Certification Policy
certSIGN

Version 1.17

Date: 18 April 2024

Important Notice

This document is the property of CERTSIGN SA

Address: 29 A Tudor Vladimirescu Avenue,
AFI Tech Park 1, Bucharest, Romania
Phone: 004-021-31.19.901
Fax: 004-021-31.19.905

Web: www.certsign.ro

Document history

Version	Effective Date[1]	Reason	The person who made the change
1.0	April 2006	Releasing the first version	Electronic Services Manager
1.1	July 2009	Changing the company's registered office to 107A Oltenitei Rd., District 4, Bucharest, Romania.	Electronic Services Manager
1.2	March 2014	Adding the new CA Class 3 Enterprise G2	Technical Director
1.3	July 2015	Adding the new certification authorities: certSIGN CA Class 2 G2 certSIGN Qualified CA Class 3 G2 certSIGN Non-Repudiation CA Class 4 G2	Technical Director
1.4	10 January 2016	Adding the new closed circuit certification authorities, that issue certificates for the Electronic Payment System operated by Transfond S.A.	Technical Director
1.5	25 January 2016	Adding a new certification authority designed for issuing code signing certificates. The OID for Non-EV Code Signing 2.23.140.1.4.1. was introduced in the description of the certification policy. Also, the OV 2.23.140.1.2.2. OID was included in the certification policy associated to SSL certificates.	Technical Director
1.6	26 November 2018	Update change headquarters	PKI Policies Manager
1.7	31 January 2019	Annual review	PKI Policies Manager
1.8	31 January 2020	Annual review	PKI Policies Manager
1.9	29 January 2021	Annual review	PKI Policies Manager
1.10	23 March 2021	Updates with SSL CA for DV & EV	PKI Policies Manager
1.11	23 November 2021	Minor updates & corrections	PKI Policies Manager
1.12	31 January 2022	Annual review	PKI Policies Manager
1.13	6 June 2022	Minor correction	PKI Policies Manager
1.14	31 Jan.2023	Annual Review	PKI Policies Manager
1.15	31 July 2023	Add mapping table to RFC 3647 outline	PKI Policies Manager
1.16	31 January 2024	Annual Review	PKI Policies Manager
1.17	18 April 2024	Add cross-certificate	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
Electronic Services Manager	Electronic Services Manager	27 January 2006

Distribution list

Destination	Distribution date
Public-Internet	25 January 2016
Public-Internet	26 November 2018
Public-Internet	31 January 2019
Public-Internet	31 January 2020
Public-Internet	29 January 2021
Public-Internet	23 March 2021
Public-Internet	23 November 2021
Public-Internet	31 January 2022
Public-Internet	6 June 2022
Public-Internet	31 Jan.2023
Public-Internet	31 July 2023
Public-Internet	31 January 2024

[1] *The effective date is the last day of the month*

This document was approved by

Version	Name	Data
1.0	Policies and Procedures Management Body	April 2006
1.1	Policies and Procedures Management Body	June 2009
1.2	Policies and Procedures Management Body	March 2014
1.3	Policies and Procedures Management Body	June 2015
1.4	Policies and Procedures Management Body	December 2015
1.5.	Policies and Procedures Management Body	January 2016
1.6.	Policies and Procedures Management Body	November 2016
1.7.	Policies and Procedures Management Body	January 2019
1.8.	Policies and Procedures Management Body	January 2020
1.9	Policies and Procedures Management Body	January 2021
1.10	Policies and Procedures Management Body	March 2021
1.11	Policies and Procedures Management Body	November 2021
1.12	Policies and Procedures Management Body	January 2022
1.13	Policies and Procedures Management Body	June 2022
1.14	Policies and Procedures Management Body	January 2023
1.15	Policies and Procedures Management Body	July 2023
1.16	Policies and Procedures Management Body	January 2024

Content

1. Introduction

certSIGN's Certification Policy (CP) describes the general rules and principles applied by certSIGN during the certification process of the public keys and in using the time stamping authority (TSA), as well as for other non-repudiation services. The certification policy defines:

- The entities involved within the certification process,
- The responsibilities and obligations of every entity,
- The types of certificates,
- The types of confirmations,
- The identity checking procedures and
- Applicability area.

The detailed description of the above-mentioned rules is presented in the **Certificate Practices Statements (CPS).**

The knowledge of the Certification Policy, as well as of the CPSs is important especially for the users and for the certSIGN's partner entities.

certSIGN complies with requirements of the latest published version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org and current version of Mozilla Root Store Policy, Apple Root Certificate Program, Microsoft Trusted Root Program and Chrome Root Program Policy.

certSIGN Root policy is to include Issuing CAs, Subordinate CAs (Subordinate CA means a CA operated by a different party than the Root), and cross-certifications, if any.

2. Certificates

The certificate is a data chain (message) that contains at least the name and the authority's identifier, the subscriber's identifier, its public key, the validity period, serial number and the signature of the issuing authority.

The certificates are used to link the subscriber's personal data with the specific public keys. The certificate's owner is also the owner of the private key corresponding with the certificate's public key. The identification data contained in the certificate allow other parties to determine the exact owner of the certificate. If the private key is used during the electronic signing of a message the receiver can be sure that the message was created using the private key corresponding with the certificate's public key (otherwise said it was created by the certificate's owner) and the message was not modified by anybody else.

By issuing a certificate to a subscriber the certSIGN Certification Authority confirms:

- Its identity or the credibility of other data, such as the electronic mail address;

- The public key contained in the certificate belongs to the respective subscriber.

Due to those mentioned above, the partner entities, after receiving a signed message, can determine who the certificate's owner is that signed the message, and optionally, can make him liable for his actions or assumed engagements.

certSIGN provides services in compliance with the legislation and the relevant practices. The certification authority's keys are protected using hardware security modules (HSM), certified according with FIPS 140-2 level 3. certSIGN implements physic and procedural checking of the system. The digital certificates are signed using RSA algorithm in combination with SHA-2 cryptographic digest, and keys with minimum 2048 bits.

The certSIGN Certification Authority issues certificates of different Classes with different credibility levels. The certificate's credibility depends on the procedure regarding the subscriber's identity checking and, on the effort, made by certSIGN's operators to check the data sent by the solicitant within his registration request. As well, the certificate's class can depend on the security Class of the server or of the network device for which the certificate is issued. certSIGN's experts can check the technical status and the security Class of one subscriber's IT system before issuing a certificate with the highest credibility Class.

The Certification Authority certSIGN CA issues certificates for the large audience and provides services specific for a public key infrastructure. Among the most important applications of the certificates issued by certSIGN CA there can be mentioned (without limiting to):

- Electronic documents signing,
- Security for Web transactions,
- Security for network communications,
- Time stamps.

2.1. Class 1 certificates

The class 1 certificates are issued by the Certification Authority **certSIGN Demo CA Class 1.** These certificates are used only for demonstrations and do not provide any warranty regarding the subject's identity. The demo certificates are mainly for testing the applications or devices' performances before buying the final certificates. The Certification Authority certSIGN Demo CA Class 1 issues certificates for almost every purpose. In most cases during the registration process the e-mail address and/or the name and first name of the natural person or the legal entity's representative are checked.

The class 1 certificates contain the following policy identifier:

{certSIGN}* id-policy(1) id-cp(1)id-Class-1(1)

certSIGN does not assume any financial obligation and does not offer any warranty for the certificates (and their content) issued under the above-mentioned policy.

2.2. Class 2 certificates

The Class 2 certificates are issued by the **certSIGN CA Class 2 G2** Certification Authority**.** These are personal certificates and are mainly used for securing electronic correspondence or for clients' authentication during online sessions. The operators of the certSIGN CA Class 2 G2 Certification Authorities check the data provided by clients during the certification process. The identity of the natural person solicitant or of the legal entity's representative is checked. The authenticity of the e-mail address included in the certificate is also checked.

The Class 2 certificates contain the following policy identifier:

{certSIGN} .id-policy(1). id-cp(1).id-Class-2(2)

The certificates issued under this policy provide limited warranties and responsibilities.

Additionally, class 2 certificates are issued with 3 closed circuit certification authorities. These certificates are issued for the Electronic Payment System (EPS) operated by Transfond S.A., based on a technical protocol. The authorities that issue certificates for EPS are:

1. CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.2.1.1
2. CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.2.1.2
3. CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.2.1.3

The class 2 certificates for EPS refer the following policy identifier:

{certSIGN} .id-policy(1). id-cp(1).id-Class-2(2).id-Transfond(1)

The certificates issued under this policy must respect the technical protocol concluded between certSIGN and Transfond.

2.3. Class 3 certificates

The Class 3 certificates are issued by the **certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3 G2, certSIGN SSL DV CA Class 3 G2** Certification Authorities. The certificates issued within this class can be qualified certificates or certificates for securing the

** {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (20715)*

binary objects and the protection of data transmissions using IPSec, SSL and TLS protocols. The certSIGN operators check the data provided by the clients (organizations or institutions) during the registration process. All data that are going to be included in the certificate are thoroughly checked. Based on a certificate issued by certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3 G2, certSIGN SSL DV CA Class 3 G2, an individual's identity or an organization's authenticity can accurately be determined.

The qualified certificates issued by certSIGN Qualified CA Class 3 G2 can be used to create electronic signatures to replace the handwritten signatures.

The qualified certificates are issued by the **certSIGN Qualified CA Class 3 G2** Certification Authorities. These certificates are compliant with the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, the Electronic Signature Law 455/2001 in Romania and the Government Decision 1259/December 2001 regarding the Electronic Signature Law Applicability Terms.

certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3 G2, certSIGN SSL DV CA Class 3 G2 use a certificate issued with the sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) algorithm.

Class 3 Certificates contain the following policy identifier:

{certSIGN} id-policy(1) id-cp(1)id-Class-3(3)

In addition, for **qualified certificates** the following policy identifier is added:
itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1); (0.4.0.1456.1.1).

For the certificates issued by **certSIGN Enterprise CA Class 3 G2**, the following policy identifier is added **{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)}; (2.23.140.1.2.2)**.

For certificates issued by **certSIGN SSL DV CA Class 3 G2**, the policy identifier is:
{certSIGN} id-policy(1) id-cp(1) id-DV-CA(5) and the following policy identifier is added:
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)}; (2.23.140.1.2.1).

certSIGN's financial responsibility for the data in the certificates issued under the above policies is described in the CPSs (CPPs) (see http://www.certSIGN.ro/repository). The certificates issued under these policies provide complete warranties and responsibilities.

Additionally, class 3 certificates are issued with a closed circuit certification authority. The certificates are issued for the Electronic Payment System (EPS) operated by Transfond S.A., based on a technical protocol. The authority that issues certificates for EPS are:

1. CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3, with the following policy identifier: 1.3.6.1.4.1.25017.1.1.3.1.1

The class 3 certificates for EPS refer the following policy identifier:

{certSIGN} .id-policy(1). id-cp(1).id-Class-3(3).id-Transfond(1)

The certificates issued under this policy must respect the technical protocol concluded between certSIGN and Transfond. The certificates issued by this authority do not include the qualified certificate identifier.

2.4. Class 4 certificates

The Class 4 certificates are issued by the **certSIGN Non-Repudiation CA Class 4 G2** Certification Authorities. These certificates are mainly for the intermediate Certification Authorities or other trust services providers (OCSP or Time Stamp Authorities). The **certSIGN Non-Repudiation CA Class 4 G2** operators check the identity of the clients that must present themselves at one of the certSIGN's counters. The power of attorney from the company, the authenticity and correctness of the identity documents as well as the organization's documents will be checked. **certSIGN Non-Repudiation CA Class 4 G2** also accept documents certified by a public notary. Based on a certificate issued by **certSIGN Non-Repudiation CA Class 4 G2** an individual's identity, an organization's authenticity or the credibility of an external Certification Authority can accurately be determined. The availability period for a Class 4 certificate is of minimum 2 years. The keys of the subscriber that owns a Class 4 certificate must be protected using hardware security modules (HSM).

The Class 4 certificates contain the following policy identifier:

{certSIGN} id-policy(1) id-cp(1)id-Class-4(4)

The certificates issued under this policy provide complete warranties and responsibilities.

The certSIGN Subscriber can choose the type of certificate fit for his needs. The certificate types are described in detail within the CPS (CPP) that can be read on certSIGN's Web site. As well, this information can be received by electronic mail after sending a message to the address: office@certSIGN.ro.

3. Non-repudiation counters

The non-repudiation counters are data structures (messages) containing at least:

- The information provided to (for example hash value, serial number of the certificate, request number etc.) a non-repudiation authority and
- The electronic signature of the respective authority.

The non-repudiation authorities that provide services to the clients are affiliated to certSIGN.

By issuing a counter a non-repudiation authority confirms the appearance of an event when it is created or at a previous moment. This event can be: sending a document, the date when the signature was created etc. The partner entity can check, based on the received data, the signature's correctness based on the trust in certSIGN CA.

3.1. OCSP Confirmation Response

OCSP responses (*Online Certificate Status Protocol*) are issued by the **certSIGN Validation Service** Authority. The OCSP responses are used mainly to determine the certificate's status. These services are publicly available and represent an alternative for the Certificate Revocation Lists (CRL). certSIGN Validation Service provides warranties for the OCSP responses issued, within the limits described in the CPS. The way in which the OCSP authority functions and the additional information regarding this service are presented on the web page (please see https://www.certsign.ro/) and in the CPS.

4. Warranties provided by certSIGN

Depending on the type of certificate issued, certSIGN warranties that will make the necessary effort to check properly the information included in the certificates (please see the CPS - Chapter 3.2). The information checking is important in first instance for the partner entities that receive messages from a subscriber that identifies himself through a qualified digital certificate issued by certSIGN. Therefore, certSIGN is responsible from financial point of view for the damages resulted following the negligence or the errors made by certSIGN regarding these types of certificates. certSIGN's responsibilities depend on the subscriber's certificate class and the responsibility is both towards the subscriber and to the partner entities that trust the information in the certificate (please see the CPS – chapter 2 and chapter 9).

The certSIGN warranties can be limited by certain restrictions. These restrictions are announced to the subscriber that confirms this thing within a statement (please see the statement for Certificate Acceptance). certSIGN warrants the uniqueness of its subscribers' electronic signatures.

5. Certificate acceptance

certSIGN's responsibilities and warranties are applicable from the moment the subscriber accepts the certificate. The way the certificate is delivered and its acceptance are described within the CPS (please see chapter 4.4 Certificate Acceptance) and are detailed within the agreements concluded with the subscribers.

6. Certification service

certSIGN provides five basic services:

(1) registration,

(2) issuing a digital certificate,

(3) renewal of a certificate,

(4) revocation of a certificate and

(5) checking the status of a certificate.

Moreover, certSIGN also provides non-repudiation services:

(6) On-line status validation service for digital certificates.

The purpose of the registration is to check a subscriber's identity and precedes the operation of issuing the certificate (please see the CPS, chapter 3 Identification and authentication and chapter 4.1 Certificate application).

The renewal of a certificate takes place when a subscriber already registered wants to obtain a certificate for the same public key with the modification of the availability period (please see the CPS, Chapter 4.6 Certificate Renewal and Chapter 4.7 Certificate Re-Key).

The revocation of a certificate takes place when the corresponding private key from the digital certificate was compromised or is susceptible of being compromised (please see the CPS, Chapter 4.9 Certificate Revocation and Suspension).

The checking of a certificate's status is a service through which certSIGN confirms the validation of a digital certificate using the Certificate Revocation Lists (CRL) issued by the affiliated authorities. The checking of a certificate's status can be done by means of the on-line validation service for the certificate status (please see the CPS, Chapter 4.10 Certificate Status Services).

certSIGN allows that every key pair (private-public) to be generated by the subscriber. certSIGN can make recommendations regarding the devices for key generation. In certain specific conditions, certSIGN can generate unique key pairs and deliver them to the subscribers.

7. The partner entity

It is mandatory for the partner entity to check every electronic signature on the received documents (including the digital certificate). During the checking process the partner entity must use the procedures and resources made available by certSIGN. Among others these specify the need to check the certificate revocation list published by certSIGN and the allowed certification ways (please see the CPS, Chapter 4.5 Key Pair and Certificate Usage).
Every document for which there are problems when checking the digital signature must be rejected and checked using other ways or procedures, such as the document's checking by a public notary.

8. The subscriber

It is mandatory for the subscriber to safely keep his/her private key to prevent the unauthorized access of a third party to it. In case there is the suspicion that the private key was accessed by a third party, the subscriber must immediately inform the authority that issued the respective digital certificate. The information sent to the authority must be detailed enough so as to allow determining the exact identity of the person whose digital certificate will be revoked.

9. Updating the certification policy

certSIGN's Policies and Procedures Management Body is responsible for the approval of this CP. certSIGN's Certification Policy is annually reviewed and updated. These modifications will be available to all subscribers via certSIGN's Web site. The subscribers who do not accept the modifications brought to the certification policy must send certSIGN a statement in this regard and to renounce the services provided by certSIGN.

10. Taxes

The certification services provided by certSIGN are commercially available. The prices for these services depend on the class of the certificates issued to or owned by a subscriber and on the type of the requested service. The taxes are described in the price lists available on certSIGN's Web site (https://www.certsign.ro/).

RFC 3647 outline to Certification Policy mapping table

RFC 3647 outline	No	Cert.Policy Outline
1. INTRODUCTION	1.	Introduction
1.1 Overview	1.	Introduction
1.2 Document name and identification	1.	Introduction
1.3 PKI participants	1.	Introduction
1.3.1 Certification authorities	1.	Introduction
1.3.2 Registration authorities	1.	Introduction
1.3.3 Subscribers	8.	The subscriber
1.3.4 Relying parties	1.	Introduction
1.3.5 Other participants	7.	The partner entity
1.4 Certificate usage	2.	Certificates
1.4.1. Appropriate certificate uses	2.	Certificates
1.4.2 Prohibited certificate uses	2.	Certificates
1.5 Policy administration	1.	Introduction
1.5.1 Organization administering the document	1.	Introduction
1.5.2 Contact person	1.	In the footer
1.5.3 Person determining CPS suitability for the policy	1.	Introduction
1.5.4 CPS approval procedures	9.	Updating the certification policy
1.6 Definitions and acronyms	1.	Introduction
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	9.	Updating the certification policy
2.1 Repositories	6.	Certification service
2.2 Publication of certification information	9.	Updating the certification policy
2.3 Time or frequency of publication	9.	Updating the certification policy
2.4 Access controls on repositories	9.	Updating the certification policy
3. IDENTIFICATION AND AUTHENTICATION (11)	1.	Introduction
3.1 Naming	1.	Introduction
3.1.1 Types of names	1.	Introduction
3.1.2 Need for names to be meaningful	1.	Introduction
3.1.3 Anonymity or pseudonymity of subscribers	1.	Introduction
3.1.4 Rules for interpreting various name forms	1.	Introduction
3.1.5 Uniqueness of names	1.	Introduction
3.1.6 Recognition, authentication, and role of trademarks	1.	Introduction
3.2 Initial identity validation	1.	Introduction
3.2.1 Method to prove possession of private key	1.	Introduction
3.2.2 Authentication of organization identity	1.	Introduction
3.2.3 Authentication of individual identity	1.	Introduction
3.2.4 Non-verified subscriber information	1.	Introduction
3.2.5 Validation of authority	1.	Introduction
3.2.6 Criteria for interoperation	1.	Introduction
3.3 Identification and authentication for re-key requests	1.	Introduction
3.3.1 Identification and authentication for routine re-key	1.	Introduction
3.3.2 Identification and authentication for re-key after revocation	1.	Introduction
3.4 Identification and authentication for revocation request	1.	Introduction
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)	1.	Introduction

RFC 3647 outline	No	Cert.Policy Outline
4.1 Certificate Application	1.	Introduction
4.1.1 Who can submit a certificate application	1.	Introduction
4.1.2 Enrollment process and responsibilities	1.	Introduction
4.2 Certificate application processing	1.	Introduction
4.2.1 Performing identification and authentication functions	1.	Introduction
4.2.2 Approval or rejection of certificate applications	1.	Introduction
4.2.3 Time to process certificate applications	1.	Introduction
4.3 Certificate issuance	1.	Introduction
4.3.1 CA actions during certificate issuance	1.	Introduction
4.3.2 Notification to subscriber by the CA of issuance of certificate	1.	Introduction
4.4 Certificate acceptance	5.	Certificate acceptance
4.4.1 Conduct constituting certificate acceptance	5.	Certificate acceptance
4.4.2 Publication of the certificate by the CA	5.	Certificate acceptance
4.4.3 Notification of certificate issuance by the CA to other entities	5.	Certificate acceptance
4.5 Key pair and certificate usage	1.	Introduction
4.5.1 Subscriber private key and certificate usage	1.	Introduction
4.5.2 Relying party public key and certificate usage	1.	Introduction
4.6 Certificate renewal	6.	Certification service
4.6.1 Circumstance for certificate renewal	6.	Certification service
4.6.2 Who may request renewal	6.	Certification service
4.6.3 Processing certificate renewal requests	6.	Certification service
4.6.4 Notification of new certificate issuance to subscriber	6.	Certification service
4.6.5 Conduct constituting acceptance of a renewal certificate	6.	Certification service
4.6.6 Publication of the renewal certificate by the CA	6.	Certification service
4.6.7 Notification of certificate issuance by the CA to other entities	6.	Certification service
4.7 Certificate re-key	6.	Certification service
4.7.1 Circumstance for certificate re-key	6.	Certification service
4.7.2 Who may request certification of a new public key	6.	Certification service
4.7.3 Processing certificate re-keying requests	6.	Certification service
4.7.4 Notification of new certificate issuance to subscriber	6.	Certification service
4.7.5 Conduct constituting acceptance of a re-keyed certificate	6.	Certification service
4.7.6 Publication of the re-keyed certificate by the CA	6.	Certification service
4.7.7 Notification of certificate issuance by the CA to other entities	6.	Certification service
4.8 Certificate modification	6.	Certification service
4.8.1 Circumstance for certificate modification	6.	Certification service
4.8.2 Who may request certificate modification	6.	Certification service
4.8.3 Processing certificate modification requests	6.	Certification service
4.8.4 Notification of new certificate issuance to subscriber	6.	Certification service
4.8.5 Conduct constituting acceptance of modified certificate	6.	Certification service
4.8.6 Publication of the modified certificate by the CA	6.	Certification service
4.8.7 Notification of certificate issuance by the CA to other entities	6.	Certification service
4.9 Certificate revocation and suspension	6.	Certification service
4.9.1 Circumstances for revocation	6.	Certification service
4.9.2 Who can request revocation	6.	Certification service
4.9.3 Procedure for revocation request	6.	Certification service
4.9.4 Revocation request grace period	6.	Certification service

RFC 3647 outline	No	Cert.Policy Outline
4.9.5 Time within which CA must process the revocation request	6.	Certification service
4.9.6 Revocation checking requirement for relying parties	6.	Certification service
4.9.7 CRL issuance frequency (if applicable)	6.	Certification service
4.9.8 Maximum latency for CRLs (if applicable)	6.	Certification service
4.9.9 On-line revocation/status checking availability	6.	Certification service
4.9.10 On-line revocation checking requirements	6.	Certification service
4.9.11 Other forms of revocation advertisements available	6.	Certification service
4.9.12 Special requirements re key compromise	6.	Certification service
4.9.13 Circumstances for suspension	6.	Certification service
4.9.14 Who can request suspension	6.	Certification service
4.9.15 Procedure for suspension request	6.	Certification service
4.9.16 Limits on suspension period	6.	Certification service
4.10 Certificate status services	1.	Introduction
4.10.1 Operational characteristics	1.	Introduction
4.10.2 Service availability	3.2	OCSP Confirmation Response
4.10.3 Optional features	1.	Introduction
4.11 End of subscription	6.	Certification service
4.12 Key escrow and recovery	6.	Certification service
4.12.1 Key escrow and recovery policy and practices	6.	Certification service
4.12.2 Session key encapsulation and recovery policy and practices	6.	Certification service
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS (11)	1.	Introduction
5.1 Physical controls	1.	Introduction
5.1.1 Site location and construction	1.	Introduction
5.1.2 Physical access	1.	Introduction
5.1.3 Power and air conditioning	1.	Introduction
5.1.4 Water exposures	1.	Introduction
5.1.5 Fire prevention and protection	1.	Introduction
5.1.6 Media storage	1.	Introduction
5.1.7 Waste disposal	1.	Introduction
5.1.8 Off-site backup	1.	Introduction
5.2 Procedural controls	1.	Introduction
5.2.1 Trusted roles	1.	Introduction
5.2.2 Number of persons required per task	1.	Introduction
5.2.3 Identification and authentication for each role	1.	Introduction
5.2.4 Roles requiring separation of duties	1.	Introduction
5.3 Personnel controls	1.	Introduction
5.3.1 Qualifications, experience, and clearance requirements	1.	Introduction
5.3.2 Background check procedures	1.	Introduction
5.3.3 Training requirements	1.	Introduction
5.3.4 Retraining frequency and requirements	1.	Introduction
5.3.5 Job rotation frequency and sequence	1.	Introduction
5.3.6 Sanctions for unauthorized actions	1.	Introduction
5.3.7 Independent contractor requirements	1.	Introduction
5.3.8 Documentation supplied to personnel	1.	Introduction
5.4 Audit logging procedures	1.	Introduction
5.4.1 Types of events recorded	1.	Introduction

RFC 3647 outline	No	Cert.Policy Outline
5.4.2 Frequency of processing log	1.	Introduction
5.4.3 Retention period for audit log	1.	Introduction
5.4.4 Protection of audit log	1.	Introduction
5.4.5 Audit log backup procedures	1.	Introduction
5.4.6 Audit collection system (internal vs. external)	1.	Introduction
5.4.7 Notification to event-causing subject	1.	Introduction
5.4.8 Vulnerability assessments	1.	Introduction
5.5 Records archival	1.	Introduction
5.5.1 Types of records archived	1.	Introduction
5.5.2 Retention period for archive	1.	Introduction
5.5.3 Protection of archive	1.	Introduction
5.5.4 Archive backup procedures	1.	Introduction
5.5.5 Requirements for time-stamping of records	1.	Introduction
5.5.6 Archive collection system (internal or external)	1.	Introduction
5.5.7 Procedures to obtain and verify archive information	1.	Introduction
5.6 Key changeover	1.	Introduction
5.7 Compromise and disaster recovery	1.	Introduction
5.7.1 Incident and compromise handling procedures	1.	Introduction
5.7.2 Computing resources, software, and/or data are corrupted	1.	Introduction
5.7.3 Entity private key compromise procedures	1.	Introduction
5.7.4 Business continuity capabilities after a disaster	1.	Introduction
5.8 CA or RA termination	1.	Introduction
6. TECHNICAL SECURITY CONTROLS (11)	1.	Introduction
6.1 Key pair generation and installation	1.	Introduction
6.1.1 Key pair generation	1.	Introduction
6.1.2 Private key delivery to subscriber	1.	Introduction
6.1.3 Public key delivery to certificate issuer	1.	Introduction
6.1.4 CA public key delivery to relying parties	1.	Introduction
6.1.5 Key sizes	1.	Introduction
6.1.6 Public key parameters generation and quality checking	1.	Introduction
6.1.7 Key usage purposes (as per X.509 v3 key usage field)	1.	Introduction
6.2 Private Key Protection and Cryptographic Module Engineering Controls	1.	Introduction
6.2.1 Cryptographic module standards and controls	1.	Introduction
6.2.2 Private key (n out of m) multi-person control	1.	Introduction
6.2.3 Private key escrow	1.	Introduction
6.2.4 Private key backup	1.	Introduction
6.2.5 Private key archival	1.	Introduction
6.2.6 Private key transfer into or from a cryptographic module	1.	Introduction
6.2.7 Private key storage on cryptographic module	1.	Introduction
6.2.8 Method of activating private key	1.	Introduction
6.2.9 Method of deactivating private key	1.	Introduction
6.2.10 Method of destroying private key	1.	Introduction
6.2.11 Cryptographic Module Rating	1.	Introduction
6.3 Other aspects of key pair management	1.	Introduction
6.3.1 Public key archival	1.	Introduction

RFC 3647 outline	No	Cert.Policy Outline
6.3.2 Certificate operational periods and key pair usage periods	1.	Introduction
6.4 Activation data	1.	Introduction
6.4.1 Activation data generation and installation	1.	Introduction
6.4.2 Activation data protection	1.	Introduction
6.4.3 Other aspects of activation data	1.	Introduction
6.5 Computer security controls	1.	Introduction
6.5.1 Specific computer security technical requirements	1.	Introduction
6.5.2 Computer security rating	1.	Introduction
6.6 Life cycle technical controls	1.	Introduction
6.6.1 System development controls	1.	Introduction
6.6.2 Security management controls	1.	Introduction
6.6.3 Life cycle security controls	1.	Introduction
6.7 Network security controls	1.	Introduction
6.8 Time-stamping	3.1	Time Stamps
7. CERTIFICATE, CRL, AND OCSP PROFILES	2.	Certificates
7.1 Certificate profile	2.	Certificates
7.1.1 Version number(s)	2.	Certificates
7.1.2 Certificate extensions	2.	Certificates
7.1.3 Algorithm object identifiers	2.	Certificates
7.1.4 Name forms	2.	Certificates
7.1.5 Name constraints	2.	Certificates
7.1.6 Certificate policy object identifier	2.	Certificates
7.1.7 Usage of Policy Constraints extension	2.	Certificates
7.1.8 Policy qualifiers syntax and semantics	2.	Certificates
7.1.9 Processing semantics for the critical Certificate Policies extension	2.	Certificates
7.2 CRL profile	1.	Introduction
7.2.1 Version number(s)	1.	Introduction
7.2.2 CRL and CRL entry extensions	1.	Introduction
7.3 OCSP profile	1.	Introduction
7.3.1 Version number(s)	1.	Introduction
7.3.2 OCSP extensions	1.	Introduction
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	1.	Introduction
8.1 Frequency or circumstances of assessment	1.	Introduction
8.2 Identity/qualifications of assessor	1.	Introduction
8.3 Assessor's relationship to assessed entity	1.	Introduction
8.4 Topics covered by assessment	1.	Introduction
8.5 Actions taken as a result of deficiency	1.	Introduction
8.6 Communication of results	1.	Introduction
9. OTHER BUSINESS AND LEGAL MATTERS	1.	Introduction
9.1 Fees	10.	Taxes
9.1.1 Certificate issuance or renewal fees	10.	Taxes
9.1.2 Certificate access fees	10.	Taxes
9.1.3 Revocation or status information access fees	10.	Taxes
9.1.4 Fees for other services	10.	Taxes
9.1.5 Refund policy	10.	Taxes

RFC 3647 outline	No	Cert.Policy Outline
9.2 Financial responsibility	1.	Introduction
9.2.1 Insurance coverage	1.	Introduction
9.2.2 Other assets	1.	Introduction
9.2.3 Insurance or warranty coverage for end-entities	1.	Introduction
9.3 Confidentiality of business information	1.	Introduction
9.3.1 Scope of confidential information	1.	Introduction
9.3.2 Information not within the scope of confidential information	1.	Introduction
9.3.3 Responsibility to protect confidential information	1.	Introduction
9.4 Privacy of personal information	1.	Introduction
9.4.1 Privacy plan	1.	Introduction
9.4.2 Information treated as private	1.	Introduction
9.4.3 Information not deemed private	1.	Introduction
9.4.4 Responsibility to protect private information	1.	Introduction
9.4.5 Notice and consent to use private information	1.	Introduction
9.4.6 Disclosure pursuant to judicial or administrative process	1.	Introduction
9.4.7 Other information disclosure circumstances	1.	Introduction
9.5 Intellectual property rights	1.	Introduction
9.6 Representations and warranties	4.	Warranties provided by certSIGN
9.6.1 CA representations and warranties	4.	Warranties provided by certSIGN
9.6.2 RA representations and warranties	4.	Warranties provided by certSIGN
9.6.3 Subscriber representations and warranties	4.	Warranties provided by certSIGN
9.6.4 Relying party representations and warranties	4.	Warranties provided by certSIGN
9.6.5 Representations and warranties of other participants	4.	Warranties provided by certSIGN
9.7 Disclaimers of warranties	4.	Warranties provided by certSIGN
9.8 Limitations of liability	1.	Introduction
9.9 Indemnities	1.	Introduction
9.10 Term and termination	1.	Introduction
9.10.1 Term	1.	Introduction
9.10.2 Termination	1.	Introduction
9.10.3 Effect of termination and survival	1.	Introduction
9.11 Individual notices and communications with participants	1.	Introduction
9.12 Amendments	1.	Introduction
9.12.1 Procedure for amendment	1.	Introduction
9.12.2 Notification mechanism and period	1.	Introduction
9.12.3 Circumstances under which OID must be changed	1.	Introduction
9.13 Dispute resolution provisions	1.	Introduction
9.14 Governing law	1.	Introduction
9.15 Compliance with applicable law	1.	Introduction
9.16 Miscellaneous provisions	1.	Introduction
9.16.1 Entire agreement	1.	Introduction
9.16.2 Assignment	1.	Introduction
9.16.3 Severability	1.	Introduction
9.16.4 Enforcement (attorneys' fees and waiver of rights)	1.	Introduction
9.16.5 Force Majeure	1.	Introduction
9.17 Other provisions	1.	Introduction