Certificate Policy for 1* server authentication certificates

ChamberSign France CA

-

ChamberSign France

Purpose of the document	This document is related to the hierarchy of certification authorities ChamberSign France "ChamberSign France CA”. It is the certificate policy for server authentication certificates attached to this hierarchy, for certificates corresponding to the French general security referential (GSR) 1* level.
Version	00
Date of release	
Diffusion	Public

Written by	Technical Manager ChamberSign
Verified by	Quality Manager ChamberSign
Approved by	General Manager ChamberSign

List of diffusion
Functions
Public

Record of versions	
Version	Nature of the evolutions
00	Creation

TABLE OF CONTENT

Warning

This document is protected by the French Code of Intellectual Property of 1st July 1992, including those relating to literary and artistic property and copyrights, as well as all applicable international conventions. These rights are the exclusive property of ChamberSign France. The reproduction, representation (including the publication and distribution), in whole or in part, by any means (including electronic, mechanical, optical, photocopying, computer), not previously authorized in writing by ChamberSign France or assigns, is strictly prohibited.

The Intellectual Property Code authorizes, pursuant to Article L.122-5, first, that "copies or reproductions strictly reserved for private use and not intended for use commu e "and, secondly, that the analysis and short quotations for the purposes of example and illustration," any representation or reproduction in whole or in part without the consent of the author or his successors or assigns is prohibited "(Article L.122-4 of the Code of Intellectual Property).

This representation or reproduction, by any means whatsoever, constitutes an infringement punishable by articles L. including 335-2 of the Intellectual Property Code.

This document, property of ChamberSign France, may be granted by licensing all private or public entities who wish to use as part of their certification services.

This English version is a translation of the French version for information only. The only applicable version of this document is the official French version.

1. INTRODUCTION

1.1. Overview

This document is related to the Public Key Infrastructure (PKI) ChamberSign France (CSF), PKI responsible for managing certificates in the hierarchy "AC ChamberSign France" (called “PKI” in the rest of this document).

It is the Certificate Policies (CP) of the PKI covering server authentication certificates, in conformity with the level * of the general security referential (cf. [RGS][1]).

Its structure is consistent with the document [RFC3647].

The objective of this document is to define the commitments of CSF through the PKI, in issuing and managing certificates for the type mentioned above, throughout their life cycle.

This policies are the foundation of the PKI relations with the outside users (certificate holders and relying parties), but also partners (other PKI which CSF wishes to recognize and from which it wishes to be recognized), public authorities and private assessment and qualification organizations.

However, given the complexity of the elements of both technical and legal content in a certificate policy, especially for non-specialist users, these policies are translated into specific documents for users that are the terms of use. These terms of use correspond to the PKI Disclosure Statement described in [RFC3647].

The commitments agreed in these CP are:

- the requirements imposed by regulations to CSF;
- the objectives set to itself by CSF, regarding the services, the security, the quality and the performance, in order to satisfy the users of its certificates, and be recognized, if necessary, by different patterns of PKI assessment / qualification.

These CP, like other CP from CSF, are public documents. The Certification Practice Statement (CPS) for these CP is a document freely available upon request from CSF. Other documents resulting from this CP and CPS are internal documents to CSF that can be accessed, if necessary, through a confidentiality agreement (external auditors, qualifying bodies, public authorities, etc..).

1.2. Document name and identification

The object identifier (OID) for these CP are:

CA Certificate : ChamberSign France Seal 1 *	
Certificate policy	
Authentication	1.2.250.1.96.1.7.4.1.1

{iso(1) member-body(2) france (250) type-org(1) chambersign (96) Arborescence AC ChamberSign France (1) AC Chambersign RGS LCR directe (7) Seal 1* (4) Authentication (1) PC Version (1)}

[1] See Appendix 1 for the list of references.

1.3. PKI participants

It is distinguished between external stakeholders[2] to the PKI and internal stakeholders[3], which are under the responsibility of CSF towards external stakeholders.

Internal stakeholders are described in the certification practice statement (CPS) associated with these CP. These stakeholders realize the implementation of the following functions:

- Registering function -This function checks the credentials of the future responsible for the server authentication certificate (RCAS) and for the IT server on which the certificate must be attached, and possibly other specific attributes before forwarding the corresponding certificate request to the certificate generation function. This function is also in charge, when necessary, of the re-verification of RCAS and / or IT server upon renewal of its certificate.
- Certificate generation function - This function generates certificates (creation of the format, electronic signature with the private key of the CA) based on the information transmitted by the registering function, including the public key of the server.
- Generation function of the secret elements of the server – The PKI generates under the exclusive control of the RCAS secret elements for the service (private key and activation code of the private key).
- Delivery to the RCAS function - This function delivers to the RCAS the relevant certificate(s) and the activation code of the server certificate.
- Publishing function – This function provides to the various concerned parties, the terms and conditions, policies and practices published by the PKI, the CA certificates and other relevant information for the RCAS and / or users of certificates, excluding information about Certificate Status. It also provides certificates of servers that are valid.
- Revocation Management function - This function handles revocation requests (including identification and authentication of the applicant) and determines actions to be taken. The results are disseminated via the certificate status information function.
- Certificate status information function - This function provides relying parties with information on certificate status (revoked, suspended, etc.). This function is implemented as a way of publishing information updates at regular intervals (CRL, ARL).

External stakeholders are:

- Responsible for the server authentication certificate (RCAS) – The physical person responsible for the server authentication certificate, including for the use of this certificate and for the relevant key pair, on behalf of the entity whose depends the IT server identified in the certificate.
- Legal Representative - This is a legal representative of the entity identified in the certificate and to which the RCAS is attached.
- Relying parties / Certificates Users - A certificate user is an individual or a technical entity (computer application, network equipment, ...) which relies on a certificate subject of this CP to check an authentication value coming from server on which the certificate is attached.
- Audit / Qualification / Referencing entities - These entities are brought to audit all or part of the PKI, at the request of a CSF customer, CSF itself (to obtain a qualification or a label), or at the request of public authorities.
- Public authorities - This is administrative or governmental entities that can be brought, in accordance with applicable laws and regulations, to have access to all or part of systems and information of the PKI.

[2] External stakeholders are entities that are not involved in the operation of the PKI but have to interact with the PKI.

[3] Internal stakeholders in the PKI are the entities involved in the operation of the PKI and that can be either directly internal to CSF or external to CSF with a contractual relationship with CSF.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

CP	Uses
[Authentication]	Uses are the servers authentication in the frame of the etablishment of secured sessions, type SSL/TLS.

Nota : Authentication isn't a signature in the legal sense of the word because it doesn't mean that the organisation manifests his consent on the exchanged data (the guarantee of non-repudiation isn't assured).

Furthermore, CSF may be required to issue test certificates. These test certificates are identified as such in their DN. They are not covered by any warranty by CSF and they should never be used for purposes other than testing purposes.

1.4.2. Prohibited certificate uses

Any use of a certificate other than those provided under these CP and the terms of use (see [PRO.ACC.42]) is prohibited. In case of non compliance with this prohibition, the responsibility of CSF can not be held.

1.5. Policy administration

1.5.1. Organization administering the document

CSF, as a provider of certification services, is responsible for the management of these CP. The evolutionary and amendments process to these CP is specified in chapter 9.12 below.

1.5.2. Contact person

Any questions or comments about these CP can be sent by email to the following address: qualite@chambersign.fr

1.5.3. Person determining CPS suitability for the policy

Determining that a CPS does or does not meet the requirements of these CP is made by the Directorate of CSF.

1.5.4. CPS approval procedures

The approval procedure that a CPS is compliant is identified in the concerned CPS.

1.6. Definitions and acronyms

1.6.1. Acronyms

Note – The French acronym is between ().

A

CA (AC)	Certification Authority
ANSSI	National Security Agency Information Systems

C

CC	Common Criteria
CCI	Chamber of Commerce and Industry
ToU (CGU)	Terms of Use
CODIR	Management Committee of ChamberSign
CSF	ChamberSign France

D

CPS (DPC)	Certification Practice Statement

I

PKI (IGC)	Public Key Infrastructure

L

ARL (LAR)	Authority Revocation List
CRL (LCR)	Certificate Revocation List

O

OID	Object Identifier

P

CP (PC)	Certification Policy
PIN	Personnal Identification Number
PP	Protection Profile
PECS (PSCE)	Provider of Electronic Certification Services

R

RCAS	Responsible for the server authentication certificate
LR (RL)	Legal Representative
RSA	Rivest Shamir Adelman

U

URL	Uniform Resource Locator

1.6.2. Definitions

Note – The French word is between ().

A

Certification Authority (Autorité de Certification)

Within a PECS, a Certification Authority is responsible, on behalf and under the responsibility of the PECS, of applying at least one certificate policy and is identified as such, as issuer ("issuer" field in the certificate), in the certificates issued under this certificate policy.

Root Certification Authority (Autorité de Certification Racine)
A CA which is a reference within a user community (including other CAs). It is an essential element of trust which may be granted to it in a given context.

B

Key pair (Bi-clé)
Pair composed of a private key (to be kept secret) and a corresponding public key, required for the implementation of a provision of cryptography based on asymmetric algorithms.

C

Certificate (Certificat)
Set of user's information, including the public key, made unforgeable by the encipherment, with the secret key of the CA that issued it, of a condensate calculated on all of this information. A certificate contains information such as:

- the identity of the server;
- the public key of the server;
- authorized use(s) of the key;
- the validity period of the certificate;
- the identity of the CA that issued it;
- signature of the CA that issued it.

A standard certificate format is defined in Recommendation X.509 v3.

Compliance monitoring (Contrôle de conformité)
Action which is a review as complete as possible to ensure the strict application of procedures and regulations within an organization.

D

Certification Practice Statement (CPS)
A CPS identifies the practices (organization, operational procedures, technical and human resources) that the AC applies through the provision of its electronic certification services to users, in order to meet the certificate policie(s) it has enacted.

Activation data (Données d'activation)
Private data associated with a server to implement its private key.

E

Recording (Enregistrement)
Action by which an authority validates a certificate request, in conformity with a certification policy.

G

Generation of a certificate (Génération)
Action by which a CA integrates the elements of a certificate, controls and signs the certificate.

I

Public Key Infrastructure (Infrastructure de Gestion de Clés)
Set of components, functions and procedures dedicated to the management of cryptographic keys and certificates used within trusted services. A PKI may consist of a certification authority, certification operator, centralized and / or local registration authority operators, certification agents, an entity for archiving, an entity for publication, etc.

J

Logging (Journalisation)
Action to record in a file devoted to this purpose certain types of events from an application or operating system of a computer system. The resulting file facilitates tracking and accountability of operations.

P

Certificate Policy (Politique de Certification)
Set of rules, identified by a name (OID), defining the requirements that an AC states to comply with, in the development and delivery of its services and indicating the applicability of a certificate to a particular community and / or to a class of applications with common security requirements. A CP can also, if necessary, identify the requirements and obligations on other stakeholders, including RCAS and users of certificates.

Provider of Electronic Certification Services (Prestataire de Services de Certification Electronique)
Any person or entity that is responsible for managing digital certificates throughout their life cycle, to RCAS and users of these certificates. A PECS can provide different types of certificates corresponding to different purposes and / or different security levels. A PECS has at least one CA but may have several, depending on its organization. The different CA of a PECS can be independent of each other and / or connected by hierarchical links or other (Roots CA / Sub CA). A PECS is identified in a certificate under its responsibility through its CA that issued this certificate and which is itself directly identified in the filed "issuer" of the certificate.

Publication of a certificate (Publication d’un certificat)
Action to register a certificate in a directory, available to users which may have to verify a signature or to encrypt information.

R

Certificate Renewal (Renouvellement de certificat)
Action performed at the request of a user or at the end of the period of validity of a certificate which is to generate a new certificate for a server.

Responsible for the server authentication certificate (Responsable du Certificat d’Authentification serveur)
See chapter 1.3.

Revocation of certificate (Révocation d’un certificat)
Action requested by an authorized entity (CA, RCAS, etc.) and from which the result is the removal of the guarantee of the CA on a particular certificate before the end of its period of validity. This action may result from different types of events such as a key compromise, modification of information contained in the certificate, etc.

S

Publication Service (Service de publication)
The Publication Service makes available public key certificates issued by a CA, to all potential users of these certificates. It publishes a list of certificates recognized as valid and a certificate revocation list (CRL). This service can be rendered by a directory (for example of X.500 type), an information server (Web), a grant from hand to hand, a messaging application, etc.

U

End User (Utilisateur final)
Any entity (natural person or legal person) receiving a certificate and relying on it to check a seal value coming from the server which the certificate is attached.

V

Certificate verification (Vérification de certificat)
The procedure for verifying a certificate consists of a set of operations to ensure that the information contained in the certificate has been validated by a trusted CA. The verification of a certificate includes the verification of its validity, its status (revoked or not), and the signature of the generating CA.

Signature verification
Verification of a signature is to decrypt the signature of a message, by implementing the public key of the purported signer. If the decrypt signature is just the same as the footprint calculated from the received message, then it is guaranteed that the message is intact and that it was signed by the holder of the private key corresponding to the public key used for verification.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

For the provision of information to be published to the RCAS and certificates users, CSF implements in its PKI a publication service and a service on certificate status.

The publication service is supported by a web server, available at HTTP www.chambersign.fr.

The service on certificate status is based on generating CRL and their publication on the website.

The commitments of availability and business continuity of these services (web server and CRL issuer) are detailed in Chapter 4.9 below.

2.2. Publication of certification information

The following information is disseminated via the CSF website:

- these CP;
- the terms of use (ToU);
- formats of certificates and CRLs object of these CP;
- CRLs;
- CA certificates.

2.3. Time or frequency of publication

Information related to the PKI (CP, ToU...) are published as soon as validated by the management of CSF.

The availability of systems publishing this information is provided during weekdays. System availability publishing CA certificates is provided 24h/24 and 7/7.

2.4. Access controls on repositories

The modification access to publishing systems (addition, deletion, modification of published information) is strictly limited to authorized internal function of the PKI, through a strong access control (authentication based on at least two factors).

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

The names used in certificates issued by CSF are as specified in X.500 and [RGS].
In each certificate, the "issuer" (issuing CA) and the "subject" (IT server) correspond to a Distinguished Name (DN).
The content of the DN is defined in the document describing the certificate profiles [GUI.ACC.11].

3.1.2. Need for names to be meaningful

The names used in the fields "issuer" and "subject" of a server authentication certificate are explicit in the field of certification of CSF (use of national identifiers structure SIREN / SIRET, use of official and complete names of entities, ...).

3.1.3. Anonymity or pseudonymity of servers

As part of this certification policy, there is no anonymity, or pseudonyms.

3.1.4. Rules for interpreting various name forms

The meanings of the different fields of DN, both of the "issuer" as the "subject", are described in [GUI.ACC.11].

3.1.5. Uniqueness of names

Product in each certificate, the DN field of "issuer" (issuing CA) and the 'subject' field (CA or server) is unique in the field of certification of CSF (see [GUI.ACC.11]).

3.1.6. Recognition, authentication, and role of trademarks

There is no use in a certificate of brand name other than the name of the corresponding body, as noted on official documents subject to verification during registration procedures (Kbis, ...).

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

Files application for a certificate containing the public key being certified, sealed with the corresponding private key.

3.2.2. Authentication of organization identity

Information regarding the structure on which the RCAS is attached are subject to verification upon registration (existence, validity, ...).

3.2.3. Authentication of individual identity

The identity of the RCAS is verified through the verification of official identity documents made whose a copy certified as conforming by the RCAS is forwarded by mail.
In the case of a RCAS change during the validity of a server authentication certificate, the new RCAS is recorded in its current form by the CA as a replacement for the old RCAS.
The identification of the new RCAS (natural person) representing an entity needs the identification of the natural person and the verification of his authorization as representative of the entity on which the server is attached and as RCAS for this server.
The holder given by the whois must be equivalent to the name of the entity (enterprise or administration) asking the certificate.

3.2.4. Non-verified RCAS and / or IT server information

All information concerning RCAS in these certificates is checked.

3.2.5. Validation of authority

This step is performed at the same time as the validation of the identity of the organism.

3.2.6. CA cross certification

The decision of the PKI recognizes CSF and / or be recognized by another PKI is the responsibility of the Board of CSF.

3.3. Identification and authentication for re-key requests

The first renewal is done online if prior to the expiration date of the certificate to be renewed. The RCAS validates online that information related to certificate renewal are always accurate. The next renewal is made after the initial registration process.

Renewal after revocation is made after the initial registration process.

3.4. Identification and authentication for revocation request

Any request for revocation is the subject of an applicant's authentication and verification of his authority to such a request.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Applications for licenses come either directly from the future RCAS, or the legal representative of the entity concerned.

4.1.2. Enrollment process and responsibilities

The establishment of a certificate request is the responsibility of the entity to which the future RCAS.

4.2. Certificate application processing

The registration of the PKI verifies the origin, integrity and consistency of the request received (see section 3.2).
Then, if no problems are detected, it formats and sends the request to the generation of certificates.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

Following validation of the application for a certificate by the recording function of the PKI, the process is to remit to the RCAS the certified public key: key pair generation under the control and under the supervision of the RCAS, in a support cryptographic (equipment or software) choose by the RCAS (in condition to respect requirements defined at the §6.2 below), sends the public key to the function of generating certificates, download the generated certificate holder.

4.3.2. Notification to RCAS by the CA of issuance of certificate

The URL enabling to download the certificate is sent to the RCAS.

4.4. *Certificate acceptance*

4.4.1. Conduct constituting certificate acceptance

The certificate is subject to an explicit acceptance by the RCAS after the download.

4.4.2. Publication of the certificate by the CA

Certificates subject of these CP are not subject to publication by CSF.

4.4.3. Notification of certificate issuance by the CA to other entities

The different components of the PKI concerned are informed of the issuance of the certificate via the information system of the PKI.

4.5. *Key pair and certificate usage*

4.5.1. RCAS private key and certificate usage

Using the private key and associated certificate is limited to conditions of use specified in these CP (see § 1.4) and in accordance with this use, as described in the certificate content (key attribute and/or use extended key usage, cf. [GUI.ACC.11]).

The use of the key pair and associated certificate are indicated in the certificate itself, via extensions concerning key uses.

The use of a private key is only allowed during the period of validity of the certificate and associate you accept the terms of use by the RCAS.

4.5.2. Relying party public key and certificate usage by the certificate user

Using the certificate and the public key is limited to conditions of use specified in these CP (see § 1.4) and the intended use specified in the certificate (attribute key usage and extended key usage, see [GUI.ACC.11]).

The user is bound to verify the validity and compliance of its use.

Responsibility of CSF can not be committed for use does not meet conditions of use.

4.6. *Certificate renewal*

Recertification without renewal of the corresponding key pair is impossible. A renewal application is therefore accompanied necessarily generating a new key pair (see section 4.7 below). This chapter is not applicable.

4.7. *Certificate re-key*

4.7.1. Circumstance for certificate re-key

The main cause for issuing a new certificate and key pair corresponding to the arrival date of expiry of the certificate. The duration of validity of CSF is 3 years. The key pairs must be renewed periodically because to minimize the risk of cryptographic attack.

Renewals may also be made in advance, following an event or incident reported by the carrier, the most frequent being the loss, theft or malfunctioning of the cryptographic support.

Modification of the information contained in the certificate also entails issuing a new certificate (with renewal of the key pair).

Issuing a new certificate is performed identically to the process of initial issuance. Only the registration phase may differ for a renewal (see section 3.3).

4.7.2. Who may request certification of a new public key

See sections 4.1 to 4.4.

4.7.3. Processing certificate re-keying requests

See sections 4.1 to 4.4.

4.7.4. Notification of new certificate issuance to RCAS

See sections 4.1 to 4.4.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

See sections 4.1 to 4.4.

4.7.6. Publication of the re-keyed certificate by the CA

See sections 4.1 to 4.4.

4.7.7. Notification of certificate issuance by the CA to other entities

See sections 4.1 to 4.4.

4.8. Certificate modification

The amendment of a certificate shall result in the renewal of the certificate and corresponding key pair: cf. Chapter 4.7. A modification is prohibited without renewal.

4.9. Certificate revocation and suspension

There is no possible suspension of certificate. Only the final revocation of certificates can be achieved.

4.9.1. Circumstances for revocation

The following circumstances may cause the revocation of a certificate subject of these CP:

- the private key of the server is lost, stolen, inoperable (malfunction of the substrate), compromised or suspected compromise (option of the RCAS itself);
- server information contained in the certificate are no longer valid or more consistent with the intended use of the certificate, this before the normal expiration of the certificate;
- it was shown that the RCAS has not complied with the applicable terms of use of the certificate;
- the CA certificate is revoked (which will revoke certificates signed by the corresponding private key);
- the definitive stop of the server or the cessation of activity of the RCAS entity.

The revocation proceedings are never published.

4.9.2. Who can request revocation

Persons and entities that can request the revocation of a certificate subject of these are:

- the RCAS for the considered server;
- the entity on which the RCAS depends;
- CSF.

4.9.3. Procedure for revocation request

The request validation includes checking the origin of the application and applicability of the cause invoked. After this validation, service management revocations formats and forwards the request to state service charge certificates to add the serial number of certificates to be revoked in the next CRL to generate and publish.

4.9.4. Revocation request grace period

The revocation request must be made from knowledge of the corresponding event.

4.9.5. Time within which CA must process the revocation request

Revocation requests are processed within 72 hours (maximum time) of receipt of the request, during working hours, excluding dismissals resulting from change requests data from the carrier.

The management function of revocations is available 24 hours on 24, 7 days on 7. The maximum duration of downtime per interruption (outage or maintenance) of the management function of revocations is 2h (working days). The maximum total duration of downtime per month of the management function is revocation of 16h (working days).

4.9.6. Revocation checking requirement for certificates users

Certificates users must verify non-revocation of licenses on which they will base their confidence. This verification is done by consulting CRLs available through the website of CSF.

4.9.7. CRL issuance frequency (if applicable)

The state service certificates publishes an update of CRL at least every three days. Each CRL contains the date and time looking for CRL issuance next. For safety, the LCR have a duration of 72 hours.

4.9.8. Maximum latency for CRLs (if applicable)

The maximum period of a CRL publication after its generation is 30 minutes.

4.9.9. On-line revocation/status checking availability

A system for online verification (OCSP) isn’t implemented.

4.9.10. On-line revocation checking requirements by certificates users

See section 4.9.6.

4.9.11. Other forms of revocation advertisements available

N / A (only the mechanism of CRL is used).

4.9.12. Special requirements re key compromise

There are no special measures concerning the private keys of the server authentication certificates, other than revocation of certificates.

4.9.13. Circumstances for suspension

Certificates can be removed only for good. It is not envisaged possibility of temporary revocation (suspension).

4.9.14. Who can request suspension

N/A.

4.9.15. Procedure for suspension request

N/A.

4.9.16. Limits on suspension period

N/A.

4.10. Certificate status services

4.10.1. Operational characteristics

CRLs are made available freely and for free via the web site of CSF. Similarly, the OCSP service is freely accessible and free.

4.10.2. Service availability

The service is available 24 hours / 24 and 7 days /7 via the website CSF.
The maximum duration of downtime per interruption (outage or maintenance) of the function information certificate status is 4 hours (working days).

The maximum total duration of downtime per month depending on the information on the status of certificates is 32 hours (working days).

4.10.3. Optional features

N/A.

4.11. End of subscription

In case of end of contractual / hierarchical / regulatory subscription between the CA and the entity on which the server is attached before the end of certificate validity, for a reason or for another, the certificate must be revoked. Moreover, the CA must revoke a server authentication certificate for which there is not anymore an identified RCAS.

4.12. Key escrow and recovery

N / A (private key object of these CP are not subject to any receivership).

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

CSF implements physical security measures, within the various components of the PKI, necessary to ensure the safe operation of its services according to commitments made in this document, particularly in terms of availability (physical access control, support services (power, cooling, ...), protection against water damage, protection against fire and protection of media).

5.2. Procedural controls

Within each component of the PKI, functional roles of trust are identified and formally assigned, observing strict rules of separation of powers.
Any allocation of roles and associated rights is subject to prior verification of the identity and permissions.
For conducting operations, the involvement of several persons may be required.

5.3. Personnel controls

All personnel, internal and external CSF, have to work within the PKI components are subject to obligations of qualifications, skills, training and retraining and clearances based on their roles.
The honesty of such personnel shall be tested according to what is permitted by law.

5.4. Audit logging procedures

The various events related to the operation of the PKI are subject to a log of events recorded manually or automatically. The resulting files, paper or electronic form, provides for traceability and accountability of operations.
These event logs are dated, protected and are the subject of an archive. They are regularly monitored to assess potential vulnerabilities imposed on the PKI.

5.5. Records archival

Provisions for archiving, paper and electronic, are taken to ensure the sustainability of newspapers made by the various components of the PKI and other data (registration dossier, CP, DCP, certificates and CRLs issued , ...).
The retention periods are specified in the archive [PRO.ACC.42].

5.6. Key changeover

The CA can not generate a certificate, the end date is later than the expiration date of the corresponding certificate of the CA. Why the period of validity of the CA certificate is greater than that of the certificates it signs.

5.7. Compromise and disaster recovery

Each entity operating a component of TGI implements procedures and means of reporting and incident handling, particularly through awareness and training of its staff and through the analysis of individual logs events, including in the event of major incidents (private key compromise, weakness of the algorithms, ...). These procedures and means must be chosen to minimize damage from security incidents and malfunctions.

Each component of the PKI has a business continuity plan to meet the availability requirements of the various functions of the PKI from the commitments of CSF in these CP particularly with regard to functions related to the publication and certificate revocation.

The different components of the PKI have the necessary means to ensure the continuity of their business in compliance with the commitments of these CP.

5.8. CA or RA termination

One or more components of the PKI, or all of the PKI, may have to retire or transfer to another entity for various reasons.
CSF will implement the measures required to achieve at least the continuity of archiving information and continuity of revocation services.
CSF has made arrangements to cover the costs for meeting these minimum requirements in case CSF would be bankrupt or for other reasons is unable to cover these costs by itself, this, as much as possible, depending on constraints of the legislation applicable in bankruptcy.
To the extent that the proposed changes may affect the commitments regarding to RCAS or users of certificates, CSF will advise as soon as necessary and, at least, under the period of one month. Similarly, CSF informs the public authorities concerned.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

The key pairs of servers are generated in the RCAS cryptographic media under the control and the supervision of themselves. The public keys to certify are transmitted to the PKI protected so as to guarantee the origin and to ensure its integrity.
The root certificate of the PKI is downloaded from the website ChamberSign.
The user can check the fingerprint of the root certificate on the secure site https://www.keymanagement.chambersign.fr CSF or contact by phone.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Each RCAS could freely choose his cryptographic media. This media must however comply with requirements of [RGS] for the level * (cf. Requirements for private keys protection of servers device). The RCAS makes a contractual commitment with CSF for this compliance.
Private keys of servers are not subject to any receivership and no backup from CSF.

6.3. Other aspects of key pair management

Public keys of servers are archived carriers as part of the archiving of certificates.
The key pairs and certificates of servers have a lifespan of three years.

6.4. Activation data

The CP doesn't state no requirement, the key pair being implemented by the RCAS themselves and under their entire responsibility.

6.5. Computer security controls

Within the various components of the PKI, the security measures relating to computer systems meet the security objectives that result from risk analysis conducted in each component.

6.6. Life cycle technical controls

Implementing a system to implement the components of the PKI is documented. System components of the PKI and any changes and upgrades are documented and controlled.
The security objectives are defined in the phases of specification and design. Systems and products used are reliable and are protected against modification.

6.7. Network security controls

The interconnection to public networks is protected by security gateways configured to accept only the protocols necessary for the operation of the component within the PKI. The components of the local area network (routers, for example) are kept in a physically secure environment and that the configurations are periodically audited to verify compliance with the requirements specified by CSF.

6.8. Time-stamping / Dating system

The dating of events in the PKI uses the system time of the PKI by providing clock synchronization systems TGI them, at least to the nearest minute, and from a reliable source of time UTC, at least to the nearest second. For transactions made offline (eg administration of a CA Root), the synchronization accuracy relative to UTC time is not required. The system may order the events with sufficient accuracy.

7. CERTIFICATE, CRL, AND OCSP PROFILES

The profiles of certificates, CRLs are defined in [GUI.ACC.11].

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This chapter deals only with audits and evaluation of CSF responsibility to ensure the proper functioning of the PKI and does not address qualification audits governed by legal regulations.

8.1. Frequency or circumstances of assessment

Before the first use of a component of the PKI or following any significant change in a component, CSF performs a check of this component. CSF also conducts regular compliance monitoring of its entire PKI, at least once three years.

8.2. Identity/qualifications of assessor

The control component is assigned to a team of CSF competent auditors in security and information systems in the field of activity of the controlled component.

8.3. Assessor's relationship to assessed entity

The audit team may not belong to the entity operating the controlled component of the PKI, whatever that component, and is duly authorized to perform the checks required.

8.4. Topics covered by assessment

Compliance checks involve a component of the PKI (spot checks) or the whole architecture of the PKI (periodic checks) and are designed to verify compliance with the commitments and practices defined in these CP and in responds that the CPD as well as elements thereunder (operational procedures, resources used, etc..).

8.5. Actions taken as a result of deficiency

Following a compliance check, the audit team travels to CSF of the following notice: "success", "failure", "TBC". CSF takes, and caught, the necessary measures according to the conclusions of the examination.

8.6. Communication of results

The results of compliance audits are made available to the qualification body in charge of the qualification of CSF.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate issuance or renewal fees

See [PRO.ACC.42] and the pricing policy of CSF.

9.1.2. Certificate access fees

N/A.

9.1.3. Revocation or status information access fees

Access to status information of certificates is free.

9.1.4. Fees for other services

See [PRO.ACC.42] and the pricing policy of CSF.

9.1.5. Refund policy

N/A.

9.2. Financial responsibility

9.2.1. Insurance coverage

See [PRO.ACC.42].

9.2.2. Other assets

See [PRO.ACC.42].

9.2.3. Insurance or warranty coverage for end-entities

See [PRO.ACC.42].

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

The following information is considered as confidential and is subject to adequate protection procedures:

- the non-public of the CPD of CA,
- the private keys of CA, components and servers,
- activation data associated with the private keys of CA and servers,
- all the secrets of the PKI,
- event logs of the components of the PKI,
- the registration records of RCAS,
- the causes of revocation, unless explicitly granted the RCAS.

9.3.2. Information not within the scope of confidential information

N/A.

9.3.3. Responsibility to protect confidential information

Confidential information is not accessible (eg, servers private keys are accessible only to people justifying the need to know and properly authorized (eg, parts of "secrets PKI").

9.4. Privacy of personal information

9.4.1. Privacy plan

The personal information is explicitly identified and procedures are subject to adequate protection, in compliance with applicable legal and regulatory requirements.
See [PRO.ACC.42].

9.4.2. Information treated as private

All registration data of RCAS are considered as personal.

9.4.3. Information not deemed private

N/A.

9.4.4. Responsibility to protect private information

See laws and regulations. On French territory, including statements see processing of personal data are doing with the CNIL.

9.4.5. Notice and consent to use private information

Accordance with national laws and regulations, particularly on French territory, the personal information submitted by RCAS to CSF are neither disclosed nor transferred to third parties except in the following cases: prior consent of the RCAS, court order or other legal authority.

9.4.6. Disclosure pursuant to judicial or administrative process

See laws and regulations.

9.4.7. Other information disclosure circumstances

N/A.

9.5. Intellectual property rights

See [PRO.ACC.42].

9.6. Representations and warranties

9.6.1. CA

Under these CP, and the area they cover (see sections 1.3 and 1.4 above), CSF ensures compliance with the commitments described in this document and in [PRO.ACC.42].

9.6.2. Recording service

See section 9.6.1.

9.6.3. RCC

See [PRO.ACC.42].

9.6.4. Certificate users

See [PRO.ACC.42].

9.6.5. Other participants

See [PRO.ACC.42].

9.7. Disclaimers of warranties

See [PRO.ACC.42].

9.8. Limitations of liability

See [PRO.ACC.42].

9.9. Indemnities

See [PRO.ACC.42].

9.10. Term and termination

9.10.1. Term

Each of these CP applies until the end of life of the last certificate issued under the considered CP.

9.10.2. Termination

Cessation of activity of the PKI, scheduled or following a disaster, the end result of validity of these CP.

9.10.3. Effect of termination and survival

The expiry of these CP cancels the commitments of CSF that are worn, with the exception of clauses dealing with end of life of the PKI, archiving and transfer activity.

9.11. Individual notices and communications with participants

In case of change of any kind in the composition of the PKI, CSF will:

- later than one month before the start of the operation, to validate this change through technical expertise to assess the impacts on the quality and safety functions of the PKI and its various components.
- later than one month after the end of the operation, inform, where appropriate, the qualification body.

9.12. Amendments

9.12.1. Procedure for amendment

The CP are regularly reviewed to ensure compliance with changes in both technical (standards, reference, ...) and legal (laws, regulations, ...).

9.12.2. Notification mechanism and period

Any new version is available in electronic format on the website of CSF upon approval by the Directorate of CSF.
It shall take effect upon its publication.

9.12.3. Circumstances under which OID must be changed

The OID of each of these CP contain the major version number. Any significant change in the CP, in particular changes affecting existing certificates involves changing the major version number and therefore, an evolution of the OID.

9.13. Dispute resolution provisions

See [PRO.ACC.42].

9.14. Governing law

See [PRO.ACC.42].

9.15. Compliance with applicable law

See [PRO.ACC.42].

9.16. Miscellaneous provisions

9.16.1. Entire agreement

See [PRO.ACC.42].

9.16.2. Assignment

See section 5.8 above.

9.16.3. Severability

Should any provision of these CPs would prove to be invalid under applicable law, this does not challenge the validity and enforceability of any remaining provisions.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

See [PRO.ACC.42].

9.16.5. Force Majeure

Are considered acts of God all those usually used by the French courts and any other agreements that could bind the parties.

9.17. Other provisions

See [PRO.ACC.42].

APPENDIX 1 - REFERENCES

10. External legal documents

[CNIL] Law No. 78-17 of 6 January 1978 relating to computers, files and liberties, as amended by Act No. 2004-801 of 6 August 2004.

[DIRSIG] Directive 1999/93/EC of the European Parliament and Council of 13 December 1999 on a Community framework for electronic signatures.

[LCEN] Act No. 2004-575 of 21 June 2004 on confidence in the digital economy, in particular Article 31 concerning the declaration of provision of cryptology and Article 33 specifies that the liability of providers of certification services issuing qualified electronic certificates.

[ORDONNANCE] Order No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between authorities.

[DécretRGS] Decree No. 2010-112 of 02/02/2010 taken for the purposes of sections 9, 10 and 12 of Ordinance No. 2005-1516 of December 8, 2005.

[ArrêtéRGS] Order of May 6, 2010 approving the general security, specifying the modalities of implementation of the validation procedure of electronic certificates.

[SIG] Decree No. 2001-272 of 30 March 2001 made pursuant to Article 1316-4 of the Civil Code and on the electronic signature.

11. External technical documents

[RGS] Repository General Security -Version 1.0

[RFC3647] IETF -Internet X.509 Public Key Infrastructure -Certificate Policy and Certification Practice Framework -November 2003

12. Internal documents ChamberSign France

[GUI.ACC.11] ChamberSign France - Profiles of Certificates and CRLs

[PRO.ACC.42] ChamberSign France - Terms & Conditions of server authentication use