number of issuers (75 % of website authentication certificates in use on the public web have been issued by just three companies: Symantec, GoDaddy, and Comodo)[34]. These companies may not see enough drives to start issuing qualified website authentication certificates, while QTSPs will need to compete with very established players with this new product.

Lack of browsers' recognition of the qualification model

Nowadays, browsers play a major and increasingly important role in the initiatives towards establishing a trust model for TSP issuing website authentication certificates (e.g. how certificates are accepted, recognized and presented by browsers in their user interfaces). Currently, the browser market is dominated by a few global companies targeting customers around the world, operating in a self-regulated environment. Browsers may find few incentives in recognizing the qualification model, which, for the moment, would be acknowledged by users from a sole region, i.e. the EU.

Lack of user understanding of the differences between types of website authentication certificates

Website owners and end users may find it difficult to understand the differences among various types of website authentication certificates. Even for advanced internet users it is not always trivial to comprehend all the legal, governance, technical and quality aspects that differentiate website authentication certificates. It will require proactive actions from the stakeholders to help users understand the full website authentication certificate ecosystem.

[34] Arnbak, Axel and Asghari, Hadi and van Eeten, Michel and van Eijk, Nico, Security Collapse in the HTTPS Market, Com. of the ACM, Vol. 57(10), Oct. 2014, p. 47-55: http://ssrn.com/abstract=2537568

Lack of market demand

An increasing demand for website authentication certificates is expected to grow in parallel with the increase of internet transactions. However, if benefits of qualified website authentication certificates are not properly communicated or perceived by users, a preference for this type of certificates will not necessarily develop in Europe. Without a website owners' or end users' demand, providers will have no incentives to issue QWAC certificates.

Lack of differentiation by browsers

Browsers' recognition of trust service providers and inclusion in their trusted root stores is a critical element for trust service providers. Without this inclusion, customers are prompted with a warning by their browsers. This warning by itself triggers trust concerns in the customer. TSPs are able to enter the browsers' trust stores by following the required audit programs, for example to be audits based on ETSI standards. A further step in this direction is that, in order to facilitate user recognition of high quality certificates, some browsers have introduced the green bar tab for websites that use EV certificates. Ideally, a different scheme (e.g. blue bar) could be introduced for qualified website authentication certificates to facilitate recognition. However this differentiation is not foreseen yet; even more, unless the provider complies with the EV guidelines as well as the qualification framework, the bar will remain grey.

Many providers issuing low quality website authentication certificates across the world

A threat for qualified website authentication certificates, and for high quality certificates in general, is that there is still a large number of TSPs around the world issuing low quality website authentication certificates, such as DV certificates, which have high demand because of their low price. The reduced cost is due to a very simple online procedure for the registration process. Although using DV certificates add benefits compared to using unencrypted links, they might not be suitable for all organizations, they can later cause security risks associated to impersonation (Recently there have been some reported cases of phishing sites have started to use automated DV certificates to deceive users[35]). But end users do not fully understand the difference, and more costly certificates, with more secure validation procedures, have not reached a majority of market share.

Lack of appeal for customers outside Europe

Qualified certificates may not be in the near future demanded outside of Europe, as non-EU customers may feel there is no incentive for them to acquire certificates protected by a regulatory framework outside of their territorial jurisdiction. At the same time, providers may reflect that by issuing qualified website authentication certificates they are restricting themselves to the European market, which, although being one of the largest digital markets in the world, sets a limit from a global market. However, other aspects may be leveraged in favor of QWAC certificates, such as increasing trust of European customers, even for non-EU businesses. Furthermore, in the EU qualification system becomes a reference in terms of quality, this may itself be an incentive to purchase QWAC certificates globally.

[35] Netcraft news, Certificate authorities issue SSL certificates to fraudsters, retrieved October 2015: http://news.netcraft.com/archives/2015/10/12/certificate-authorities-issue-hundreds-of-deceptive-ssl-certificates-to-fraudsters.html

7. Recommendations for the successful introduction in the market of qualified website authentication certificates

The overall goal of the eIDAS framework in the area of website authentication must be to radically increase the number of website authentication certificates securing websites located within the EU, and to step-up the percentage of those websites that use higher assurance certificates by promoting the use of qualified website authentication certificates, in order to increase trust among European customers and boost online transactions.

To achieve this, our study has identified short-term, medium-term and long-term strategies, which come as the result of the market and SWOT analysis conducted in the previous chapters. All the strategies have been broken down in concrete recommended actions that should be undertaken to achieve them.

The six strategies and twelve recommended actions propose an escalated approach that targets the most important aspects detected to be critical for (i) improving the website authentication market in Europe and (ii) successfully introducing qualified website authentication certificates as a mean to increase transparency in this market.

7.1.1 Short-term Strategies

I. INCREASE THE NUMBER OF WEBSITES USING WEBSITE AUTHENTICATION CERTIFICATES IN EUROPE

Recommended action **EU governments and web browsers developers should increase efforts to help end users understand the key role website authentication certificates play in protecting their personal information and their online transactions.**

Rationale Demand by users should be a driving force to incentive adoption of website authentication certificates by website. To create this demand, end users need to better understand what website authentication certificates are and how they protect the personal information they transmit and the online transactions they perform via websites.

Detail Stakeholders should create online campaigns and resources with a clear and easy to understand information, targeted to the general population, to assist in understanding the risks associated to unsecure connections and how website authentication certificates can mitigate many of the risks.

Output Increase demand for website authentication certificates and users' trust in online transactions

Recommended action **EU governments and trust service providers should undertake initiatives to communicate to website owners the importance of using website authentication certificates to protect themselves from fraud**

Rationale Website owners should be made aware of the benefits website authentication certificates in general add to their websites; especially to protect themselves and their customers against online fraud. They should also understand that their websites are perceived to be less secure than those using website authentication certificates and that trust can been seen as an asset.

Detail This awareness raising might take the form of online campaigns and resources, as well as stakeholder conference presentations. Emphasis should be focused on risk reduction, consistency of certification, increased reputation and customer protection.

Output Increase in the total number of websites deploying website authentication certificates.

Recommended action **All involved stakeholders should try to communicate more clearly to users the different types of website authentication certificates and their distinct assurance level**

Rationale Website owners and end users may find it difficult to understand the differences among different types of website authentication certificates. Even for advanced internet users it is not always trivial to comprehend all the legal, governance, technical and quality aspects that differentiate website authentication certificates.

Detail Stakeholders (in particular developers of browsers) should create a consistent terminology with clear descriptions to help users (both website owners and end users) to understand the differences between existing website authentication certificate types, together with practical examples.

Output Increased trust through a clear understating by users of differences among website authentication certificates.

II. ESTABLISH A MARKET FOR QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES

Recommended action **Public administrations at all EU levels should lead the way in the adoption of qualified website authentication certificates**

Rationale Public administrations should be early adopters of QWAC certificates, as this would establish a critical mass of usage at an early stage and encourages vendors to supply QWAC certificates.

Detail EU institutions and EU governments should recommend and implement the use of QWAC certificates in all public services web portals. By adopting the qualification scheme they provide a consistent image regarding their support for online security and privacy protection measures that will increase citizens' trust.

Output Early adoption of qualified website authentication certificates by Member State administrations' on official websites.

Recommended action **Qualified providers should consider to provide a full range of trust services to seize more business opportunities**

Rationale Qualified services could become an integral business model for providers, instead of focusing on a particular service. This is an added value for customers, which can acquire all services from a single provider.

Detail Qualified providers focused on certificates for electronic signatures should consider taking advantage of the provisions of the eIDAS Regulation to offer, with a low adaption cost, a full range of trust services (e.g. signatures, seals, time stamps and website authentication certificates).

Output Qualified providers will strengthen their position in the global website authentication certificate market by providing an integral portfolio of trust services

III. ALIGN EXISTING REGULATORY AND INDUSTRY LED INITIATIVES

Recommended action **EU regulators should take into account existing good practices from industry led initiatives during the implementation of the eIDAS regulation**

Rationale Website authentication under the eIDAS Regulation builds upon CA/Browser Forum's work. In this context, it might be considered to launch an EU implementing action taking into account the good practices that emerged from this and industry-led initiatives.

Detail In the context of the implementing activities carried out under the eIDAS framework, guidelines supporting the implementation of security measures should be provided in order to facilitate trust service providers' compliance with their obligations. The good practices developed by the CA/Browser Forum EV guidelines (or other industry-led initiatives) could be referred to in such recommendations, as measures to ensure the level of security is commensurate to the degree of risk for TSPs issuing QWAC certificates.

Output Increased alignment between existing practices as well as economic and legal certainty for trust service providers aiming at matching the requirement of the Regulation.

7.1.2 Medium-term Strategies

IV. INCREASE RECOGNITION OF QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES BY END USERS

Recommended action **EU Regulators and qualified providers should promote the acceptance of qualified website authentication certificates by browsers, as an equivalent to high quality certificates or with their own distinctive feature.**

Rationale The CA Security Council, in its 2015 Consumer Trust Survey[36] found that 42 percent consumer respondents associated the green bar and organization name in the URL with greater safety.

Detail In order for users to easily recognise QWAC certificates, it is important to create a clear differentiator between the QWAC certificates and high quality commercial certificates versus other less quality certificates in the browsers' interfaces. Direct approaches to browsers and SDOs should be conducted to advance in this area. The differentiator should ideally be clearly visible to any user without any action on their part.

Output Visual acknowledgement on browsers that QWAC certificates are securing a website as equivalent to EV certificates

Recommended action **EU Member States should support the recognition of the EU trust mark through nationwide promotions as part of NIS and cybersecurity campaigns**

Rationale Promoting trust enhancing instruments should be considered as a seamless action as part of cybersecurity best practice.

Detail The EU trust mark should be given prominence to increase recognition. EU institutions should liaise with NIS initiatives across the EU Member States to make sure that the use of QWAC certificates is promoted in all campaigns, together with the eIDAS Trust Mark.

Output Recognition of the EU trust mark, raised awareness of QWAC certificates among end users

[36] CA Security Council Consumer Trust Survey Report, 2015: https://casecurity.org/2015/04/13/ca-security-council-report/

V. STRENGTHEN THE MARKET POSITION OF QTSPS

Recommended action **Qualified providers should cooperate to strengthen their position in the website authentication certificate market**

Rationale QTSPs are currently of a small size, especially if compared to players in the global website authentication certificate market. Strategies to strengthen them will benefit the deployment of QWAC certificates overall.

Detail Associations and forums of providers should be promoted in order to increase competitiveness of qualified providers; for example, by creating consortiums from providers that serve different national markets. Providers focusing on different trust services can also cooperate to offer full range of services.

Output Larger qualified providers who will become better positioned to compete in the website authentication certificate market.

Recommended action **EU institutions and governments should incentivize qualified providers to expand beyond their national market**

Rationale QTSPs are currently mostly oriented to their national markets, missing businesses opportunities in a global market like website authentication certificates.

Detail EU governments should give incentives and support the expansion of their national qualified providers to the European and international market. They should also support providers to create a branding that is recognisable by the general public in Europe.

Output Qualified providers will strengthen their position in the global website authentication certificate market by reaching more potential customers.

VI. SUBSTANTIALLY INCREASE THE MARKET SHARE OF QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES

Recommended action **EU institutions and governments should communicate to businesses the benefits the clarified legal framework of qualified website authentication certificates will offer them**

Rationale EU businesses should understand the legal framework QWAC certificates offer them, in order to be able to make an informed decision when choosing how to secure their website.

Detail Create a clear documentation and online resource to assist in understanding the benefits of QWAC certificates for businesses as presented in this document, and introduce them as a solid choice for website authentication certificates within the EU.

Output Increased adoption of qualified website authentication certificates among EU businesses.

Recommended action **EU institutions and governments should promote the use of qualified website authentication certificates by targeting specific critical sectors such as health and finance**

Rationale There are specific sectors with higher requirements in terms of privacy and integrity of the transactions that can especially benefit from the legal provisions and additional protection for the customer features that the qualification scheme offers.

Detail EU Institutions and governments should make specific campaigns to raise awareness of the benefits of qualified trust services for critical sectors, where some features of QWAC certificates such as liability, legal presumption of integrity and authenticity, or mandatory breach notifications could be perceived as important protection measures.

Output Increase use of qualified website authentication certificates in online transactions in European critical sectors.

7.1.3 Long-term Strategy

VII. MAKE QUALIFIED WEBSITE AUTHENTICATION CERTIFICATES THE REFERENCE FOR HIGH QUALITY WEBSITE AUTHENTICATION CERTIFICATES GLOBALLY

Recommended action	**EU institutions should promote the recognition of qualified website authentication certificates outside of the EU as a high quality product**
Rationale	EU organisations and customers need to trust non-EU websites and servers and QWAC certificates can be an instrument to facilitate this trust by European users.
Detail	Non-EU businesses will realise that EU organisations and customers will be more likely to trade if there is trust, and if jurisdictional disparities are resolved through common certificate practices. Encouragement could be given to European trade insurers to consider a positive asset for organizations having their online trust is assured through EU regulations and law.
Output	Increased adoption of website authentication certificates by non EU organizations

Annex A: Analysis of the website authentication certificate market

This section utilizes comprehensive studies of the HTTPS ecosystem from the past several years to reveal important implications and considerations for the current status and future growth of the market for trust certificates. These data have been obtained from a number of different sources; two of the more important studies of which are the 2010 EFF SSL/TLS Observatory and the exhaustive HTTPS ecosystem scans which Zakir Durumeric et al. at the University of Michigan performed between 2012 and 2014. These two studies scanned the entire public IPv4 address space, performing handshakes with all public-facing HTTPS servers, systematically identifying and analysing trustworthiness for all SSL/TLS certificates accessible on port 443. Additional data, analysis and information come from current studies conducted by, among others, Netcraft, W3Techs and universities in Europe and the United States.

The empirical information acquired from these studies presents deeply useful statistics about the market for website authentication certificates in general, and reveals some interesting facts about the market which are somewhat contrary to economic intuition.

A.1 Size of the global website authentication certificate market

The market for website authentication certificates has grown exponentially in the past few decades. According to a recent SSL/TLS Server Survey release by Netcraft, there is currently more than one thousand times the number of certificates today as there were in 1996.[37] The global ecosystem is populated by an estimated 250-700 organizations providing trust services[38], though the website authentication market is dominated by a small handful of larger companies.

The top three spots in the past few years have been held by Symantec, Comodo and GoDaddy (with GlobalSign trailing close behind in position four), which account for nearly three-quarters of all issued website authentication certificates, though through mergers, acquisitions, and other market forces, these positions are subject to a level of unpredictability and change. To illustrate this point, consider the effect of the past two years in the market. In May 2013, Symantec issued over a third of trusted website authentication certificates, GoDaddy 29%, Comodo 15% and GlobalSign 5%.[39] By the same time in 2015, Comodo had risen to first place with nearly 37%, followed by Symantec with 31%, GoDaddy with less than half at 14%, and GlobalSign on an apparent rise with over 10%, double its 2013 market share.

Netcraft and others have publicly speculated the possibility of smaller, more innovative companies shaking up the market by offering free certificates in conjunction with other user-friendly benefits. While these product offerings are hardly new to the market, support from a variety of key actors along the electronic trust services value chain could permanently and fundamentally alter the HTTPS ecosystem. However, the current state of the market is characterized by a high overall number of TSPs (each generally with 0.1% or less of the market share), but with the bulk of economic weight located in only a few large corporate competitors.

The information derived from the 2013 Durumeric et al. SSL/TLS ecosystem study (in Table 4 in the next page) provides a comprehensive look into the size of the "demand side" of the market for website authentication certificates. Read left to right, the table represents a longitudinal study during the course of the years 2010 to

[37] Netcraft news, Counting SSL certificates, May 2015, retrieved October 2015: http://news.netcraft.com/archives/2015/05/13/counting-SSL/TLS-certificates.html

[38] Arnbak, Axel and Asghari, Hadi and van Eeten, Michel and van Eijk, Nico, Security Collapse in the HTTPS Market, Com. of the ACM, Vol. 57(10), Oct. 2014, p. 47-55: http://ssrn.com/abstract=2537568

[39] Netcraft SSL Survey, 2013: http://www.netcraft.com/internet-data-mining/ssl-survey/

late 2013. A few pieces of information can readily be extrapolated from this set of data: Market saturation has not yet been reached and is still expanding with plenty of room for growth.

A number of factors help fuel regular demand, and the creation of a sense of necessity for secured connection can ever increase the value of the market, especially given that a recent release from W3Techs shows nearly 40% of websites use no website authentication certificate. That is to say, 15% of all websites represent 100% of the market, meaning that approximately 85% of the total market is still untouched. However, it is not clear what per cent of internet commerce (or of other sectors) is captured by this 15%.

SCAN DATE COMPLETED	EFF (2010-8)	PS & QS (2011-10)	FIRST (2012-6)	REPRESENTATIVE (2013-3)	LATEST (2013-8)	TOTAL UNIQUE
Hosts, port 443 open (millions)	16.2	28.9	31.9	33.1	36.0	unknown
Hosts service HTTPS (millions)	7.7	12.8	18.9	21.4	24.4	108.8
Unique Certs (millions)	4.0	5.8	7.8	8.4	9.0	42.4
Unique Trusted Certs (millions)	1.5	1.9	2.9	3.2	3.3	6.9
Alexa Top 1 Mil. Certs (thousands)	unknown	89.9	116.1	141.2	143.2	261.3
EV Certs (thousands)	33.9	71.1	89.2	103.2	104.2	186.2

Table 4 Internet-wide scan results on port 443, collection of website authentication certificates from responsive hosts

The interesting fact within the market about individual pricing strategies makes it somewhat difficult to define a more accurate economic forecast, but there are a few factors that would indicate an increase in market strength. A steady increase in the annual number of total unique certificates over the past many years, the average price per certificate from the top issuers, and the fact that only 15% of total number of websites globally are represented, all point towards the reasoning that the market is currently at a place for further expansion and is of high potential value.

A.2 Distribution of the market based on types of certificates

Table 5 below shows the percentage of the website authentication certificates deployed based on the identity validation procedures, which are inversely related to price.

CERTIFICATE TYPE	DEPLOYED MARKET	MIN PRICE	MAX PRICE	AVERAGE
DV	70%	€0	€232	€72
OV	26%	€34	€1050	€231
EV	4%	€89	€1361	€557

Table 5 Market range of website authentication certificates based on identity[40]

There are several reasons for the dominance of the DV over the OV. A possible explanation is that browsers do not distinguishing visually between DV and OV, they set the “security bar” at the EV level, resulting in a

[40] H Asghari, M van Eeten, A Arnbak & N Van Eijk. Security Economics in the HTTPS Value Chain, WEIS 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2277806

binary condition in which either EV or non-EV certificates are recognized. This might disincentive website owners to purchase OV certificates, as they are treated analogously to DV by browsers, with the later having an effective lower price.

At the same time, the DV segment TSPs are currently facing extreme competition from various actors:

1. Let's Encrypt[41] is an initiative aiming at delivering automatically DV certificates to any website. On October 2015, Let's Encrypt announced that they have been cross-signed by IdenTrust[42], meaning that all browsers now trust Let's Encrypt certificates. Request and issuance of a Let's Encrypt certificate is entirely automated (as well as configuration of the web server if needed), so the whole process is very simple.
2. Cloudflare is a cloud-based content delivery network which offers free DV certificates to their users. Even their free offer includes free SSL/TLS[43].
3. Finally, some CAs offer free DV certificates under special conditions[4445].

As a consequence, the market for commercial DV certificates could significantly shrink in the coming years due to this free and aggressive competition. As OV certificates are somewhat of an in-between solution and don't benefit from any special visual indication in browsers, there does not seem to be much reasons for future increase of their adoption. This leaves EV certificates, on which I expect CAs to refocus in the coming years. A recent study claims that the EV SSL/TLS market will grow on average 32% per year until 2019[46].

Regarding number of domains secured, Table 6 below shows the percentage of the domains registrations opt for a single domain, while only 20% of the website authentication certificate purchases are for a multi-domain or wildcard certificates. It should be noted that, according to CA/B Forums guidelines, EV certificates do not allow wildcards, but do allow multiple domains.

CERTIFICATE "DOMAIN" TYPE	MARKET DEPLOYMENT
Wildcard	9%
Multi-domain	11%
Single -domain	80%

Table 6 Market range of website authentication certificates based on domain registration

[41] Let's Encrypt: https://letsencrypt.org

[42] Let's Encrypt is Trusted, Retrieved October 2015: https://letsencrypt.org/2015/10/19/lets-encrypt-is-trusted.html

[43] CloudFlare one-click SSL: https://www.cloudflare.com/SSL/TLS

[44] Start SSL free certificates, https://startSSL/TLS.com/?app=33

[45] Wosign free certificates, https://buy.wosign.com/free/

[46] Reuters, The Global EV SSL Certification Market Will Pass the US$550 Million Mark by 2019, March 9 2015, retrieved October 2015: http://www.reuters.com/article/2015/03/09/technavio-idUSnBw095266a+100+BSW20150309

A.3 Geographic distribution

In the 2013 SSL/TLS ecosystem scan, 9 million certificates from 24.4 million IP addresses were retrieved, of which more than a third were browser-trusted. Mapping TSPs showed them spread across 57 countries worldwide.[47] However, and according to the data collected, over 98% of both trusted certificates as well as hosts serving trusted certificates were actually located in only ten countries across the world.

COUNTRY	AUTHORITIES	CERTIFICATES	HOSTS
United States	30.3%	77.6%	75.6%
United Kingdom	3.3%	10.9%	18.2%
Belgium	2.7%	3.3%	1.5%
Israel	1.6%	2. 6%	0.9%
Netherlands	2.2%	1.3%	0.5%
Japan	3.4%	1.1%	1.2%
Germany	21.3%	0.9%	0.4%
France	4.0%	0.4%	0.1%
Australia	0.8%	0.3%	0.1%
Korea	1.4%	0.2%	0.1%

Table 7 Geographic distribution of top 10 countries issuing trusted certificates, 2013 [48]

Table 7 above shows the geographic breakdown of these figures and reveals some interesting ideas about the state of and potential direction of movement in the global market for trusted certificates. The United States currently holds the most authorities, certificates and hosts, though Germany by itself comes in second with over a fifth of global trust service providers issuing publicly trusted website authentication certificates. The EU in total has over a 33% of these trust service providers, nearly 17% of issued trusted certificates and over 20% of hosts reside within the EU member states. These are not insignificant numbers, especially in comparison with the figures from the rest of the top countries from the list.

The market landscape has transformed somewhat in the past few years, affected by mergers and acquisitions and by an increased presence in Asia. Access to the Chinese trust services market is highly regulated, and only a small number of commercial vendors such as WoSign have relevant market shares.

Another indicator we can use to measure the number of active TSPs per region is a sample browser root store. For example, in the case of the Windows root certificate program[49], which incorporates the TSPs that come included by default in windows products. There are 132 organizations included (note the aggregate number is higher due to some TSPs having more than one issuing CA or different legal entities under the same parent company). Out of them, more than half are originating from Europe.

[47] c Arnbak, Axel and Asghari, Hadi and van Eeten, Michel and van Eijk, Nico, Security Collapse in the HTTPS Market, Com. of the ACM, Vol. 57(10), Oct. 2014, p. 47-55: http://ssrn.com/abstract=2537568

[48] Zakir Durumeric, James Kasten, Michael Bailey, J. Alex Halderman, Analysis of the HTTPS certificate ecosystem, October 2013 IMC '13, http://conferences.sigcomm.org/imc/2013/papers/imc257-durumericAemb.pdf

[49] Windows Root Certificate Program - Members List (All CAs): http://social.technet.microsoft.com/wiki/contents/documents/2592.windows-root-certificate-program-members-list-all-cas.aspx

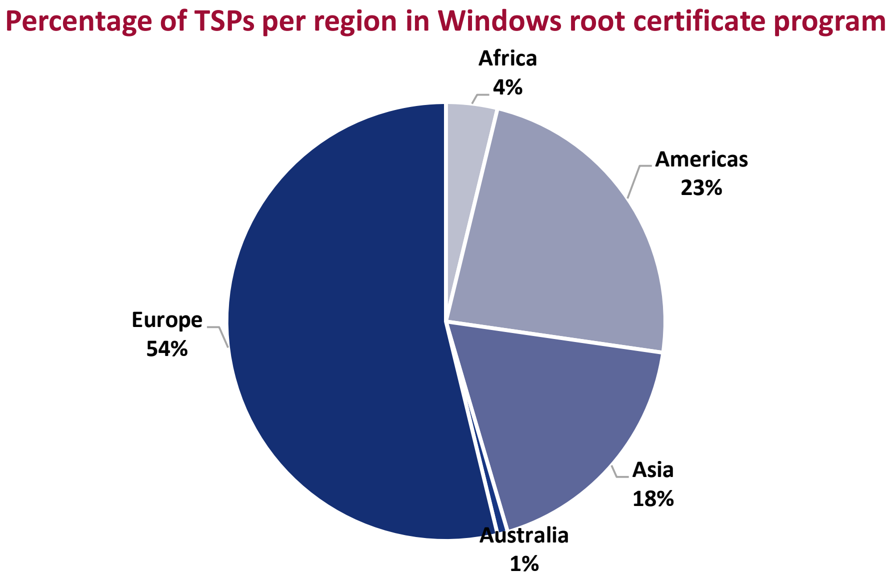
Percentage of TSPs per region in Windows root certificate program

Figure 4 Percentage of TSPs per region in Windows root certificate program

We can find a similar regional distribution in the case of Mozilla Included TSP certificate list[50], which incorporates the TSPs that come included by default in Mozilla products. There are 65 organizations included (again note the aggregate number is higher due to some having more than one issuing CA or different legal entities under the same parent company). Again, nearly half of them are of European origin.

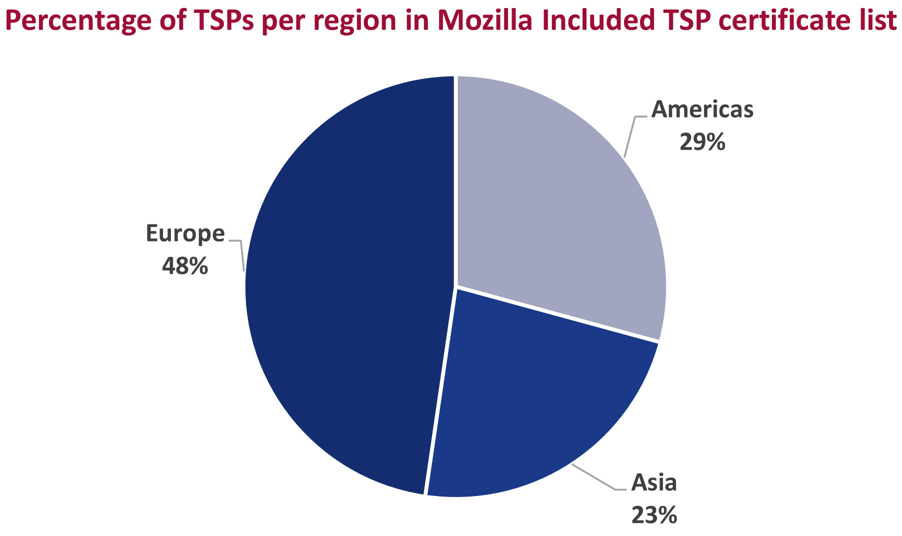
Percentage of TSPs per region in Mozilla Included TSP certificate list

Figure 5 Percentage of TSPs per region in Mozilla Included TSP certificate

Data from the SSL/TLS ecosystem scan and browsers trusted TSPs lists are more or less consistent, and show that (i) a majority of the TSPs are located in Europe, and (ii) many active EU trust service providers, present in browsers trust stores, have a negligible share in the website authentication market.

[50] Mozilla Included CA Certificate List: https://wiki.mozilla.org/CA:IncludedCAs

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-04-15-888-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-152-6,
DOI: 10.2824/464966