Linköping University | Department of Computer and Information Science
Bachelor's thesis, 15 ECTS | Information Technology
2021 | LIU-IDA/LITH-EX-G--2021/065--SE

Public certificate management

– An analysis of policies and practices used by CAs

Offentlig certifikathantering: En analys av policys och praxis som används av CAs

Emily Berghäll
Anna Bergström

Supervisor : Niklas Carlsson
Examiner : Marcus Bendtsen

Linköpings universitet
SE–581 83 Linköping
+46 13 28 10 00 , www.liu.se

Upphovsrätt

Copyright

Abstract

Certificate Authorities (CAs) carry a huge responsibility in today's internet security landscape as they issue certificates that establish secure end-to-end connections.

This thesis conducts a policy review and survey of CAs' Certificate Policies and Certificate Practice Statements to find similarities and differences that could lead to possible vulnerabilities. Based on this, the thesis then presents a taxonomy-based analysis as well as comparisons of the top CAs to the Baseline Requirements.

The main areas of the policies that were focused on are the issuance, revocation and expiration practices of the top 30 CAs as determined by the use of Tranco's list. We also determine the top CA groups, meaning the CAs whose policies are being used by the most other CAs as well as including a top 100 CAs list. The study suggests that the most popular CAs hold such a position because of two main reasons: they are easy to acquire and/or because they are connected to several other CAs.

The results suggest that some of the biggest vulnerabilities in the policies are what the CAs do not mention in any section as it puts the CA at risk for vulnerabilities. The results also suggest that the most dangerous attacks are social engineering attacks, as some of the stipulations for issuance and revocations make it possible to pretend to be the entity of subscribes to the certificate rather than a malicious one.

Acknowledgments

We want to thank our supervisor Niklas Carlsson for the advice and guidance with this thesis. We also want to thank Max Danielsson, Adam Halim, Nina Lindström and Sebastian Klasson for the work on the joint project, the results of which were used for this thesis.

Also, we would like to thank Otto Engström Heino, Richard Johansson, Clara Gallon, Rebecca Södereng, Sofia Bertmar and Johanna Gerhardsen for reviewing our thesis and providing feedback.

Contents

List of Tables

1 Introduction

In today's trust landscape Certificate Authorities (CAs) carry a huge responsibility as a trusted third party. The CAs issue certificates to create secure end-to-end connections, that assure ownership of a particular public key. Certificates are the foundation of Public Key Infrastructure (PKI) of insecure public networks, which makes it of great importance to internet security.

The number of CAs on the market keeps increasing and a closer look indicates that there might be distinct differences regarding the certificate policies as well as the success of CAs. These differences may leave CAs vulnerable, as a smaller difference in practices can end up having a big impact when dealing with major processes such as issuance, revocation or expiration of certificates.

This paper conducts a survey and a policy review to examine if there are such vulnerabilities in the issuance, revocation or expiration processes of the policies, as these are the largest parts of certificate management. The results of this paper will have structured a taxonomy-based analysis of policies from the top CAs as well as a vulnerability analysis.

1.1 Aim

This thesis aims to build a taxonomy-based analysis of the public certificate management policies and practices used by the most popular CAs using the public certificate policies. More specifically, the study investigates the issuance, revocation and expiration processes, to see if any of these might impact the vulnerabilities or popularity of the CAs.

1.2 Research questions

Through the combination of policy review and survey, this thesis answers the following questions:

1. What similarities and differences can be found in the Baseline Requirements (BR) and the policies regarding issuance, revocation and expiration?
2. Do the distinctions impact the popularity of the CAs?
3. To what extent do the distinctions impact the vulnerabilities of the CAs?

1.3 Delimitations

This report introduces some delimitations in regards to which data will be analyzed. The first of these delimitations is that this study will only entail studies of selected CAs policies. This means that there could be results that are missed because of the limited study.

Secondly, the study will solely handle the parts in the policy documents regarding issuance, revocation and expiration, as a consequence of these being the largest processes when handling certificates. That means there might be vulnerabilities in other aspects of the policy that this study will not take into account.

Thirdly the results has been presented in the form of tables were for the most part there are no gray-zones about what subjects may be categorized as. However in the discussion's Table 6.1 as it is a summarized list based on the other tables to show to what extent the CAs follow the BR there are some gray-zones as we tried to have a concise amount of categories.

1.4 Contributions

In this thesis, we have produced a list of the 100 largest CAs with regard to the number of certificates issued. We also produced a list of the top CA groups, which groups together the CAs based on what policy is used. From the lists, it can be shown that the Certificate Policy and Practice Statements differ from the BR and that these differences may lead to vulnerabilities regarding social engineering attacks.

1.5 Thesis outline

The remainder of this thesis is structured as follows. Chapter 2 explains core concepts to help understand the result and Chapter 3 contains findings from other papers on the same topics. In Chapter 4, the method, including the selection of CAs and the design of the taxonomy-based analysis, is introduced. The results, supported by tables, are presented in Chapter 5 and further discussed in Chapter 6 along with a discussion about the method used. Finally, in Chapter 7 the conclusions are presented with a discussion about vulnerabilities and potential attacks.

2 Background

In this chapter a background for the thesis is presented including Internet security protocols, some properties of the X.509 certificates, Certificate Authorities (CA), Certificate Policy (CP) and Certification Practice Statement (CPS). Furthermore, the Baseline Requirements (BR) for managing certificates and standards from some RFC documents are presented.

2.1 Internet security protocols

Hypertext Transfer Protocol (HTTP) [20] is an application layer protocol used to transfer data over the internet. Although as of recently the transition to Hypertext Transfer Protocol Secure (HTTPS) [21], an encrypted protocol for the same actions has increased.

HTTPS was developed to ensure secure transactions on the internet using encryption in the transport layer over TCP through the Transport Layer Security (TLS) [22] or its precursor the Secure Sockets Layer (SSL) [6]. The TLS protocol uses a specific handshake to establish a secure connection and as a part of the handshake, a digital certificate is shared by the entities to prove authenticity stated by a trusted third party.

2.2 X.509 certificate

SSL/TLS protocols use X.509 certificates to establish trust with users, which is known as public key certificates [4]. X.509 certificates have the same standardized fields, for example a validity period, and contain a lot of information about for example the issuing CA [4]. For this thesis, some fields have higher importance: *Issuer* and the extension *Certificate Policies*. The issuer contains information about the CA responsible for issuing the certificate. The certificate policies contain a policy number called *Object Identifier* (OID) as well as *Certification Practice Statement* (CPS) which is a pointer to the policy which the CA uses for managing certificates.

A certificate can be classified into a type, based on the security aspect [1]. The types of interest for this thesis are: Domain Validation (DV), Organisation Validation (OV) and Extended Validation (EV) . Out of the three, DV has the least security and only assures that the applicant has access to the domain entered in the request. OV assures that the applicant belongs to the organization and can be issued for multiple domains at once. EV has the highest security and is needed for banks for example. Another type of certificate, that this thesis will not focus on, is IV certificates which are intended for individuals.

Validity period

A certificate's validity period is defined by sequence of dates: *notBefore* and *notAfter* [4]. During this period, starting on the *notBefore* date and ending at the end of the *notAfter* date, the CA maintain updated information about a certificate's status.

After the *notAfter* date the certificate is expired, thus is no longer valid for use.

Revoked certificates

Revoking a certificate is called revocation and it occurs when a certificate becomes invalid before the expiration date [4]. The revocation can depend on multiple reasons, where some of the more common situations are: the subject changes name or a compromise of the private key is discovered or suspected.

There are multiple ways to keep track of revocation statuses [4]. The most common ways are Online Checking Status Protocol (OCSP) servers and Certificate Revocation Lists (CRLs), which provide a public record that is kept and signed by the CAs that shows the current statuses for certificates.

Re-key

Re-keying of a certificate is when a new key is generated followed by an application for issuance of a new certificate [5]. The reason for re-keying can be revocation because of a key compromise or certificate expiration combined with an expired usage period of the key pair.

Re-key is different from renewal since re-keying leads to a new certificate with a new key, whereas renewal leads to a new certificate with the same key and information [5].

Signature Algorithm

Certificates contain a field named *signature algorithm*, which indicates the algorithm used for signing a certificate [4]. According to the BR there are many supported algorithms when signing X.509 certificates that may be used. Some types of supported algorithms are: One-way hash function, RSA, DSA and ECDSA [11]. The most used algorithm is SHA-256 with RSA.

This thesis does not aim to go into details about the different algorithms but instead focuses on to what extent the CAs follow the BR in terms of chosen algorithms. Therefore a more detailed background about algorithms will not be presented.

2.3 Certificate Authority (CA)

A Certificate Authority (CA) is a trusted third-party that provides the authenticity of public keys by issuing and managing certificates for domains [14]. A CA, who has a certified public key, signs a message to issue the certificates containing the serial number, relevant data and expiration date. After a certificate has been issued, the CA will manage the certificates and may revoke them before the date of expiration.

There are no mandatory requirements for a CA to meet until they are enforced by Application Software Suppliers, see Section 2.5. Other than CAs issuing and signing certificates, there also exists self-signed certificates that anybody can issue [4]. Self-signed certificates are often used by malicious entities [7].

2.4 Certificate Policy (CP) and Certification Practice Statement (CPS)

As stated in Section 2.2, the field *Certificate Policies* contains information about what policies the CAs use while managing a certificate. These policies indicate under which terms a certificate has been issued and the purpose for which the certificate may be used [4].

The Certificate Policy (CP) is developed from the BR, which contains information about all the stages of issuance, revocation, expiring as well as different entities, their roles and much more [1]. The Certification Practice Statement (CPS) is also developed from the same BR with the difference that the CPS states the practices for the CAs in all stages of the certificate, from application to expiration.

2.5 Baseline Requirements (BR)

The Baseline Requirements (BR) that are in action are written by the Certification Authority Browser Forum (CAB-Forum) and are called “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” [1]. The CAB-Forum consist of approximately 50 CAs, including some of the biggest on the market, and other associates, which is one of the reasons that many CP and CPS are very similar to the BR.

The BR is used to give CAs requirements that must be met for their certificates to be widely trusted by browsers [1] and contains requirements about all parts of certificate management, for example how an application for a certificate should be performed. As the BR is the minimum level of action required by CAs, the CAs are allowed to increase the security within their own CP or CPS as long as they meet the minimum requirements.

Furthermore, the CAB-Forum has adapted a document called "Guidelines for the Issuance and Management of Extended Validation Certificates", also called "EV guidelines", which states details about a CAs practice regarding certificates of EV type [9].

2.6 RFC documents

Request for Comments (RFC) are documents about different areas of computer networking by the Internet Engineering Task Force (IETF) which cover eq. proposed internet standards, protocols, concepts and procedures among other topics [13]. In this report, 4 RFC documents are brought up as they are mentioned in the CAs policy documents. The 4 RFCs in question are: RFC6960, RFC6962, RFC5280 and RFC5019.

RFC6960 is the X.509 Internet Public Key Infrastructure Online Certificate Status Protocol or OCSP for short [23]. The RFC6960 document was created in June 2013 and was updated by the RFC8954 document in November 2020. The document describes how the revocation state of a certificate is obtained without having to go through CRLs in a more timely manner. The RFC6960 protocol specifies what data is exchanged when checking the status such as eq. revocationTime and nextUpdate. OCSPs have a validity period defined in RFC6960 which describes that as long as the certificate has not been revoked the response is "good".

The RFC6962 is the experimental Certificate Transparency document and was also created in June 2013 and is the experimental protocol for logging TLS certificates [18]. The purpose of certificate transparency is so anyone can look into CAs activities such as suspect certificates and logs. The reasoning for making the logs public was to prevent and lower the number of misused certificates at a scale where it is the norm to log certificates and in other cases not trust un-logged which will be rejected by TLS clients.

The 2008 document RFC5280 describes in detail version 3 of certificates and version 2 of Certificate Revocation List (CRL) as a proposed internet standard to encourage interoperability [4]. The document details a format for what the fields of the certificates and CRLs should contain. The document was later updated in 2013 and again in 2018.

The RFC5019 is an OCSP document from September 2007 and was updated as late as March 2021 [12]. The document is aimed to deal with high-volume environments to keep the load on OCSP responders low by minimizing bandwidth usage and processing complexity. The document addresses scalability issues by defining a message profile and behavior that will allow for eq. OCSP responses pre-distribution reduced OCSP message size and caching of both the network and the client.

3 Related work

CAs as trusted third parties and certificates have been the topic of many studies and discussions, although rarely in the form of analyzing the contents of the CP and CPS in regards to the BR.

Heinl et al. [10] studied the trustworthiness of CAs and introduced a metric with a set of criteria to assess existing policies, technical guidelines, and research. The metric aimed to support entities dealing with CAs, which resulted in an independent method of evaluating CAs based on technical, economical, political and legal considerations without taking the CP and CPS into account.

Similarly, Berkowsky and Hayajneh [2] studied security issues as a result of the security model of the time. Some of the issues Berkowsky and Hayajneh looked into were certificate revocation, CAs practices and behaviors when it comes to security breaches and lack of transparency. In the paper, they concluded that these factors did create security concerns that could be aided by reexamining the ways the models in use at the time.

On a similar track, three years later Korzhitskii and Carlsson [15] published a separate paper as CAs have begun enforcing Certificate Transparency (CT) for security reasons. Even the BR contains stipulations around the usage of CT in accordance with RFC6962. In the paper, Korzhitskii and Carlsson conduct a survey focusing mainly on Apple's and Google's transparency logging. They concluded that while the use of CT is largely established it is not in all cases to the standard that it should and thus should continue to be reworked in the future as well.

Furthermore, in another paper Korzhitskii and Carlsson [16] presents a study about revocation statuses delivered by CRLs and OCSP servers, with a focus on the time between expiration and status disappearance. Among other things about revocation statuses, the study shows differences in practices within and between CAs and motivates the development of a standard for revocation transparency. Furthermore, they conclude that there is a lack of policy and information for actions after the expiration of a certificate.

Additionally, Wazan et al. [27] examined behaviors of Web Browsers during the validation process of certificates including OCSP Stapling and HTTP interception products, such as proxies. These behaviors were analyzed and compared to standards, which showed that the validation process is a complex issue. Wazan et al. write that the most important findings are that the validation process is highly neglected by interception products and that none of the

existing techniques to check revocation statuses work consistently today, which implicates vulnerabilities for the web users.

In a paper by Ma et al. [19] they present a study about the belonging and identity of CAs done by developing a system that clusters the CAs to detect the ownership. From the system, a new database was built based on the ownership, which in turn showed that the embedded ownership data often are inaccurate due to for instance record keeping failures.

Kumar et al. [17] introduced a linter based on the BR and RFC5280 to monitor how well CAs construct certificates. The paper states that the error rates for certificates are marginal due to there being close to no errors by the largest CAs, meaning that the smaller CAs are responsible. They also state that certificates with errors are largely linked to other types of mismanagement and browser action.

In a study by Gasser et al. [8] information regarding the issuance of certificates from CT logs were analyzed to identify whether or not certificates follow the BR. The study focused on finding violations regarding four aspects: Identity, Signature, Keys and Time-Validity. The largest share of the violations regards identity and keys. The violations were mapped to the issuing CAs and the CAs were contacted regarding the findings. Furthermore, Gasser et al. studied other parts of the CT logs, for example CT gossiping.

Scheitle et al. [24] published a paper in October 2018 discussing the evolution of CT logging and the possible dangers thereof. The full view of the TLS ecosystem was made possible as a result of Google mandating the usage of CT logs in Chrome. Potential dangers, as well as protections discussed by them, were eq. the leak of sensitive information in the logs but also that CT logs are useful in detecting phishing attempts.

The related work differentiates from our work in the sense that we perform a CP and CPS review in detail for selected CAs to highlight vulnerabilities, while much of the related work is heavily focused on developing tools and aids to evaluate CAs and certificates. Furthermore, a lot of research focuses on revocation only, while we focus on multiple processes.

4 Taxonomy design

The taxonomy design was the method used to perform the study. The method was split into two parts: firstly retrieving the top CAs, done by collecting certificates, and secondly analyzing the certificate policies, done by taxonomy-based research and analysis.

4.1 Retrieving the top CAs

The first part of the taxonomy design was to determine which CAs ranked as the top in the world. In this case, the rank was concerning the number of signed certificates by each CA. This was done as part of another project by collecting data from certificates to analyze.

Using Tranco's list of top 1 million sites on the web [26], requests were sent to domains to start a TLS handshake including a certificate. The certificates were downloaded in pem-format and empty files were removed. The remaining certificates were converted using OpenSSL from pem-format to txt-format to make the information human readable. Only certificates from websites with an HTTPS-addresses can be downloaded because HTTP addresses do not need or provide certificates as a result of the connection not being encrypted.

From the txt-format, wanted information was retrieved and exported into a new file in csv-format. This wanted information included the domain, details about the issuer and subject as well as details about the policy used by the CA to manage certificates and the link to this policy.

With this csv-file self-signed certificates were eliminated because self-signed certificates were not interesting with regards to the popularity of CAs as they do not use a CA. Furthermore, IV certificates were eliminated as the focus for this thesis is on DV, OV and EV certificates, as described in Section 2.2.

With self-signed and IV certificates removed, the data was summarised per CA and the percentage per CA was calculated to generate a list that shows the popularity of each CA on the market.

4.2 Analyzing the certificate policies

The second part of the taxonomy design was departmentalizing the process into three steps: reading and marking, comparison and structuring and lastly creating the taxonomy and analysis.

Policy study

The first step of analyzing the policies was to study them and mark points of interest manually. Such points, in this case, were: issuance, revocation and expiration processes as mentioned in Section 1.2. The information in the policies that were of particular interest was saved to be used in step two of the process. This information was for example who can and how to request revocation as well as methods for submission and re-key public keys.

Structure and comparison

The second step of the analysis was to structure up the information gathered during the policy study and then compare the results to spot similarities and differences to create a basis for the taxonomy. This was done by structuring the information through tables and similar means to create a visual aid for the third step.

Taxonomy and analysis

The third and last step was performing the taxonomy and analysis. The taxonomy was heavily based on the information gathered and structured previously. The resulting figures showed the correlation between CAs and the way they manage the issuance, revocation and expiration processes as well as to which extent they use similar or the same policies. This was further analyzed in search of potential vulnerabilities.

5 Results

In this chapter the results of the taxonomy are presented. The results are largely based on tables to easier show the similarities and differences between the different CAs and the BR for various aspects of the certificates. To specify which CAs that were studied further the top CAs and top CA groups are presented before each aspect in detail. The links to the web pages of the CPs and CPSs as well as the version of the documents are available in Appendix A.4.

In the cases within the tables of the results where "no stipulation" are used as a statement in the BR or by the CAs it means that no requirements are stated.

5.1 Top CAs and CA groups

After summarizing the list of the top 100 CAs (see Appendix A.1), focus was set on the top 30, shown in Table 5.1. Also shown in the table are the ranking and common name of the CA, followed by the percentage of certificates collected signed by the CA and lastly the CA group.

The CA group indicates if the CA in question links to a policy written by another CA, thus they use the same policy and can be grouped for the following results. Table 5.2 shows the percentage for the top 30 CA groups, which is summarized based on the top list of CAs (see Appendix A.1). The full list of top CA groups is presented in Appendix A.2.

Table 5.1: Top 30 CAs

No.	Issuing CA	% of certs.	Mem. of CAB	CA Group
1	Let's Encrypt	39.395	Yes	Let's Encrypt
2	Cloudflare, Inc.	19.198	Indirect	Digicert
3	DigiCert Inc	9.412	Yes	Digicert
4	Sectigo Limited	8.622	Yes	Sectigo
5	cPanel, Inc.	4.866	Indirect	Sectigo
6	GoDaddy.com, Inc.	4.238	Yes	Starfield
7	Amazon	3.554	Yes	Amazon
8	GlobalSign nv-sa	3.010	Yes	GlobalSign
9	Starfield Technologies, Inc.	1.598	Indirect	Starfield
10	TrustAsia Technologies, Inc.	0.633	Indirect	Digicert
11	Asseco Data Systems	0.613	Yes	Certum
12	Entrust, Inc.	0.612	Yes	Entrust
13	Google Trust Services	0.556	Yes	Google Trust
14	COMODO CA Limited	0.327	Yes	Sectigo
15	ZeroSSL	0.257	Indirect	Sectigo
16	Gandi	0.247	Indirect	Sectigo
17	GoGetSSL	0.247	Indirect	Sectigo
18	Actalis S.p.A.	0.214	Yes	Actalis
19	Network Solutions L.L.C.	0.173	Yes	Network Solutions
20	GEANT Vereniging	0.132	Indirect	Sectigo
21	Corporation Service Company	0.130	Indirect	Sectigo
22	InCommon	0.129	Indirect	Sectigo
23	Japan Registry Services Co., Ltd.	0.127	Indirect	JPRS
24	home.pl S.A.	0.109	Indirect	Certum
25	Trustwave Holdings, Inc.	0.100	Yes	Trustwave
26	SECOM Trust Systems CO.,LTD.	0.098	Yes	SECOM
27	Microsoft Corporation	0.093	Yes	Microsoft
28	Cybertrust Japan Co., Ltd.	0.091	Indirect	Cybertrust
29	QuoVadis Limited	0.083	Yes	QuoVadis
30	Gehirn Inc.	0.082	Indirect	Sectigo

Table 5.2: Top 30 CA groups

No.	CA group	% of certs.
1	Let's Encrypt	39.395
2	DigiCert Inc	29.427
3	Sectigo Limited	15.279
4	Starfield Technologies, Inc.	5.839
5	Amazon	3.554
6	GlobalSign nv-sa	3.019
7	Certum	0.794
8	Entrust, Inc.	0.618
9	Google Trust Services	0.556
10	Actalis S.p.A.	0.214
11	SECOM Trust Systems CO.,LTD.	0.189
12	Network Solutions L.L.C.	0.173
13	Japan Registry Services Co., Ltd.	0.127
14	Telesec	0.117
15	Trustwave Holdings, Inc.	0.100
16	Microsoft Corporation	0.093
17	Cybertrust	0.091
18	SecureCore	0.066
19	SwissSign	0.032
20	TAIWAN-CA	0.031
21	Buypass	0.021
22	QuoVadis Limited	0.021
23	E-tugra	0.020
24	KPN	0.020
25	DHIMYOTIS	0.018
26	NetLock	0.016
27	AC Camerfirma	0.016
28	TeliaSonera	0.016
29	HongKong	0.016
30	D-Trust	0.014

In Table 5.1 Let's Encrypt has the biggest percentage of certificates of the whole market, followed by Cloudflare, Digicert and Sectigo. Overall the gap between percentages decreases fast as the list goes on and already at number ten the percentages are below one. As Table 5.1 shows there are 17 unique policies marked in green, as the remaining 13 CAs are linked to a CA group. Many of the top 30 CAs are linked to Sectigo as their CA group.

Also in Table 5.2 the percentages of the whole market decrease fast between the different CA groups, meaning that the first groups have larger parts of the market. Furthermore, there are some new names of CAs compared to Table 5.1.

The two lists presented in Table 5.1 and Table 5.2 are similar with some of the bigger CAs at the top, although they are not the same since Table 5.2 addresses the top policies used as a total. Therefore, the 17 unique policies marked in green from Table 5.1 will be mentioned in the ensuing tables.

5.2 General observations

Some general observations were that the BR often changes, which leads to changes in CP and CPS for the CAs and possible wrongdoing in the meantime. The changes make it difficult to find the newest document and keep updated as an outsider.

Another observation was that smaller CAs, who perhaps usually operate with another language than English, have fewer details within the English version of the CP and CPS. These CAs offer both an English version and a version with their native language, in this case Japanese, however the English version lacks details that other CAs who only operate in English offer. This results in fewer statements in the tables above or sometimes no stipulation at all. Therefore, when only analyzing the English version it is harder with a lesser amount of data to compare details to other CAs. The CAs in question are JPRS and Cybertrust. Also, SECOM is a Japanese CA, however they do provide a more detailed English version.

5.3 Issuance

The CP and CPS contain information about actions made by both the CA and the subscriber during the issuance process of a new certificate. The most interesting parts are the application process, the verification of a subscriber's identity, the submission of a public key, the process of re-key and the supported signatures since these are the ones that differ between CAs. As a point of reference, the statements of the BR are also included.

Application

The application process refers to the method that the subscribers use to request a certificate. This process includes multiple segments and different CAs require different of these segments to be performed, see Table 5.3.

Table 5.3: Segments of the application process per CA.

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
Generate and deliver key pair		x	x	x		x			x	x	x	x		x				x
CSR with public key				x			x							x				
Subscriber Agreement	x	x	x	x	x	x	x		x	x	x		x		x	x	x	x
Receive Certificate Request	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x
By appropriate Applicant Representative	x				x			x			x	x	x		x			
Certification that information is correct	x	x		x	x	x			x	x	x	x	x		x	x	x	x
May be made, submitted and/or signed electronically	x				x			x	x						x	x	x	
Pay fees			x			x			x									x
Multiple certificate available	x				x					x								x

As Table 5.3 shows the BR states that a subscriber agreement and a certificate request with correct information is to be signed by an appropriate representative. This may also be done electronically and may include multiple certificates at once. It also states that the segments of the application process are to be completed in no particular order. The table also shows that almost all of the CAs agree with the BR regarding the subscriber agreement and certificate request with correct information, but not regarding appropriate representatives, electronic applications and multiple certificates at once. For example, Let's Encrypt agrees with the BR regarding a subscriber agreement and certificate request with correct information, but do not mentioned the other stipulations by the BR, although they are a part of the application process for Let's Encrypt.

Apart from the aspects of the BR, varying CAs also states that the applicant needs to generate a key pair, send a CSR request with a public key and/or pay fees. These statements are a part of the agreement that the applicant accepts and will vary between different policies.

Furthermore, some CAs do charge for certificates and/or require a CSR-request even though it is not state in Table 5.3 due to missing statements within the CP and CPS in conjunction with segments of the application process.

Verification

The verification process differs with respect to what type of certificate is requested. Not all CAs offer all types, which is shown in Table 5.4 marked with a dash. Further, it is interesting to look closer at the percentages of the whole market between the types both overall and per CA, see Table 5.4.

Table 5.4: Percentages of the market per type of certificates issued overall and per CA.

	Overall	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
DV	66.083	100	45.291	87.855	100	58.968	57.015	89.613	-	86.489	54.423	35.131	91.886	1.903	66.617	90.110	-	-
OV	25.995	-	45.429	8.904	-	34.398	2.015	7.392	83.135	13.511	44.835	61.668	8.114	93.851	29.970	9.419	67.949	52.784
EV	2.220	-	9.101	3.240	-	5.564	40.906	2.234	16.841	-	0.743	3.201	-	3.221	2.671	-	31.731	22.165
Not specified	5.696	-	0.136	-	-	1.069	0.064	0.761	0.024	-	-	-	-	1.025	0.742	0.471	0.321	25.052

Table 5.4 shows that overall about 66% of certificates are DV, about 25% are OV and about 2% are EV. Furthermore, overall about 6% of the certificates were not specified as either of the types.

For each of these types: DV, OV and EV certificates, three separate tables are presented below with a focus on the BR and the CAs in question for that specific type of certificate. As each type of certificate is used to increase security in regards to the previous type, the increasing security is also reflected in the BR for that type.

Some CAs argue that DV certificates are at the core of some malicious activity involving certificates [28]. Therefore they have chosen not to offer DV certificates, even though 14 out of 17 CAs still do and their verification process for DV certificates are presented in Table 5.5.

Table 5.5: Verification regarding DV certificates.

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	Globalsign	Starfield	Asseco	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft
Subject Identity Information via Reliable Method of Communication	x	x	x		x				x				x	x	
Subject Identity Information via email, telephone, postal service				x		x	x	x		x					
Allow only specified individuals to request certificates on behalf of that domain	x	x	x		x	x	x	x	x			x	x	x	x
Applicant with control over domain			x									x			
Other form of verification				x		x					x				

For DV certificates, see Table 5.5, the BR are that the CA must use a reliable method of communication to confirm the information about the subject and that only specified individuals by the subject may act on the behalf of a domain. In this case, a reliable method of communication may be one or several of the following means of communication: a government agency, a third-party database, a site visit or an attestation letter.

Table 5.5 also shows that the BR is largely followed by the CAs in this aspect, although some CAs have interpreted a reliable method of communication as contact via email, telephone or postal service. Furthermore, in regards to Sectigo, Globalsign and Network Solutions other more elaborated forms of verification are used, involving techniques of proving the control over a specific domain or IP address. Digicert and JPRS also state that the applicant needs control over the domain, but do not state how this is done, which is different compared to Sectigo, GlobalSign and Network Solutions.

Moving on to OV certificates, all CAs apart from Let's Encrypt and Amazon offers the type. Table 5.6 displays that the BR are the same as for DV certificates, see Table 5.5, meaning that there are no added requirements for the changes in certificate types and the reliable method of communications are the same.

Table 5.6: Verification regarding OV certificates.

	Baseline Requirements	Digicert	Sectigo	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
Subject Identity Information via Reliable Method of Communication	x	x	x				x	x		x		x	x			x
Subject Identity Information via email, telephone, postal service				x	x	x			x						x	
Allow only specified individuals to request certificates on behalf of that domain	x	x	x	x	x	x	x	x		x		x	x	x	x	x
Applicant with control over domain		x														
Other form of verification				x							x					

Concerning GlobalSign, in Table 5.6, their verification process for OV certificates is identical to the one for DV certificates, while both Sectigo and Network Solutions change to resemble the BR. At the same time, the verification process of JPRS seems to deviate a lot from the other and address other issues than it should. Continuing, Digicert still states the control over the domain without stating how.

Continuing with EV certificates, the requirements used are not the BR. Instead, the EV guidelines are used, which are included along with the CAs regarding verification for EV certificates in Table 5.7.

Table 5.7: Verification regarding EV certificates.

		EV Guidelines	Digicert	Sectigo	GlobalSign	Starfield	Asseco	Entrust	Actalis	Network Solutions	Trustwave	SECOM	Cybertrust	QuoVadis
Verify a telephone number, fax number, email address or postal delivery address as a Verified Method of Communication		x	x			x			x	x	x	x		
Verify belonging to applicant or representative	**Through records from phone company**	x	x		x			x	x	x	x			
	Through QGIS, QTIS or QIIS	x	x		x			x	x	x	x			
	Through verified professional letter	x	x		x			x	x	x	x			
Confirm method by using it to obtain a sufficient response		x	x		x			x	x	x	x			
Same verification as per DV or OV				x	x	x	x					x	x	x

As pertained in Table 5.7 the EV guidelines state that the CA must verify a method of communication by verifying that it belongs to the applicant and confirm it by receiving a response when using the method. About half of the CAs that are offering EV certificates mention that extra verification in line with the EV guidelines is needed, while the other half fail to mention it at all. If they fail to mention extra verification it means that the verification process for EV certificates is the same as per DV or OV, which means that the security increase between the types is not fulfilled. Although in practice the CAs might act according to the EV guideline even though they fail to mention the routines within the CP and CPS.

Public key

During the issuance process, a key pair must be shared between the CA and the applicant. There are multiple different ways to do this, as shown in Table 5.8.

Table 5.8: Allowed methods for submission of public key.

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
Public key submission through certificate request		x					x	x								x		
Public key submission through certificate signing request, usually PKCS #10				x	x				x	x	x	x	x	x	x		x	x
No stipulation regarding submission of public key	x		x				x											

The BR does not state a specific method that must be used for the subscriber to submit its public key. Although there is no requirement, among the top CAs there are only two methods used according to the CPS documents. The first method is submission through a certificate request, which is the request used when applying for a certificate. This request will then contain the public key and the applicant will sign with its private key, which is something that is done whether or not the CA uses this method for submission of the public key. The second method, which is used by the majority, is submission through a certificate signing request (CSR) usually using PKCS #10, a separate request from the application itself although the certificate request still needs to be signed as well.

Re-key

The process of re-key starts when a subscriber wants to change the key pair associated with a certificate. The different methods that the CAs allow for the re-key process are presented in Table 5.9.

Table 5.9: Allowed methods for re-key.

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
Re-key treated as a new certificate		x			x			x	x	x	x		x	x	x	x	x	x
Re-key treated as a new certificate with same username and password			x	x		x	x					x						
Re-key through shared secret						x												
No stipulation regarding re-key	x																	

The table shows that the BR has no stipulation about the methods for re-key, yet the CAs do not differ far from one another. The most used method is that when a subscriber wants to re-key the CA will revoke the live certificate and start a certificate request for a new certificate. Others allow the subscriber to re-key if the same username and password is used but will still perform checks along the lines of a regular request. Starfield both allows re-key with the same username and password and allows re-key with help from a shared secret. In both cases, checks are performed according to the process of a regular request.

Supported signatures

Each CA presents within the CP and CPS a list of supported signatures for both the CA itself and the subscriber to use when signing in connection to a certificate. The signing is used to prove identity between the two, as well as when the CA ensures a secure connection by signing the certificate and issue it. Table 5.10 show which signatures the different CAs support.

Table 5.10: Supported algorithms for signatures.

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
RSASSA-PKCS1-v1_5 with SHA-256	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RSASSA-PKCS1-v1_5 with SHA-384	x	x	x	x	x	x		x	x	x		x				x		x
RSASSA-PKCS1-v1_5 with SHA-512	x	x	x		x	x		x	x	x						x		x
RSASSA-PSS with SHA-256, MGF-1 with SHA-256	x	x								x								
RSASSA-PSS with SHA-384, MGF-1 with SHA-384	x	x								x								
RSASSA-PSS with SHA-512, MGF-1 with SHA-512	x	x								x								
RSASSA-PKCS1-v1_5 with SHA-1	x	x	x	x		x	x			x		x				x	x	
ECDSA with SHA-1			x															
ECDSA with SHA-224			x															
ECDSA with SHA-256	x	x	x	x	x	x			x	x		x		x				x
ECDSA with SHA-384	x	x	x	x	x	x	x		x	x		x		x				x
ECDSA with SHA-512	x	x	x		x	x			x	x								
RSASSA-PSS			x			x												
DSA with SHA-1			x															

Table 5.10 tells that the BR supports a large number of different algorithms for signing. Many CAs offer a variety of algorithms, usually the larger a CA is the more algorithms there are to choose from. The only algorithm used by all the CAs is RSASSA-PKCS1-v1_5 with SHA-256, which is usually called SHA-256 RSA. Some CAs support RSASSA-PSS, although as of recently the BR has removed that algorithm in regards to X.509 certificates.

Furthermore, Digicert presents an even longer list with possible algorithms and does not mention for which type of certificate they are supported for use. These algorithms are *ECDSA with SHA-1*, *ECDSA with SHA-224* and *DSA with SHA-1*.

5.4 Revocation

Certificate Policy documents contain information about how the CAs manage revocation of their certificates as well as, but to a lesser degree, certificates of subordinate CAs. The information from the CP(S)s that will be presented in this section is: reasons for revocation, who can request a revocation, procedure for revocation requests, identification and authentication for revocation request, on-line revocation checking requirements and end of the subscription. In addition to the 17 CAs, the BR is also included in the tables. In the case that a CA is not included in a table that means that there are no stipulations from the CA on that matter thus will not be represented in the table.

Reasons for revocation

There are three tables in this section and they display the reasons for revocation given by the CAs in the CP documents. The tables show reasons why the certificate can be revoked as well as in which time frame it should or must happen. Table 5.11 presents what reasons should make the CA revoke a certificate within 24 hours of discovery as well as which reasons can be cause for revocation within 5 days. "Should" represents that the stipulations are recommended to be revoked in that time frame and "shall" represents that the stipulations are required to be revoked in that time frame. In the table, 24 hour stipulations are represented by "X" and 5 day stipulations are represented by "□" and if the stipulation is relevant for both it is represented by "☒".

Table 5.11: Reasons for revocation: The CA SHALL revoke a certificate within 24 hours and SHOULD revoke of a certificate within 24 hours and MUST revoke within 5 days

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
Subscriber requests revocation in writing	X	X	X	X	X	X			X	X	X	X		X		X	X	X
The original certification request was not authorized and the subscriber does not retroactively grant authorization	X	X	X	X	X	X			X	X	X	X		X		X	X	X
Private key suffered a key compromise	X	X	X	X	X	X			X	X	X	X		X		X	X	X
The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key or if there is clear evidence that the specific method used to generate the Private Key was flawed	☒		☒	X		☒			☒	☒		☐					☒	☒
The FQDN or IP-adress in the certificate should not be relied upon	X		X			X			X	X	X	X		X		X	X	X
The certificate was misused	☐	X	☐		X	☐			☐	☐	☐			☐		☐	☐	☐
The subscriber has violated one or more material obligations from the Subscriber Agreement or Terms of Use	☐	X	☐	☐	X	☐			☐	☐	☐	☐		☐		☐	☐	☐
The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted	☐	X	☐	☐	X	☐			☐	☐	☐	☐					☐	☐
The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN	☐	X	☐	☐	X	☐			☐	☐	☐	☐		☐		☐	☐	☐
The CA is made aware of a material change in the information contained in the Certificate	☐	X	☐	☐	X	☐			☐	☐	☐	☐		☐		☐	☐	☐
The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement	☐	X	☐	☐	X	☐			☐	☐	☐	☐		☐		☐		☐
The CA determines that any of the information appearing in the Certificate is inaccurate or misleading	☐	X	☐	☐	X	☐			☐	☐	☐	☐		☐		☐	☐	☐
The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate		X			X													
The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository	☐	X	☐	☐	X	☐			☐	☐	☐	☐		☐		☐	☐	☐
Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement	☐	X	☐	☐	X	☐			☐	☐		☐		☐		☐	☐	☐
The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties		X			X													
The NCA requests revocation for a PSD2 Certificate where the Subscriber (PSP) has lost its authorisation to act as a PSP or any PSP role in the Certificate has been removed						X												X
For code signing, the Application Software Supplier requests revocation and the Issuer Ca does not intend to pursue an alternative course of action			☐											☐				☐
For code signing, the certificate is being used for SuspectCode			☐						☐		☐			☐				☐
Either the Subscriber's or the CA's obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised				☐								☐						
A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way				☐								☐						
The Subscriber has used the Certificate contrary to law, rule or regulation, or the CAs reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity												☐						
The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities												☐						
The Certificate was issued as a result of fraud or negligence												☐						

The first row of Table 5.11 represents the BR. The CAs that utilize the BR most commonly use almost all of them, the only exceptions being Let's Encrypt and Amazon that uses three of them. The table also shows that the majority of the CAs are content with only using the BR for this part of the CP(S). Whereas Let's Encrypt and Amazon has several more scenarios that evoke revocation within 24 hours beyond the BR stipulations. Most of the stipulations

that Let's Encrypt and Amazon revoke within 24 hours the majority of CAs revoke within 5 days.

Some of the reasons listed by the BR that are reasons to revoke a certificate in the relatively short time span of 24 hours are: if the subscriber requests revocation or if their certificate was issued wrongfully, key compromises or the possibility thereof or if the domain name or IP address should not be relied upon any longer.

There are almost double the amount of stipulations where revocation should happen within 5 days compared to revocation within 24h and the CAs are quite consistent in stipulation usage on this time span as well. There are some smaller CAs that have more stipulations on this subject such as Network solutions and Trustwave. And the topic of stipulations for revocation within 5 days are e.q: changed or inaccurate information in the certificate, if the CA loses right to or can not issue certificates or if there the certificate is used in a way that could become harmful.

Table 5.12 is the table with the longest set time frame and presents which reasons the subordinate CAs certificates can be revoked. The distribution of points is similar in distribution to Table 5.11 with Network Solutions adding more than the BR in this table as well as Sectigo. The stipulations are similar in content to the two previous revocation tables with the difference of the subject being the subordinate CA instead of a subscriber.

Table 5.12: Reasons for revocation: The issuing CA SHALL revoke a subordinate CA certificate within 7 days

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Entrust	Google Trust	Network Solutions	Trustwave	QuoVadis
The Subordinate CA requests revocation in writing	x	x	x	x	x	x	x	x	x	x	x
The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization	x	x	x	x	x	x	x	x	x	x	x
The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise	x	x	x	x	x	x	x	x	x	x	x
The Issuing CA obtains evidence that the Certificate was misused	x	x	x	x	x	x	x	x	x	x	x
The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement	x	x	x	x	x	x	x	x	x	x	x
The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading	x	x	x	x	x	x	x	x	x	x	x
The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate	x	x	x	x	x	x	x	x	x	x	x
The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository	x	x	x	x	x	x	x	x	x	x	x
Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement	x	x	x	x	x	x	x	x	x	x	x
The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties		x	x		x	x				x	x
The Subordinate CA has used the Certificate contrary to law, rule or regulation, or Sectigo reasonably believes that the Subordinate CA is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity				x					x		
The Subordinate CA Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities				x					x		
The Subordinate CA Certificate was issued as a result of fraud or negligence				x					x		
The Subordinate CA Certificate, if not revoked, will compromise the trust status of CA				x					x	x	
By order from authority										x	
The CA receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation										x	

The fourth and last revocation table is Table 5.13 which contains reasons for revocation that do not include a time frame in which action should be taken.

Table 5.13: Circumstances for revocation with no set time frame.

	Baseline Requirements	Digicert	GlobalSign	Starfield	Asseco	JPRS	SECOM	Microsoft	Cybertrust	QuoVadis
The Certificate no longer complies with the requirements			x	x				x		x
The certificate subject can be shown to have violated the stipulations of this CP/CPS, Baseline Requirements (BR), or compromise the security or integrity or The Subscriber can be shown to have violated the stipulations of the Subscriber Agreement				x	x	x	x		x	
Compromise of the Subscriber's private key is known or suspected or if there is clear evidence that the specific method used to generate the Private Key was flawed				x	x	x	x	x	x	
The authenticated organization or individual name in the Subject field of the Subscriber's certificate changes before the certificate expires				x	x	x	x		x	x
The Subscriber fails to pay any invoice				x	x				x	x
The CA receives notice or otherwise becomes aware that the Subscriber has been added as a denied party or prohibited person to a blocklist, or is operating from a prohibited destination under the laws of the CA:s jurisdiction of operation		x	x				x		x	x
Following the request for cancellation of a Certificate			x		x	x			x	
If a Certificate has been re-issued, the CA may revoke the previously issued Certificate			x							
Under certain licensing arrangements, the CA may revoke Certificates following expiration or termination of the license agreement			x							
The CA determines the continued use of the Certificate is otherwise harmful to the business of the CA or third parties or the technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others		x	x		x		x		x	x
Death of a Subscriber			x							
Either the Subscriber's or the Issuer CA's obligations under the CP or CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised		x							x	x
The Issuer CA received a lawful and binding order from a government or regulatory body to revoke the Certificate		x			x				x	
The Issuer CA ceased operations and did not arrange for another CA to provide revocation support for the Certificate		x			x				x	x
The subscriber resigns from services provided by the CA., if the subscriber does not request the revocation by himself/herself/itself, a certification authority or a representative of the institution in which the subscriber is employed, has the right to do it					x					
When a signatory is unable to enter into legal transactions					x					
The subscriber, being an employee of an organization, has not returned the electronic cryptographic card, used for storing the certificate and the corresponding private key, when terminating the contract for employment					x					
Other circumstances, delaying or preventing the subscriber from execution of regulations of this Certificate Policy and Certification Practice Statement, emerging from disasters, computer system or network malfunction, changes in the subscriber's legal environment or official regulations of the government or its agencies					x					
Certificate was not issued in accordance with the relevant requirements of the CP or CPS or the subscriber agreement									x	
The information described in the certificate has changed						x				x
The certificate was issued as a result of fraud or negligence									x	
The use of the Certificate is being terminated							x		x	
The Secret Key of the Subscriber and CA is compromised, and the reasonable evidence is found, which shows that the key isn't complying with the algorithm type and the requirement for the key size as standard, or the certificate is abused by some other way							x			
The CA learns that an improper string has been designated for, or is included in, a value set in any information in the certificate						x				

These stipulations are from CAs that have not followed the BR for this section or have added further stipulations with no set time frame. The contents of the stipulations are similar to the previous tables but add some external factors as well as subscriber-based reasons

for revocation. Some examples of what stipulations contains are various levels of certificate misuse, key compromises and economical reasons.

Who can request revocation

Pertaining to revocation there are stipulations in the CPs regarding who is eligible to request the revocations which are displayed in Table 5.14.

Table 5.14: Who can request revocation

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
The Subscriber	x		x	x	x	x	x	x	x	x	x	x		x	x	x	x	x
The Registration Authority	x		x	x		x		x	x	x	x	x				x		x
The Issuing CA	x	x	x			x	x	x	x	x	x		x	x		x		x
Certificate Problem Reports	x		x	x		x			x	x	x	x		x			x	x
An affiliated organization			x			x												
Other authorized parties				x			x	x	x			x	x	x	x	x	x	x
A court of law								x			x							
Anyone can revoke a certificate via the API if they can sign with the private key		x																
Anyone can revoke via the API if they can demonstrate control of all domains covered by the certificate		x																
Subscribers can revoke certificates belonging to their accounts via the API if they can sign the revocation request with the associated account private key		x																

The BR has 4 main entities that can request revocation: the subscriber, the Registration Authority, the issuing CA and any individual can report a certificate for possible revocation through a Certificate Problem Report (CPR). Some other parties that common among the CAs can request revocation are subscriber's affiliated organizations or other authorized parties as well as authorities such as courts of law. Let's Encrypt have some other stipulations relating to who can request revocation through their API.

Procedure for revocation request

In the previous section, the table showed who can request revocation and this chapter's Table 5.15 displays different procedures of how subscribers and other parties can request revocation.

Table 5.15: Procedure for revocation requests

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
The CA SHALL provide a process for Subscribers to request revocation of their own Certificates	x	x	x		x		x		x	x	x				x	x	x	
The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports	x	x	x	x			x			x	x	x						x
The CA SHALL publicly disclose the instructions through a readily accessible online means and in their CP(S)	x		x					x		x			x	x		x	x	x
Request revocation by email		x					x				x			x		x	x	x
Launch an investigation into whether revocation or other appropriate action is warranted will be based on at least the following criteria		x							x		x							x
Has been authenticated by the procedures in this CP(S)				x	x		x		x			x	x	x			x	x
Certificate revocation may be carried out by submission of a request by phone call								x										
By use of a national/regional postal service, facsimile, or overnight courie														x				
Due to the nature of revocation requests and the need for efficiency, Issuing CAs and RAs may provide automated mechanisms for requesting and authenticating revocation requests						x												
Issuing CAs and RAs will record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved						x												

For this Section, the BR contains 3 stipulations that describe that the CA shall provide a process for subscribers to request revocation on their own and that they should maintain a 24x7 ability to respond to and accept CPRs. Among the most common methods pertained from Table 5.15 are online or by email, but there are also methods such as phone calls, by post or visitations in person. The majority of the CAs maintain that the procedures should also contain some form of authorization method that will be shown in the next section of this report.

Identification and authentication for revocation request

For safety reasons, the CAs should have an authentication method for revocation requests to make sure that the appropriate entity is requesting the revocation and that not anyone can revoke any certificate. The BR has no stipulation for this so the CAs have more freedom of methods to use.

Table 5.16: Identification and authentication for revocation requests

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
By use of public key			x		x													
Using a username & password or other details to login/verify				x		x					x	x		x				x
By use of S/MIME email and private key				x								x						
By use of an online revocation request page							x								x		x	x
Using a shared secret							x											
By phone call								x						x				
Multi-factor authentication process									x	x						x		
Using the provided email address														x			x	
Authentication details				x							x							
Administrator contact				x								x	x					
The Administrator contact verifies details by phone or fax				x								x						
In compliance with the reasons for revocation		x			x													
By using unique elements in the certificate to authenticate					x													
Show ID (passport, drivers license, eq.) in person																		x

In Table 5.16 the diverse methods of authentication and identification are displayed. Some of the methods are online based in the sense that the subscriber can request revocation by themselves through logging in with a password and username. In other methods, the subscriber needs to communicate in some ways with their administrative contact from their CA to request revocation. Those methods can be sending emails or S/MIME emails with the correct private key, others use more analog methods such as calling or faxing to confirm the revocation or even confirming with a form of ID in person. Some CAs have very extensive methods in their CP(S) descriptions while some others keep it vague when explaining their methods, only referring to the methods as using unique elements or a shared secret.

On-line revocation checking requirements

The on-line revocation checking requirements section in the CP(S) documents is about OCSP validity periods and issuances as well as which RFC documents are relevant for the certificates. These topics are separated into three tables.

Table 5.17 displays the most commonly mentioned RFC documents by the CAs, the full list of every RFC mentioned by the CAs is available in Appendix A.3. The yellow in the table represents that the RFC document has been updated by another RFC.

Table 5.17: RFCs most commonly mentioned by the CAs

RFC	RFC Name	Updated by	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
RFC 3647	**Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework**		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RFC 5019	**The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments**	**RFC 8996**	x	x	x	x	x	x	x			x		x		x	x		x	
RFC 5280	**Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**	**RFC 6818, RFC 8398, RFC 8399**	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RFC 6960	**X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP**	**RFC 8954**	x	x	x	x		x	x	x	x	x	x	x		x	x		x	x
RFC 6962	**Certificate Transparency**		x	x		x	x		x		x	x		x	x	x	x	x	x	x

There are 5 different RFC documents mentioned in nearly all CAs in the CP(S)s: RFC3647, RFC6960, RFC5019, RFC6962 and RFC5280. As per mentioned in Section 2.6 RFC3647 is a framework for CP and CPSs. RFC6960 is an OCSP document, RFC5019 is an OCSP document regarding usage in high volume environments, RFC6962 is an experimental document regarding Certificate Transparency and RFC5280 is a certificate and CRL profile document. The table exhibits that all of the CAs mention RFC 3647 and RFC 5280 and the remaining three are mentioned by all but a few. The table also conveys that JPRS nor Microsoft mentions any OCSP RFC.

As mentioned in Section 2.6 the OCSPs has a validity period that informs that in that period of time the certificate has not been revoked if the response is "good". Displayed in Table 5.18 are the descriptions of how long those validity periods may be between OCSP checks.

Table 5.18: OCSP Validity period

	Baseline Requirements	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	Trustwave	Microsoft	Cybertrust
OCSP validity period is greater or equal to 8 hours	x	x			x				x	x			x	
OCSP validity period is less than or equal to 10 days	x	x		x	x				x	x			x	x
OCSP validity period is less than or equal to 16h and by the half of nextUpdate time the information updates	x	x			x				x	x			x	
OCSP validity period is greater or equal to 16 hours, updates information 8 hours prior to and no late than 4 days after thisUpdate	x	x			x				x	x			x	
Subordinate CA updates OCSP responses every 12 months and within 24h of revocation	x	x			x			x	x					
Root CA updates OCSP repsonses every 365 days or less						x								
Issuing CA updates OCSP response every 4 days or less				x		x								x
OCSP response updates every 3.5 days			x								x			
OCSP validity period of maximum 5 days												x		
OCSP validation period for max 7 days			x					x			x			
Status available not later than 60 seconds after revocation							x							
New OCSP response available before half to the validity period has expired												x		

The validity period lasts between 8 hours to 10 days but updates within 24 hours of revocation in general. Remarkably Assecco offers updates to be under 60 seconds after revocation. The table shows that about half of the CAs use the BR validity period and the other half utilize other shorter periods.

Other stipulations from the Online-checking requirements part of the policy documents are displayed in Table 5.19 as the stipulations are more so aimed towards definitions.

Table 5.19: Other online-checking requirements

	Baseline Requirements	Let's Encrypt	Digicert	Amazon	GlobalSign	Starfield	Google Trust	Actalis	JPRS	Trustwave	SECOM	Cybertrust	QuoVadis
The CA monitors unused serial numbers	x		x									x	x
Assigned if: issued by the issuing ca, current or previous key associated with that CA subject	x												
Reserved if: Issued by issuing CA or pre-certificate signing certification	x												
Unused: if it is neither assigned nor reserved	x												
If OCSP responder recieves request of a cert that hasn't been issued the responder don't respond with "good" status			x		x	x		x		x		x	x
Relying parties that cannot or choose not to check the revocation status but decides to rely on the certificate anyways does so at their own risk		x							x		x		
If practical platforms should consult blacklists of suspect software				x									
If OCSP responder recieves request of a cert serial number that is unused the responder shouldn't respond with "good" status							x						

This table presents one of the occasions where the BR are available but most CAs carry no stipulation on the subject. Something of note is that Amazon consults a blacklist check in addition to the revocation check of the OCSP.

5.5 Expiration

Expiration is explained in Section 2.2 which says that the certificate is expired when the notAfter date has passed. In the CP documents, there is a section dedicated to the end of the subscriber's subscription, to which the BR document has no stipulation and neither does a large part of the CAs, which can be shown in Table 5.20.

Table 5.20: End of subscription.

	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
No stipulation	x				x		x	x	x	x	x					x		
Notice through email to subscriber		x												x				
The Issuer CA shall allow subscribers to end their subscription to certificate services by having their certificate revoked or by allowing the certificate applicable Subscriber Agreement to expire without renewal			x			x												
Ends if the CA ceases operations				x								x						
All of subscriber's certificates issued by the CA are revoked without the renewal or re-key of the certificate				x								x						
The subscriber's Subscriber Agreement terminates or expires without renewal				x								x	x		x			x
If a subscriber ceases to use its certificate or cancels the services, the subscriber shall apply for revocation of its certificate													x				x	

The table also shows that the ones that do have stipulations explain why the subscription might have ended. Some CAs wish that the subscriber requests revocation when the subscription is about to end and that in that case all of the certificates will be revoked.

6 Discussion

In this Chapter the results, the method and the work in a wider context are discussed.

6.1 Results

In general, the larger CAs follow the BR to a larger degree, than the smaller CAs. This seems to correlate with Kumar et al. [17] discoveries about misissuance of certificates. This may be a result of the amount of impact each CA has over the content within the BR, which also means that many CAs have the same stipulations.

A summary of the results from in Chapter 5 is presented in Table 6.1, where the statements of the CAs have been categorised as one of five different categories. The categories are represented by the following symbols: "■" means *Follow with additional constraints*, "☒" means *Follow*, "◪" means *Follow to some extent*, "□" means *Does not follow* and "•" means *No stipulation*.

Table 6.1: Summary of to what extent the results follow the BR.

			Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
Issuance	Application		Requirements	☒	◪	■	☒	☒	◪	◪	■	☒	☒	◪	☒	□	☒	☒	☒	☒
	Verification	DV	Requirements	☒	■	■	☒	■	◪	◪	-	☒	-	■	◪	☒	☒	◪	-	-
		OV	Requirements	-	■	☒	-	■	◪	◪	☒	☒	□	☒	■	☒	☒	☒	□	☒
		EV	Requirements	-	☒	□	-	◪	□	□	◪	-	☒	☒	-	☒	□	-	□	□
	Public key submission		No stipulation	■	•	■	■	■	•	■	■	■	■	■	■	■	■	■	■	■
	Re-key		No stipulation	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
	Supported signatures		Requirements	☒	□	☒	☒	□	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Revocation	Reasons for revocation	24 hours, 5 days	Requirements	■	☒	☒	■	☒	•	•	☒	☒	☒	■	•	☒	•	☒	☒	■
		Subordinate 7 days	Requirements	☒	☒	■	☒	☒	•	•	☒	☒	•	■	•	☒	•	•	•	☒
		No set time frame	No stipulation	•	■	•	•	■	■	■	•	•	•	•	■	•	■	■	■	■
	Who can request revocation		Requirements	■	☒	☒	□	☒	◪	☒	☒	☒	☒	☒	◪	◪	◪	☒	◪	☒
	Procedure for revocation request		Requirements	■	☒	◪	◪	□	■	◪	◪	☒	◪	◪	◪	◪	◪	◪	◪	◪
	Identification and authentication for revocation request		No stipulation	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
	On-line revocation checking requirements	RFC	Requirements	☒	◪	☒	◪	◪	☒	◪	◪	☒	◪	☒	◪	☒	☒	◪	☒	◪
		OCSP Validity	Requirements	•	☒	□	□	☒	□	■	□	☒	☒	□	•	□	•	☒	□	•
		Other requirements	Requirements	◪	◪	•	□	◪	◪	•	•	◪	◪	•	◪	◪	◪	•	◪	◪
Expiration			No stipulation	■	■	■	•	■	•	•	•	•	•	■	■	■	■	•	■	■

Within Table 6.1 the statements of the BR regarding all areas of the study can be seen as either *Requirements*, meaning that there are requirements to meet, or *No stipulation*, meaning that there are no requirements stated. This means that a CA who states requirements when the BR does not will be categorized as *Follow with additional constraints*. Although, a statement of *No stipulation* made by a CA is not treated as *Follow* even though the BR states the same. Furthermore, dashes mean that the CA does not offer the process in question.

With the BR being a joint initiative it is interesting that not all of the CAs have adopted the full content, even though most of the CAs are members of the CAB-Forum who is responsible for the BR. For areas where the BR states no stipulation, it is fair for the CAs to have their own approach, as well as when the CA determines to be stricter than what the BR is. However, some CAs practice lesser requirements than those stated in the BR according to their CP and CPS. There are some speculations as to why that might be, such as the CA not agreeing to the stipulation or the membership status when the stipulation was decided. The votes on stipulations are displayed publicly on the CAB-Forum website and only 50% of the members need to vote yes for it to pass [1]. There could thus be stipulations that some CAs do not want to follow despite it being in the BR. Another reason could be the CAs membership status as some CAs have joined and left the CAB-Forum and therefore possibly have not updated accordingly. Some CAs are also not members but choose to follow the BR anyway which might be the reason they don't include certain stipulations. Having said that, the BR is the minimum level of action required by the CAs, which leads to the possibility of different interpretations for different types of certificates. From this it seems that even non-members see the advantages of utilizing the BR even if it is not fully using all stipulations.

Something that stood out regarding the different CAs through all the processes was that the CP and CPS of mainly JPRS, but also in some aspects Cybertrust, were lacking details and deviated from the BR, as they are not direct members of the CAB-Forum. This is interesting as they both are indirect members through SECOM but still present their own policies even though the policy made by SECOM, who is a member of the CAB-Forum, is better overall. Although, since SECOM is a member and JPRS and Cybertrust are a part of SECOM, it makes JPRS and Cybertrust indirect members. As all these three CAs are based in Japan, this may have something to do with how CAs are normally used there. Furthermore, the originals of their policies are written in Japanese and then released as an English version, which might have impacted the content. This also implies a larger vulnerability, which might be eliminated if the policy of SECOM would be used instead.

Another discovery is that a large amount of CAs is connected to or owned by other CAs, making the market for certificate issuer hard to understand. For example, Sectigo as a CA has a smaller percentage of the market than Sectigo as a CA group does, while Let's Encrypt remains the same for the CA and the CA group. Although Sectigo as a group is still smaller than Let's Encrypt. This means that there are fewer competitors than what it looks like and fewer policies that the CAs rely on. This result seems to comply with what Ma et al. [19] discovered about clusters of CAs hidden true identity and ownership. Therefore it is more complicated to determine the popularity of each CA, as it requires a decision whether to focus on the actual CAs or the CA groups.

Moving on towards the application process for a certificate, all CAs require a request in which the applicant confirms that the information included is correct. This is also followed by a signing of the request, which decreases the risk for vulnerabilities. The CA will then follow up by verification to make a secure decision before issuing a certificate.

Regarding the application process, it is interesting that not all CAs discuss the electronic application and multiple certificates per application although they very likely practice both of them. It might not be mentioned as a consequence of it being evident in today's society with electronic applications or it might be more clear when applying for a certificate, but the ambiguity remains. Furthermore, the statements that differ from the BR regarding the application only adds to the security aspect. Meaning that it will not impact the CA to be more vulnerable.

As for verification of the subject in a certificate request, all CAs perform some form of a check. The most interesting difference is that Sectigo and GlobalSign perform checks on control of the domain or IP address in regards to DV certificates. For OV certificates GlobalSign does not change method while Sectigo changes to using a reliable method of communication. The most reasonable alternative would be as Sectigo has chosen to do, because of DV certificates being the least secure which would need a better method of verification. Having said that, both ways are approved according to the BR as the added checks add to the security.

Within the BR there are no obvious differences between the requirements for DV and OV certificates, even though there are large differences in security in the two cases. Therefore, it is interesting that both DV and OV certificate require the same process for verification according to the BR even though OV certificates offers a higher degree of security. This might be a consequence of the requirements being fitted for OV certificates and in that case are of a higher degree of security than what DV certificates require. At the same time, the security can always be increased, for example as Sectigo and GlobalSign offer.

Furthermore, some CAs have interpreted a reliable method of communication for example via telephone or email both for DV and OV certificates, rather than the approved methods by the BR. This may be a vulnerability as the subject can pretend to be someone they are not. These vulnerabilities seem to be reflected within the violations about identity found by Gasser et al. [8]. Although, the vulnerabilities would be eliminated if the reliable method of communication involves a third party, for example the government, as the BR states.

Another interesting fact about the verification is that the majority of CAs only allow specified individuals to act on the behalf of the applicant, therefore adding a layer of extra security as the representative has to identify beforehand.

In the BR there are no stipulations in regards to authenticating revocation requests so that a correct entity requested the revocation of certificates as mentioned previously. This leads to quite the diversity in methods used to identify the entity making the request among the CAs in regards to revocation as well. Some CAs rely on a singular method while others combine them, but the most usual way is using some form of website log-in or sending an email to request revocation. These methods are sometimes combined with another entity signing on to confirm it as well or that their contact from the CA confirms details with them. Overall the procedures seem secure as they usually consist of multiple steps which makes it harder for a malicious entity to get every piece of information required for an attack. Some methods include more analog ways of authentication such as phone calls and/or faxes. There could however be windows for a malicious entity to initiate or complete revocation if they can secure the correct information such as private or public key, shared secrets or other verification details.

Moving on to public keys, the BR does not stipulate allowed methods for submission of public keys. Despite that, the CAs have a pretty standardized way of handling the submission via a request that is signed by the applicant. Having said that, it might be even more secure to perform some kind of challenge with a challenge-response by the CA, which might be needed accordingly to findings about keys done by Gasser et al. [8].

On the same note, regarding re-key, all the CAs have a method of dealing with the action which more or less includes the same checks as for the regular verification process if the applicant has control over the username and password. Therefore there are no added vulnerabilities in regards to re-key.

The BR often changes regarding supported algorithms for signing and the requirements clearly state that no other algorithms are to be used. Therefore it can be assumed that there are no greater threats before the BR choose to edit the allowed methods. Although, Gasser et al. [8] indicate that some CAs showed violations in regards to signatures, but these have decreased over the years.

Regarding reasons for revocation, there are various time spans with their own reasons for revocation. The time span dictates the level of urgency in which the certificate should be removed. Thus something worth noting is that Starfield, Asseco and JPRS do not set a

time frame which opens up the question of how long a risky certificate remains un-revoked. The speed at which CAs revoke certificates that are deemed insecure affects security on the internet, as the certificate might still pass authentication steps until it has been revoked. This can put domains and other certificates at risk. RFC5280 states that "the availability and freshness of revocation information affect the degree of assurance that ought to be placed in a certificate" and that "If revocation information is untimely or unavailable, the assurance associated with the binding is clearly reduced" [4]. Which can indicate that faster revocation of certificates is preferred especially when it comes to matters such as misuse of or at risk certificates. RFC5019 mentions possible attacks that might occur against an OCSP eq. Man-in-the-Middle-, Impersonation-, and Denial of Service attacks [12]. These are also some of the dangers that might occur if a certificate has been compromised. Which can lead to eq. stopped traffic for domains by issuance or revocation of certificates or other certificates being at risk of compromise if the private keys are found out by the malicious entity. Thus the faster a certificate is deemed unsafe and is revoked the less possibility it might have to cause harm through such attacks.

The online checking requirements section of the BR is extensively detailed, despite that the CAs largely decide their stipulations own on this matter rather than using the BR. The topic that is particularly in this position is OCSP, where less than half of the CAs follow the BR stipulations. Those CAs who provide their own OCSP stipulations usually choose a much shorter validity period, often closer to 4 days. This could indicate that this part of the BR is somewhat outdated and could use some overseeing. Perhaps that might be the reason why those stipulations are not as well used as previous stipulations in the BR. Some of this can also be reflected in the usage of RFC documents as most of the more commonly mentioned RFCs are obsoleted or updated by more recent documents. Certificate Transparency (RFC 6962) is mentioned by the majority of CAs and is a RFC document that has not been updated. RFC6962 is an initiative by Google, which later in 2018 mandated the use of CT logs in Chrome as discussed by Scheitle et al. [24]. Scheitle et al. also discuss the possible dangers that can appear with the surge of CT usages such as sensitive information appearing and phishing. Korzhitskii and Carlsson [16] also discusses the usage of CT logs and takes it a step beyond and suggests a new safer more transparent verification standard similar to CT logs. They also address the dangers that OCSP and CRL might generate and the number of other papers discussing the safety of certain RFC documents one might wonder if they are going to be obsoleted in a foreseeable future.

The end of the subscription is sparsely stipulated in the BR and the policies which are in accordance with the findings of Korzhitskii and Carlsson [16]. If there are stipulations on the matter they are usually requested to the subscriber of what they wish to be done before the expiration date.

6.2 Method

In this section issues in the method used that could be improved are discussed.

Retrieving the top CAs

When retrieving the top CAs the method relied on Tranco's list of the top 1 million sites on the web, which contains websites using either HTTP or HTTPS. HTTP does not provide a certificate upon request since there are non, as a consequence of lesser security than HTTPS offers. Therefore, the result was about 700 thousand certificates from the 1 million websites. Websites using HTTP do not affect the results more than reducing the number of certificates received from the top 1 million sites.

Furthermore during the sorting, calculating and grouping of the top CAs, the list presented difficulties in form of different ways of spelling the name of each CA as well as presenting a large number of self-signed certificates. This resulted in some difficulties when

trying to ensure that the top list retrieved was the correct one for that specific collection, which led to the multiple retrieving of lists based on Tranco's list to conclude the final list.

Analyzing the certificate policies

The analysis of the certificate policies was quite reliable in the sense of technological errors, as it consisted of manually fetching information from the CP and CPS. Manually collecting data comes with some risks as humans are not perfect and mishaps such as missing or misinterpreting information can occur despite re-comparing the information.

Some difficulties did however come with finding the correct documents as some of them were harder to find because of some inaccessibility which in some cases were combined with language barriers. During the study, some of the policy documents were updated which created some issues in the analysis phase. The updates of the documents could make the results different if changes are being made over time and could make this paper irrelevant in a couple of years.

6.3 The work in a wider context

There are no direct impacts in regards to ethical or societal aspects in this study. However, with an expanded view on topics discussed in this analysis, there are some subjects related to security issues that could have some societal and ethical impact from a security perspective.

In the CP and CPSs, some things are being left unsaid in the stipulations as well as some aspects that could be considered outdated, that could be a societal issue if a malicious entity were to conduct hacking and social engineering attacks on the certification processes. It could be a potential risk because there is a need for certificates and CAs to maintain a safe environment on the internet.

Furthermore, for a well-functioning society, the webPKI is of high importance as a greater part of helping all daily activity that takes place on the Internet to do so safer. It is of great importance as it can be dangerous if domains can get certificates issued or revoked without their consent. A CA that has been having issues with both of the aspects is Symantec, as discussed in blog posts by Google Security Blog [25] and Hanno Böck [3]. Google decided to stop trusting Symantec as a CA after it had been proven that certificates had been issued for unregistered domains. Böck showed that Symantec would revoke a certificate based on a private key that he forged and that the CA did not disclose the proper information to the domain owner.

7 Conclusion

From the study, there have been some conclusions found to answer the research questions in Section 1.2. The initial conclusion that can be drawn is regarding similarities between the BR and the CAs. The tables in Chapter 5 show that there are differences in correlation to the size of CA and how they adapt to the BR. There are greater similarities to the BR usage and stipulations by larger CAs than smaller ones.

With respect to the process of issuance, the few distinctions noted are due to what type of certificate is requested and issued more so than the steps during the process. As for the revocation process, the policies varied greatly amongst topics between both the BR and CAs as well as between the CAs. At last, the expiration process, which was not emphasized in such great length by the BR or the policies, as no further actions are carried out after the expiration date and that the CA prefers the subject to request a new certificate or revocation of the expiring one before expiration occurs.

With the summarised results in Table 6.1 in mind, it can be concluded that the popularity of the CA derives from the difficulty of requesting and receiving a certificate as well as the types of certificates available. An easier process and availability of the type requested will lead to more applicants and therefore also more certificates. Furthermore, from a security perspective the most popular CAs rarely deviate from the BR whereas the less popular tend to deviate more. Although, these distinctions do not seem to impact the applicants when choosing a CA as all CAs promise to follow the BR.

Vulnerabilities found when reflecting upon the policy review is mainly the risk of social engineering attacks. This is because through using strictly the understanding from the policy documents the most probable attack in our opinion is an impersonation attack. Such an attack could be done by gathering information of a subscriber and impersonating them to get control over the issuance and revocation of certificates. Which can result in other attacks such as denial of service or MITM-attacks. The most vulnerable entities to this are the smaller CAs, for example JPRS, QuoVadis and Cybertrust, as their policies are less detailed or use older forms of identification and authentication. But even bigger CAs have the occasional old-fashioned method eq. Sectigo and the use of fax as the authentication method.

This thesis suggests that the most trustworthy CAs are Let's Encrypt, Digicert and Sectigo, where the choice for the applicant depends on the type of certificate requested. In general, as a subscriber the most secure alternative in terms of certificate managements is a larger CA since they seem to follow the BR to a greater extent.

7.1 Future work

For the future, it would be interesting to study changes within each policy over a larger period of time. This would highlight how internet security regarding especially HTTPS and TLS evolves.

Another interesting study would be to look further into the BR to analyze what causes the requirements to change and how that process works in regards to the CAB-Forum.

Bibliography

[1] *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*. Version 1.7.4. CA/Browser Forum, 2021. URL: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.7.3.pdf.

[2] Jake A. Berkowsky and Thaier Hayajneh. "Security issues with certificate authorities". In: *Proceedings of the IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*. 2017, pp. 449–455. DOI: 10.1109/UEMCON.2017.8249081.

[3] Hanno Böck. *How I tricked Symantec with a Fake Private Key*. URL: https://blog.hboeck.de/archives/888-How-I-tricked-Symantec-with-a-Fake-Private-Key.html. (accessed: 26.05.2021).

[4] Sharon Boeyen, Stefan Santesson, Tim Polk, Russ Housley, Stephen Farrell, and Dave Cooper. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280. May 2008. DOI: 10.17487/RFC5280.

[5] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. RFC 3647. Nov. 2003. DOI: 10.17487/RFC3647.

[6] Alan O. Freier, Philip Karlton, and Paul C. Kocher. *The Secure Sockets Layer (SSL) Protocol Version 3.0*. RFC 6101. Aug. 2011. DOI: 10.17487/RFC6101.

[7] P. Fu, Z. Li, G. Xiong, Z. Cao, and C. Kang. "SSL/TLS Security Exploration Through X.509 Certificate's Life Cycle Measurement". In: *Proceedings of the IEEE Symposium on Computers and Communications (ISCC)*. 2018. DOI: 10.1109/ISCC.2018.8538533.

[8] Oliver Gasser, Benjamin Hof, Max Helm, Maciej Korczynski, Ralph Holz, and Georg Carle. "In Log We Trust: Revealing Poor Security Practices with Certificate Transparency Logs and Internet Measurements." In: *Proceedings of Passive and Active Measurement (PAM)*. 2018, pp. 173–185. DOI: 10.1007/978-3-319-76481-8_13.

[9] *Guidelines for the Issuance and Management of Extended Validation Certificates*. Version 1.7.5. CA/Browser Forum, 2021. URL: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.7.5.pdf.

[10] Michael P. Heinl, Alexander Giehl, Norbert Wiedermann, Sven Plaga, and Frank Kargl. "MERCAT: A Metric for the Evaluation and Reconsideration of Certificate Authority Trustworthiness". In: *Proceedings of the ACM SIGSAC Conference on Cloud Computing Security Workshop (CCSW)*. 2019, pp. 1–15. DOI: 10.1145/3338466.3358917.

[11] Russ Housley, Tim Polk, and Lawrence E. Bassham III. *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 3279. May 2002. DOI: 10.17487/RFC3279.

[12] Ryan Hurst and Alex Deacon. *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*. RFC 5019. Sept. 2007. DOI: 10.17487/RFC5019.

[13] IETF. *RFCs*. URL: https://www.ietf.org/standards/rfcs/. (accessed: 12.05.2021).

[14] S. Kent. *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*. RFC 1422. Feb. 1993. DOI: 10.17487/RFC1422.

[15] Nikita Korzhitskii and Niklas Carlsson. "Characterizing the Root Landscape of Certificate Transparency Logs". In: *Proceedings of the IFIP Networking Conference (Networking)*. 2020, pp. 190–198.

[16] Nikita Korzhitskii and Niklas Carlsson. "Revocation Statuses on the Internet." In: *Proceedings of Passive and Active Measurement (PAM)*. 2021, pp. 175–191.

[17] Deepak Kumar, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Gabrielle Beck, David Adrian, Joshua Mason, Zakir Durumeric, J. Alex Halderman, and Michael Bailey. "Tracking Certificate Misissuance in the Wild". In: *Proceedings of the IEEE Symposium on Security and Privacy (SP)*. 2018, pp. 785–798. DOI: 10.1109/SP.2018.00015.

[18] Ben Laurie, Adam Langley, and Emilia Kasper. *Certificate Transparency*. RFC 6962. June 2013. DOI: 10.17487/RFC6962.

[19] Zane Ma, Joshua Mason, Manos Antonakakis, Zakir Durumeric, and Michael Bailey. "What's in a Name? Exploring CA Certificate Control". In: *Proceedings of the USENIX Security Symposium (USENIX Security)*. Aug. 2021.

[20] Henrik Nielsen, Roy T. Fielding, and Tim Berners-Lee. *Hypertext Transfer Protocol – HTTP/1.0*. RFC 1945. May 1996. DOI: 10.17487/RFC1945.

[21] Eric Rescorla. *HTTP Over TLS*. RFC 2818. May 2000. DOI: 10.17487/RFC2818.

[22] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Aug. 2018. DOI: 10.17487/RFC8446.

[23] Stefan Santesson, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Dr. Carlisle Adams. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. RFC 6960. June 2013. DOI: 10.17487/RFC6960.

[24] Quirin Scheitle, Oliver Gasser, Theodor Nolte, Johanna Amann, Lexi Brent, Georg Carle, Ralph Holz, Thomas C. Schmidt, and Matthias Wählisch. "The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem". In: *Proceedings of the Internet Measurement Conference (IMC)*. 2018, pp. 343–349. DOI: 10.1145/3278532.3278562.

[25] Ryan Sleevi. *Sustaining Digital Certificate Security*. URL: https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html. (accessed: 26.05.2021).

[26] *Tranco's list of the top 1 million sites on the web*. Mar. 2021. URL: https://tranco-list.eu.

[27] Ahmad Samer Wazan, Romain Laborde, David Chadwick, Remi Venant, Abdelmalek Benzekri, Eddie Billoir, and Omar Alfandi. "On the Validation of Web X.509 Certificates by TLS interception products". In: *Proceedings of IEEE Transactions on Dependable and Secure Computing*. 2020. DOI: 10.1109/TDSC.2020.3000595.

[28] *What's the difference between DV, OV & EV SSL Certificates?* Accessed: 2021-06-16. URL: https://www.digicert.com/difference-between-dv-ov-and-ev-ssl-certificates.

A Appendix

A.1 Top 100 CAs

Table A.1: Top 100 CAs

No.	Issuing CA	% of certs.	CA Group
1	Let's Encrypt	39.395	Let's Encrypt
2	Cloudflare, Inc.	19.198	Digicert
3	DigiCert Inc	9.412	Digicert
4	Sectigo Limited	8.622	Sectigo
5	cPanel, Inc.	4.866	Sectigo
6	GoDaddy.com, Inc.	4.238	Starfield
7	Amazon	3.554	Amazon
8	GlobalSign nv-sa	3.010	GlobalSign
9	Starfield Technologies, Inc.	1.598	Starfield
10	TrustAsia Technologies, Inc.	0.633	Digicert
11	Asseco Data Systems	0.613	Certum
12	Entrust, Inc.	0.612	Entrust
13	Google Trust Services	0.556	Google Trust
14	COMODO CA Limited	0.327	Sectigo
15	ZeroSSL	0.257	Sectigo
16	Gandi	0.247	Sectigo
17	GoGetSSL	0.247	Sectigo
18	Actalis S.p.A.	0.214	Actalis
19	Network Solutions L.L.C.	0.173	Network Solutions
20	GEANT Vereniging	0.132	Sectigo
21	Corporation Service Company	0.130	Sectigo
22	InCommon	0.129	Sectigo
23	Japan Registry Services Co., Ltd.	0.127	JPRS
24	home.pl S.A.	0.109	Certum

Continued on next page

Table A.1: Continued from previous page

No.	Issuing CA	% of certs.	CA Group
25	Trustwave Holdings, Inc.	0.100	SecureTrust
26	SECOM Trust Systems CO.,LTD.	0.098	SECOM
27	Microsoft Corporation	0.093	Microsoft
28	Cybertrust Japan Co., Ltd.	0.091	Cybertrust
29	QuoVadis Limited	0.083	QuoVadis
30	Gehirn Inc.	0.082	Sectigo
31	TERENA	0.082	Digicert
32	Verein zur Foerderung eines Deutschen Forschungsnetzes e. V.	0.078	Telesec
33	SecureCore	0.066	SecureCore
34	WoTrus CA Limited	0.056	Sectigo
35	nazwa.pl sp. z o.o.	0.045	Certum
36	GeoTrust Inc.	0.044	Digicert
37	DOMENY.PL sp. z o.o	0.037	Sectigo
38	T-Systems International GmbH	0.036	Telesec
39	SwissSign AG	0.032	SwissSign
40	TAIWAN-CA	0.031	TAIWAN-CA
41	Soluciones Corporativas IP, SL	0.029	Sectigo
42	The USERTRUST Network	0.022	Sectigo
43	Buypass AS-983163327	0.021	Buypass
44	Trust Provider B.V.	0.021	Digicert
45	Symantec Corporation	0.021	Digicert
46	KPN B.V.	0.020	KPN
47	DHIMYOTIS	0.018	DHIMYOTIS
48	The Trustico Group Ltd	0.018	Sectigo
49	CentralNic Luxembourg	0.016	Sectigo
50	NetLock Kft.	0.016	NetLock
51	Hongkong Post	0.014	Hongkong
52	TeliaSonera	0.013	TeliaSonera
53	HydrantID (Avalanche Cloud Corporation)	0.011	QuoVadis
54	thawte, Inc.	0.011	Digicert
55	AC Camerfirma S.A.	0.010	AC Camerfirma
56	E-Tugra EBG Biligim Teknolojileri ve Hizmetleri	0.010	E-tugra
57	Fiducia & GAD IT AG	0.010	QuoVadis
58	D-Trust GmbH	0.010	D-Trust
59	Isimtescil Bilisim Anonim Sirketi	0.010	E-tugra
60	StartCom Ltd.	0.009	StartCom Ltd.
61	Alpiro s.r.o.	0.009	Sectigo
62	Snake Oil, Ltd	0.008	Snake Oil, Ltd
63	Deutsche Post AG	0.008	Globalsign
64	FNMT-RCM	0.008	FNMT
65	Beijing Xinchacha Credit Management Co., Ltd.	0.008	Certum
66	EUNETIC GmbH	0.008	Sectigo
67	Yandex LLC	0.007	Certum
68	Apple Inc.	0.007	Apple
69	Globe Hosting, Inc.	0.007	Sectigo
70	TBS INTERNET	0.006	Sectigo
71	MULTICERT - Servicios de Certificado Electronica	0.006	AC Camerfirma

Continued on next page

Table A.1: Continued from previous page

No.	Issuing CA	% of certs.	CA Group
72	AffirmTrust	0.006	Entrust
73	Chunghwa Telecom Co., Ltd.	0.005	Chunghwa Telecom
74	eMudhra Technologies Limited	0.005	Sectigo
75	China Financial Certification Authority	0.005	CFCA
76	Microsec Ltd.	0.005	Microsec
77	Site Blindado S.A.	0.005	Sectigo
78	Firmaprofesional S.A.	0.004	Firmaprofesional
79	IZENPE S.A.	0.004	IZENPE
80	Shanghai Ping An Credit Reference Company Limited	0.004	Certum
81	WoSign CA Limited	0.004	WoSign
82	CertCloud Pte. Ltd.	0.004	Sectigo
83	Nijimo K.K.	0.004	Sectigo
84	LH.pl Sp. z o.o.	0.003	Certum
85	Fortinet	0.003	Digicert
86	Fortinet	0.003	Starfield
87	Baidu, Inc.	0.003	Sectigo
88	BitCert	0.003	Sectigo
89	ICP-Brasil	0.003	ICP-Brasil
90	iTrusChina Co., Ltd.	0.003	Certum
91	K Software	0.003	Sectigo
92	SSL.com	0.003	Sectigo
93	TrustSign Certificadora Dig. & Soluciones Seguranda da Inf. Ltda.	0.003	Sectigo
94	Aetna Inc	0.002	Digicert
95	Global Digital Cybersecurity Authority Co., Ltd.	0.002	GDCA
96	Max-Planck-Gesellschaft	0.002	Telesec
97	Telia Finland Oyj	0.002	TeliaSonera
98	certSIGN	0.002	certSign
99	Dreamcommerce S.A.	0.002	Certum
100	Turkiye Bilimsel ve Teknolojik Arastirma Kurumu	0.002	Turkiye Bilimsel

A.2 Full list of top CA groups

Table A.2: Full list of top CA groups

No.	CA group	% of certs.
1	Let's Encrypt	39.395
2	DigiCert Inc	29.427
3	Sectigo Limited	15.279
4	Starfield Technologies, Inc.	5.839
5	Amazon	3.554
6	GlobalSign nv-sa	3.019
7	Certum	0.794
8	Entrust, Inc.	0.618
9	Google Trust Services	0.556
10	Actalis S.p.A.	0.214
11	SECOM Trust Systems CO.,LTD.	0.189
12	Network Solutions L.L.C.	0.173
13	Japan Registry Services Co., Ltd.	0.127
14	Telesec	0.117
15	Trustwave Holdings, Inc.	0.100
16	Microsoft Corporation	0.093
17	Cybertrust	0.091
18	SecureCore	0.066
19	SwissSign	0.032
20	TAIWAN-CA	0.031
21	Buypass	0.021
22	QuoVadis Limited	0.021
23	E-tugra	0.020
24	KPN	0.020
25	DHIMYOTIS	0.018
26	NetLock	0.016
27	AC Camerfirma	0.016
28	TeliaSonera	0.016
29	HongKong	0.016
30	D-Trust	0.014
31	StartCom Ltd.	0.010
32	FNMT	0.008
33	Apple	0.007
34	Chunghwa Telecom	0.005
35	CFCA	0.005
36	Microsec	0.005
37	Firmaprofesional	0.004
38	IZENPE	0.004
39	WoSign	0.004
40	ICP-Brasil	0.003
41	GDCA	0.002
42	certSign	0.002

A.3 Full RFC list

Table A.3 displays all RFCs mentioned in the CP documents, the RFCs that has been obsoleted by another RFC document is coloured orange and those that has been updated by another RFC document is coloured yellow.

Table A.3: Complete list of RFCs mentioned by the CAs.

RFC	RFC Name	Obsoleted by	Updated by	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
RFC 1766	Tags for the Identification of Languages	RFC 3066, RFC 3282									x										
RFC 1918	Address Allocation for Private Internets		RFC 6761						x												
RFC 2044	UTF-8, a transformation format of Unicode and ISO 10646	RFC 2279									x										
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels		RFC 8174	x	x		x	x					x		x		x				
RFC 2247	Using Domains in LDAP/X.500 Distinguished Names		RFC 4519, RFC 4524								x										
RFC 2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names	RFC 4510, RFC 4514	RFC 3377		x		x		x						x						
RFC 2314	PKCS 10: Certification Request Syntax Version 1.5	RFC 2986												x							
RFC 2460	Internet Protocol, Version 6 (IPv6 Specification	RFC 8200	RFC 5095, RFC 5722, RFC 5871, RFC 6437, RFC 6564, RFC 6935, RFC 6946, RFC 7045, RFC 7112						x												
RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	RFC 4210									x										
RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	RFC 3647		x				x	x				x				x				
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	RFC 6960	RFC 6277					x			x								x		

Continued on next page

Table A.3: Continued from previous page

RFC	RFC Name	Obsoleted by	Updated by	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
RFC 2616	Hypertext Transfer Protocol – HTTP/1.1	RFC 7230, RFC 7231, RFC 7232, RFC 7233, RFC 7234, RFC 7235	RFC 2817, RFC 5785, RFC 6266, RFC 6585		x					x											
RFC 2630	Cryptographic Message Syntax	RFC 3369, RFC 3370									x										
RFC 2986	PKCS 10: Certification Request Syntax Specification Version 1.7		RFC 5967											x							
RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols										x										
RFC 3126	Electronic Signature Formats for long term electronic signatures	RFC 5126									x										
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)						x		x		x	x				x					
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile		RFC 4055, RFC 4491, RFC 5480, RFC 5758, RFC 8692				x									x		x			
RFC 3492	Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)		RFC 5891																	x	
RFC 3546	Transport Layer Security (TLS) Extensions	RFC 4366															x				
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RFC 3709	Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates		RFC 6170									x									
RFC 3739	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile																x				
RFC 3912	WHOIS Protocol Specification			x					x				x				x				

Continued on next page

Table A.3: Continued from previous page

RFC	RFC Name	Obsoleted by	Updated by	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
RFC 3966	The tel URI for Telephone Numbers		RFC 5341	x																	
RFC 4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile																x				
RFC 4366	Transport Layer Security (TLS) Extensions	RFC 5246, RFC 6066	RFC 5746	x				x	x				x					x		x	
RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map																				x
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments		RFC 8996	x	x	x	x	x	x	x			x		x		x	x		x	
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile		RFC 6818, RFC 8398, RFC 8399	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RFC 5754	Using SHA2 Algorithms with Cryptographic Message Syntax						x								x						
RFC 5758	Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA						x								x						
RFC 6170	Internet X.509 Public Key Infrastructure – Certificate Image											x									
RFC 6454	The Web Origin Concept			x		x		x				x	x				x			x	
RFC 6532	Internationalized Email Headers			x																	
RFC 6844	DNS Certification Authority Authorization (CAA) Resource Record						x	x		x					x	x	x		x		
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP		RFC 8954	x	x	x	x		x	x	x	x	x	x	x		x	x		x	x
RFC 6962	Certificate Transparency			x	x		x	x		x		x	x		x	x	x	x	x	x	x

Continued on next page

Table A.3: Continued from previous page

RFC	RFC Name	Obsoleted by	Updated by	Baseline Requirements	Let's Encrypt	Digicert	Sectigo	Amazon	GlobalSign	Starfield	Asseco	Entrust	Google Trust	Actalis	Network Solutions	JPRS	Trustwave	SECOM	Microsoft	Cybertrust	QuoVadis
RFC 791	DARPA Internet Program Protocol Specification		RFC 1349, RFC 2474, RFC 6864						x												
RFC 7231	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content			x						x		x	x				x			x	
RFC 7301	Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension			x									x								
RFC 7482	Registration Data Access Protocol (RDAP) Query Format			x					x				x				x				
RFC 7686	The ".onion" Special-Use Domain Name			x																	
RFC 7719	DNS Terminology	RFC 8499		x								x	x								
RFC 822	Standard for the Format of ARPA Internet Text Messages	RFC 2822	RFC 1123, RFC 1138, RFC 1148, RFC 1327, RFC 2156			x	x		x		x	x									
RFC 8555	Automatic Certificate Management Environment (ACME)			x						x							x				
RFC 8659	DNS Certification Authority Authorization (CAA) Resource Record			x						x		x	x							x	x
RFC 8737	Automated Certificate Management Environment (ACME) TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension			x								x									

A.4 URLs for CP and CPS

Example:

- *Certificate Authority*
  - *URL of Certificate Policy*
  - *Version of CP*
  - *URL of Certificate Practice Statement*
  - *Version of CPS*

List of links:

- Let's Encrypt
  - https://letsencrypt.org/documents/isrg-cps-v3.1/
  - Version: 3.1
  - Same as CP.
  - Version: Same as CP.
- Digicert
  - https://www.digicert.com/content/dam/digicert/pdfs/legal/DigiCert-CP-v5.6.pdf
  - Version: 5.6
  - https://www.digicert.com/content/dam/digicert/pdfs/legal/DigiCert-CPS-V.5.6.pdf
  - Version: 5.6
- Sectigo
  - https://sectigo.com/uploads/files/Sectigo-CPS-v5_2_2.pdf
  - Version: 5.2.2
  - Same as CP.
  - Version: Same as CP.
- Amazon
  - https://www.amazontrust.com/repository/cp-1.0.1.pdf
  - Version: 1.0.1
  - https://www.amazontrust.com/repository/cps-1.0.10.pdf
  - Version: 1.0.10
- GlobalSign
  - https://www.globalsign.com/en/repository/GlobalSign_CP_v6.7_final.pdf
  - Version: 6.7
  - https://www.globalsign.com/en/repository/GlobalSign_CPS_v9.7_final.pdf
  - Version: 9.7
- Starfield
  - https://certs.starfieldtech.com/repository/certificate_practices/StarfieldCertificatePolicyandCertificationPracticeStatement.pdf

  - Version: 4.9
  - Same as CP.
  - Version: Same as CP.

- Asseco
  - https://files.certum.eu/documents/repsitory/1-cert-policycert-pract-state-qcs/CCK-DK02-ZK02-CP-and-CPS-5.7.pdf
  - Version: 5.7
  - Same as CP.
  - Version: Same as CP.

- Entrust
  - https://www.entrust.com/-/media/documentation/licensingandagreements/ssl-cps-english-20201231-version-38.pdf
  - Version: 3.8
  - Same as CP.
  - Version: Same as CP.

- Google Trust
  - https://static.googleusercontent.com/media/pki.goog/sv//repo/cp/2.0/GTS-CP.pdf
  - Version: 2.0
  - Same as CP.
  - Version: Same as CP.

- Actalis
  - https://www.actalis.it/documenti-it/caact-free-s-mime-certificates-policy.aspx
  - Version 1.2
  - https://www.actalis.it/documenti-en/qualified-certificates-cps.aspx
  - Version: 1.8

- Network Solutions
  - https://assets.web.com/legal/English/CertificationPracticeStatement32.pdf
  - Version: 3.2
  - Same as CP.
  - Version: Same as CP.

- JPRS
  - https://jprs.jp/pubcert/info/repository/JPRS-CP-en.pdf
  - Version: 2.22
  - https://jprs.jp/pubcert/info/repository/JPRS-CPS-en.pdf
  - Version: 1.11

- Trustwave
  - https://certs.securetrust.com/CA/SecureTrustCPS_64.pdf

  - Version: 6.4
  - Same as CP.
  - Version: Same as CP.

- SECOM
  - https://repo1.secomtrust.net/spcpp/pfw/pfwev2ca/Contents/PfWEVCA-CP-EN.pdf
  - Version: 2.75
  - https://repo1.secomtrust.net/spcpp/cps/SECOM-CPS-EN.pdf
  - Version: 2.14

- Microsoft
  - https://www.microsoft.com/pki/mscorp/cps/default.htm
  - Version: 2.7
  - Same as CP.
  - Version: Same as CP.

- Cybertrust
  - https://www.cybertrust.ne.jp/ssl/repository/OVCP_English.pdf
  - Version: 1.6
  - Same as CP.
  - Version: Same as CP.

- QuoVadis
  - https://www.quovadisglobal.com/wp-content/uploads/2021/03/QV_RCA1_RCA3_CPCP§_V4_32_Approved.pdf
  - Version: 4.32
  - Same as CP.
  - Version: Same as CP.