Certificate and timestamp authority

Certificate policy YOUSIGN SAS - QUALIFIED SEAL2 CA

Export at 23/04/2020

Creator : Kevin Dubourg - 25/02/2020

last change : Kevin Dubourg - 25/02/2020

Diffusion : C1 - Public

Summary:

1 - Revisions history 11
2 - Introduction 11
2.1 - Acronyms and terms 11
2.1.1 - Acronyms 11
2.1.2 - Terms 12
2.2 - General presentation 14
2.3 - Document identification 15
2.4 - Entities involved in PKI 15
2.4.1 - Certification Authority (CA) 15
2.4.2 - Registration Authority (RA) 15
2.4.3 - Certification Services Operator (CSO) 15
2.4.4 - Seal Certificate Officer (SOC) 16
2.4.5 - Certificate users 16
2.5 - Certificate usage 16
2.5.1 - Applicable areas of use 16
2.5.2 - Key pairs, CA certificates and components certificates 16
2.5.3 - Prohibited areas of use 16
2.6 - CP Management 17
2.6.1 - CP management body 17
2.6.2 - Contact 17
2.7 - References 17
3 - Responsibilities relating to the provision of information to be published .18
3.1 - Entities responsible for the provision of information 18
3.2 - Information to be published 18
3.3 - Publication frequency and deadlines 18
3.4 - Access control to the published information 18
4 - Identification and authentication 18
4.1 - Naming 18
4.1.1 - Types of name 18
4.1.2 - Need for use of explicit names 19

4.1.3 - Pseudonyms for seal creation service 19
4.1.4 - Rules for interpretation of the different name forms 19
4.1.5 - Uniqueness of names 19
4.1.6 - Identification, authentication and role of registered trademarks 20
4.2 - Initial validation of the identity 20
4.2.1 - Method for proving possession of the private key 20
4.2.2 - Validation of the identity of an organisation 20
4.2.3 - Validation of the identity of a holder 20
4.2.3.1 - Registration of a SCO to a certificate to issue 20
4.2.3.2 - Registration of a new SCO for a seal certificate already issued 21
4.2.4 - Non-verified holder information 22
4.2.5 - Validation of the applicant's authority 22
4.2.6 - Cross-certification of a CA 22
4.3 - Identification and validation of an application to renew keys 23
4.3.1 - Identification and validation for a current renewal 23
4.3.2 - Identification and validation for a renewal after revocation 23
4.4 - Identification and validation of a revocation application 23
5 - Operational requirements concerning the life cycle of the certificates 23
5.1 - Certificate application 23
5.1.1 - Origin of a certificate application 23
5.1.2 - Process and responsibilities for establishing a certificate application 23
5.2 - Processing of a certificate application 24
5.2.1 - Execution of the processes of identification and validation of the application 24
5.2.2 - Acceptance or rejection of the application 24
5.2.3 - Certificate creation time 24
5.3 - Issue of the certificate 24
5.3.1 - Actions of the CA concerning the issue of the certificate 24
5.3.2 - Notification by the CA of the issue of the certificate to the holder 24
5.4 - Acceptance of the certificate 25
5.4.1 - Process for accepting the certificate 25
5.4.2 - Publication of the certificate 25
5.4.3 - Notification by the CA to other entities of the issue of a certificate 25
5.5 - Use of the key pair and the certificate 25
5.5.1 - Use of the private key and the certificate by SCO 25

5.5.2 - Use of the public key and the certificate by the user of the certificate 25
5.6 - Renewal of a certificate 25
5.7 - Issue of a new certificate following a change of key pair 25
5.7.1 - Possible cause of change of key pair 26
5.7.2 - Origin of an application for a new certificate 26
5.7.3 - Procedure for processing an application for a new certificate 26
5.7.4 - Notification to the SCO of the creation of a new certificate 26
5.7.5 - Process for accepting the new certificate 26
5.7.6 - Publication of the new certificate 26
5.7.7 - Notification by the CA to other entities of the issue of a new certificate 26
5.8 - Modifying a certificate 26
5.9 - Revocation and Suspension of certificates 26
5.9.1 - Possible causes of a revocation 26
5.9.1.1 - Seal certificate 26
5.9.1.2 - CA components certificate 27
5.9.2 - Origin of a revocation application 27
5.9.2.1 - Seal certificate 27
5.9.2.2 - CA components certificate 27
5.9.3 - Procedure for processing a revocation application 28
5.9.3.1 - Revocation of a seal certificate 28
5.9.3.2 - Revocation of a certificate's component of the PKI 28
5.9.4 - Time granted to the SCO to make a revocation application 28
5.9.5 - Time limit for CA to process a revocation application 29
5.9.5.1 - Revocation of a seal certificate 29
5.9.5.2 - Revocation of a certificate's component of the PKI 29
5.9.6 - Requirements for verification of the revocation by the certificate users 29
5.9.7 - Frequency of producing CRLs 29
5.9.8 - Time limit for publication of an CRL 29
5.9.9 - Availability of an online system for checking the revocation and status of certificates 29
5.9.10 - Requirements for online verification of the revocation of certificates by the certificate users 29
5.9.11 - Other sources of information on revocations 29
5.9.12 - Specific requirements in the event the private key is compromised 30
5.9.13 - Possible causes of a suspension 30
5.10 - Certificate status information function 30

5.10.1 - Operational characteristics 30
5.10.2 - Availability of the function 30
5.11 - End of subscription 30
5.12 - Key escrow and recovery 30
5.12.1 - Recovery policy and practices by key escrow 31
5.12.2 - Recovery policy and practices by encapsulation of session keys 31
6 - Non-technical security measures 31
6.1 - Physical security measures 31
6.1.1 - Geographical situation and construction of sites 31
6.1.2 - Physical access 31
6.1.3 - Electricity supply and air conditioning 31
6.1.4 - Exposure to water damage 31
6.1.5 - Fire prevention and protection 31
6.1.6 - Preservation of media 31
6.1.7 - Deactivation of the media 32
6.1.8 - Off-site backup 32
6.2 - Procedural security measures 32
6.2.1 - Trusted roles 32
6.2.2 - Number of people required per task 32
6.2.3 - Identification and authentication for each role 33
6.2.4 - Roles requiring a separation of responsibilities 33
6.3 - Staff security measures 33
6.3.1 - Qualifications, competencies and authorisations required 33
6.3.2 - Procedures for background checks 33
6.3.3 - Initial training requirements 33
6.3.4 - Continuing training requirements and frequency of courses 34
6.3.5 - Frequency and sequence of rotations between different assignments 34
6.3.6 - Penalties in the case of unauthorised actions 34
6.3.7 - Requirements for staff of external service providers 34
6.3.8 - Documentation provided to staff 34
6.4 - Procedures for audit data constitution 34
6.4.1 - Frequency of processing the event logs 35
6.4.2 - Period for the preservation of event logs 35
6.4.3 - Protection of event logs 35

6.4.4 - Backup procedure for the event logs 36
6.4.5 - System for collecting event logs 36
6.4.6 - Notification of the record of an event to the event manager 36
6.4.7 - Vulnerabilities assessment 36
6.5 - Data archiving 36
6.5.1 - Types of data to be archived 36
6.5.2 - Archive retention period 36
6.5.3 - Certificate request 36
6.5.3.1 - Certificates, CRL and ARL issued by CA 37
6.5.3.2 - Event logs 37
6.5.4 - Protection of the archives 37
6.5.5 - Archive backup procedure 37
6.5.6 - Data timestamping requirements 37
6.5.7 - Archive collection system 37
6.5.8 - Archive recovery and verification procedure 37
6.6 - Changing CA keys 37
6.7 - Recovery after compromise and disaster 38
6.7.1 - Procedure for recovery and processing of incidents and compromises 38
6.7.2 - Recovery procedure in the event of corrupted computer resources (equipment, software and/or data) 38
6.7.3 - Recovery procedures in the event of compromise of the private key of a component 38
6.7.4 - Business continuity capabilities after a disaster 39
6.8 - End of life of PKI 39
6.8.1 - Transfer of activity or termination of activity affecting a CA's component 39
6.8.2 - Termination of activity affecting the CA 39
7 - Technical security measures 40
7.1 - Generation and installation of key pairs 40
7.1.1 - Key pairs generation 40
7.1.1.1 - CA's keys 40
7.1.1.2 - Seal's certificate keys 40
7.1.2 - Transmission of the private key to its owner 41
7.1.3 - Transmission of the public key to the CA 41
7.1.4 - Transmission of the CA's public key to the certificate users 41
7.1.5 - Key sizes 41
7.1.6 - Checking the generation and quality of the parameters of key pairs 41

7.1.7 - Key usage objectives 41
7.2 - Security measures for the protection of private keys and for cryptographic modules.. 41
7.2.1 - Security standards and controls for cryptographic modules 41
7.2.2 - Control of private keys by several persons 42
7.2.3 - Private key escrow 42
7.2.4 - Emergency copy of the private key 42
7.2.5 - Private key archiving 42
7.2.6 - Transfer of the private key to/from the cryptographic module 42
7.2.7 - Storage of the private key in the cryptographic module 42
7.2.8 - Method of activating the private key 43
7.2.9 - Method of deactivating the private key 43
7.2.10 - Method of destruction of private keys 43
7.2.11 - Security assessment level of the cryptographic module 43
7.3 - Other aspects of key pair management 43
7.3.1 - Public key archiving 43
7.3.2 - Lifespan of key pairs and certificates 43
7.4 - Activation data 44
7.4.1 - Generation and installation of activation data 44
7.4.1.1 - CA keys 44
7.4.1.2 - Seal keys 44
7.4.2 - Protection of activation data 44
7.4.2.1 - CA keys 44
7.4.2.2 - Seal keys 44
7.4.3 - Other aspects related to the activation data 44
7.5 - Computer systems security measures 44
7.5.1 - Technical security requirements specific to the computer systems 44
7.5.2 - Security assessment level of the computer systems 45
7.6 - Security measures related to the development of the systems 45
7.6.1 - Measures related to security management 45
7.6.2 - Security assessment level of the life cycle of the systems 45
7.7 - Network security measures 45
7.8 - Timestamping / dating system 45
8 - Certificates and CRL profiles 45
8.1 - Certificates profiles 45

8.1.1 - Root CA certificate 45
8.1.2 - "YOUSIGN SAS - QUALIFIED SEAL2 CA" 46
8.1.3 - Seal certificate 47
8.1.4 - OCSP certificate 49
8.2 - CRL profiles 50
8.3 - OCSP responder 51
8.3.1 - OCSP request 51
8.3.2 - OCSP responses 51
9 - Compliance audit and other assessments 52
9.1 - Frequency and/or circumstances of the assessments 52
9.2 - Identities: qualification by the assessors 52
9.3 - Relationship between assessors and assessed entities 52
9.4 - Scope of the assessments 52
9.5 - Actions taken as a result of the assessments 53
10 - Other professional and legal problems 53
10.1 - Fees 53
10.1.1 - Certificate and renewal fees 53
10.1.2 - Certificate access fees 53
10.1.3 - CRL access fees 53
10.1.4 - Refund policy 53
10.2 - Financial liability 53
10.2.1 - Insurance cover 53
10.2.2 - Other resources 53
10.2.3 - Cover and guarantee concerning the user entities 54
10.3 - Confidentiality of professional data 54
10.3.1 - Scope of the confidential information 54
10.3.2 - Information not classified as confidential 54
10.3.3 - Responsibilities in terms of protection of confidential information 54
10.4 - Protection of personal data 54
10.4.1 - Personal data protection policy 54
10.4.2 - Personal information 54
10.4.3 - Non-personal information 54
10.4.4 - Liability in terms of personal data protection 54

10.4.5 - Notification of and consent to use of personal data 55
10.4.6 - Conditions for disclosing personal information to the judicial or administrative authorities 55
10.4.7 - Other circumstances for disclosing personal information 55
10.5 - Intellectual and industrial property rights 55
10.6 - Contractual interpretations and guarantees 55
10.6.1 - Certificate Authority 55
10.6.2 - Registration Authority 56
10.6.3 - SCO 56
10.6.4 - Users 56
10.6.5 - Other parties 56
10.7 - Limit of warranty 56
10.8 - Limit of liability 56
10.9 - Indemnities 57
10.10 - Termination and early end of validity of the CP 57
10.10.1 - Validity period 57
10.10.2 - Early end of validity 57
10.10.3 - Effects of the end of validity and clauses that remain applicable 57
10.11 - Amendments to the CP 57
10.11.1 - Amendment procedures 57
10.11.1.1 - Decision 57
10.11.1.2 - Operational procedure 57
10.11.2 - Amendment process and reporting period 58
10.11.3 - Circumstances in which the OID must be changed 58
10.12 - Provisions concerning conflict resolution 58
10.13 - Jurisdiction 58
10.14 - Compliance with legislation and regulations 58
10.15 - Miscellaneous provisions 58
10.15.1 - Overall agreement 58
10.15.2 - Transfer of activities 58
10.15.3 - Consequences of a non-valid clause 58
10.15.4 - Application and cancellation 58
10.15.5 - Force majeure 59
10.15.6 - Other provisions 59

11 - Annex 1: Security requirements of the CA cryptographic module 59
11.1 - Security objectives requirements 59
11.2 - Certification requirements 59
12 - Annex 2: Security requirements of the seal creation device 59
12.1 - Security objectives requirements 59
12.2 - Certification requirements 60

1 - Revisions history

Version	Objet de la révision	Date	Auteur
1.0.3	Certification Services Operator (CSO) - Remove providers listing and add ISO 27001 compliance	02 Apr 2020	Kevin Dubourg
1.0.2	12 month LAR duration update Archiving of logs over 17 years	26 Sep 2018	Antoine Louiset
1.0.1	Modification of the certificate profile.	22 Oct 2015	Antoine Louiset
1.0	Initial version	07 May 2015	Antoine Louiset

2 - Introduction

2.1 - Acronyms and terms

2.1.1 - Acronyms

The acronyms used in this CP are as follows:

Acronym	Signification
ANSSI	French National Agency of System Security Information
ARL	Authority Revocation List
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statements
CRL	Certificate Revocation List
CSO	Certification Service Operator
DN	Distinguished Name
eIDAS	electronic IDentification, Authentication and trust Services
HSM	Hardware Security Module

Acronym	Signification
ICA	Intermediate Certificate Authority
IDS	Intrusion Detection System
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PDS	Public Disclosure Statements
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certificate Authority
RSA	Rivest Shamir Adelman
SCO	Seal Certificate Officer
SMS	Short Message Service
TSP	Trust Service Provider
URL	Uniform Resource Locator

2.1.2 - Terms

The terms used in this CP are as follows:

Terms	Signification
Authorized person	It is a person other than the SCO who is authorized by the CA's certification policy or by contract with the CA to carry out certain actions on behalf of the SCO (request for revocation, renewal, etc.) . Typically, in a company or an administration, it can be a manager of the SCO.
Certificate	Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it
Certificate Authority	Authority trusted by one or more users to create and assign certificates

Terms	Signification
Certificate generation function	This function generates (creation of format, electronic signature with the CA private key) certificates from information transmitted by the registration authority and from the public key associated to the SCO
Certificate Policy	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
Certificate Practice Statements	Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
Certificates status information function	This function provides certificate users information on the status of certificates (revoked, suspended, etc.). This function is implemented according to a method of publishing updated information at regular intervals (CRL, ARL, OCSP).
Certificate user	It's a third party (natural person, legal person, application or service) that's need to have confidence to the signed data and that can be able to check the certificate used.
Component	Platform operated by an entity and consisting of at least one computer station, an application and, if applicable, a means of cryptology and that has a determined role in the operational implementation of at least one function of the PKI. The entity can be the TSP itself or an external entity linked to the TSP by contractual, regulatory or hierarchical means.
Entity	Refers to an administrative authority or a company in the broadest sense, including legal persons responsive of associations
Hardware Security Module	In the context of a CA, the cryptographic module is an evaluated and certified material cryptographic resource used to store and implement the private key of CA, the key pairs of RCCs and to carry out cryptographic operations.
Keys pair	A key pair is a pairing composed of a private key (which must be kept secret) and a public key, necessary when using cryptologic techniques based on asymmetric algorithms
Private key	Part of the keys pair of an entity that It has to be kept under control of this entity
Public Key	Part of the keys pair of an entity that It can be made public

Terms	Signification
Publication function	This function makes available to third parties terms, certificate policies, trust chain certificates and all relevent information intended for SCO and / or certificate users, excluding certificate status information.
Public Key Infrastructure	All of the components providing management services for keys and certificates for use by a group of users.
Registration Authority	Registration Authority is responsible to check the identification of the future Seal Certificate officer.
Revocation function	This function processes revocation requests (in particular identification and authentication of the applicant) and determines the actions to be taken. The results of the processing are disseminated via the information function on the status of the certificates.
Seal Certicate Officer	It is a natural person whose is responsible for managing the seal certificate for a server or an application identified into the corresponding certificate and the associated private key on the behalf of the entity identified into the certificate too.
Secret key generation function	This function generates the keys pair of the SCO
Technical Management Committee	Technical Management Committee is an internal committee of Yousign that is in charge to the well running of the Yousign's PKI
Timestamping Authority	Authority responsible to manage the timestamping service
Trust Service Provider	Is a legal entity providing and preserving digital certificate to create and validate electronic signature and to authenticate their signatories. Trust service providers are qualified certificate authorities required in the European Union in the context of regulated electronic signing procedures.
Yousign's signature service	It's an application provided by "Yousign SAS" allowing a SCO to use the private key corresponding to the public key which is in the certificate and which identifies it in order to perform electronic signatures and authorize the signed data by other users. It is the only system authorized to access SCO private keys. To be able to use their private key, SCO must use its own activation data.

2.2 - General presentation

Yousign company is a Trust Service Provider (TSP) which provides to its customers and for its own use services involving electronic certificates and in particular electronic signature.

In this context, this document describes the Certification Policy (CP) as well as the Certificate Practice Statement (CPS) of the Certification Authority "YOUSIGN SAS - QUALIFIED SEAL2 CA". This document describes all of Yousign's commitments and practices in the context of the deployment and operation of the CA "YOUSIGN SAS - QUALIFIED SEAL2 CA", both on technical and organizational levels.

CA "YOUSIGN SAS - QUALIFIED SEAL2 CA" can only be used:

- to produce electronic seal qualified certificates,
- to produce Revocation Certificate Lists (CRL),
- to produce OCSP signing certificates for its own OCSP responder.

Electronic seal qualified certificates are exclusively fort legal person. These certificates are compliant with the standard ETSI EN 319411-2 at the QCP level.

The trust certification chain is as follows:

- ROOT CA: "YOUSIGN SAS -ROOT2 CA"
    - Intermediate CA: "YOUSIGN SAS - QUALIFIED SEAL2 CA"

2.3 - Document identification

This document corresponds to the Certification Policy (CP) and the Certificate Practice Statements (CPS) of the Certification Authority "YOUSIGN SAS - QUALIFIED SEAL2 CA". The identifier for this document is:

- OID : **2.250.1.302.1.13.1.0**, for the production of electronic seal qualified certificates

OIDs can change when major changes occur to the CP. When a new OID is generated, the last digit is incremented. The initial version uses the number 0.

2.4 - Entities involved in PKI

2.4.1 - Certification Authority (CA)

The meaning of Certification Authority (CA) as used in this CP is defined in chapter 1.6 below.

The CA is responsible for providing certificate management services for all of life cycle (enrolment, providing, renewal, revocation, ...) and uses for this a technical infrastructure: a Public Key Infrastructure (PKI). The services of the CA are the result of different functions which correspond to the different steps of the life cycle of key pairs and certificates. The CA maintains a risk analysis on the extent of the certification services that the CA offers. The Technical Management Committee of the CA decides on the risk management strategy, validates and follows the corresponding action plans.

The CA is the “Yousign SAS” company whose assumes all the CA’s functions.

2.4.2 - Registration Authority (RA)

Registration Authority is responsible to check the identification of the future Seal Certificate officer.

Registration Authority is operated by an internal service of Yousign.

2.4.3 - Certification Services Operator (CSO)

Yousign operates its various services itself. Yousign hosts its infrastructure by their third-party hosting providers (compliant to ISO 27001).

2.4.4 - Seal Certificate Officer (SOC)

In the context of this CP, a Seal Certificate Officer (SCO) is a natural person whose is responsible for managing the seal certificate for a server or an application identified into the corresponding certificate and the associated private key on the behalf of the entity identified into the certificate too. The SCO has a contractual / hierarchical / regulatory link with this entity.

The SCO complies with the conditions imposed on it defined in the CP of the CA "YOUSIGN SAS - QUALIFIED SEAL2 CA" and which are summarized in the Public Disclosure Statements (PDS) he must accept before using its certificate. It should be noted that the certificate being attached to the server and not to the SCO, which one the latter may have to change during the certificate's validity: departure of the SCO from the entity, change of assignment and responsibilities into the entity, etc.

2.4.5 - Certificate users

A certificate user designates an entity or part of an entity (including natural and legal persons) that may be required to use certificates to check their validity and their link with the signed data.

Certificate users access the information contained in the certificate, and those made available online by the CA, to check the validity of certificate (revocation, validity period, etc.).

Certificate users must comply with their obligations, as defined in this CP, in particular in §9.6.4

2.5 - Certificate usage

2.5.1 - Applicable areas of use

This CP is for usage of key pairs and certificates managed by SCO, so that entities can electronically sign data (documents or messages) in the context of dematerialized exchanges with the categories of certificate users identified in chapter above. A Such electronic signature provides, in addition to the authenticity and integrity of the data which are signed, the identity of the entity of the signatory.

2.5.2 - Key pairs, CA certificates and components certificates

This CP also covers requirements concerning the keys pair and certificates of the CA "YOUSIGN SAS - QUALIFIED SEAL2 CA".

The CA generates and signs different types of objects: certificates and CRL. To sign these objects, the CA has a key pair, whose corresponding certificate is attached to a higher-level CA (see hierarchy in §1.1). OCSP responses are signed by a specific certificate issued by the CA (see below).

The keys pair and certificates of the CA "YOUSIGN SAS - QUALIFIED SEAL2 CA" are only used for signing certificates, LCR and only for this purpose. In particular, they are never used either for confidentiality or authentication purposes.

The CA also signs certificates intended exclusively for sealing the OCSP responses of its service. These certificates are differentiated from certificate of the signature service by a specific policy identifier (OID: 1.2.250.1.302.1.14.1.0, see §7.1.4). The OCSP certificate management process corresponds to an internal procedure which is not detailed in this CP.

2.5.3 - Prohibited areas of use

All perimeter not provided for in the previous chapter applicable_usages is prohibited. Moreover, the purpose of the certificate must be in accordance with laws and regulations.

2.6 - CP Management

2.6.1 - CP management body

«Yousign SAS » company is responsible of this CP.

Yousign manages a Technical Management Committee composed by members of the top management of Yousign, functional and technical experts. The Technical Management Committee is responsible for the validation of the CP, the qualification and the implementation.

The Technical Management Committee is responsible for setting up and monitoring the operational technical infrastructure. He organizes audits and evaluations to ensure that the practices (technical and organizational) comply with the CA commitments made in this CP.

The process to modify this document is described in §9.11.

2.6.2 - Contact

Any request relating to this CP should be addressed to:

Gestion de l'AC Yousign

Yousign SAS

8 allée Henri Pigis

14000 CAEN

Email : contact@yousign.fr

2.7 - References

Reference	Description
[ANSSI_DELIV_CERT]	https://www.ssi.gouv.fr/uploads/2016/06/eidas_delivrance-certificats-qualifies_v1.1_anssi.pdf
[ANSSI_PSCO]	https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf
[EN_319401]	https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.01_60/en_319401v020201p.pdf
[EN_319411-2]	https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.02.02_60/en_31941102v020202p.pdf
[GDPR]	https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[EIDAS]	https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910

3 - Responsibilities relating to the provision of information to be published

3.1 - Entities responsible for the provision of information

Yousign has set up a page grouping publications at the following address:

https://yousign.com/documentation-technique-des-certifications/

3.2 - Information to be published

Yousign publishes the following information:

- This one and all of Certificate Policies managed by Yousign
- The list of revoked certificates (CRL/ARL)
- The trust chain certificates up to root certificate
- The Terms and Conditions of Use of Yousign for the different CA

3.3 - Publication frequency and deadlines

The publication deadlines and frequencies are as follows:

- The CP is published before any issuance of an end-entity certificate containing the corresponding OID
- CRLs are published daily, LARs annually
- CA certificates are published following their issuance and before any end-entity certificate is signed
- Terms and Conditions are published following each update.

This information is available seven days a week, twenty-four hours a day, with an availability of 99.7% over a month.
Technical Management Committee decides which third parties (customers, users, subcontractors for the provision of the service, assesment bodies, etc.) are to be informed during the effective or future publication of a new CP (initial version or modification of an existing CP) depending on the nature of the changes.

3.4 - Access control to the published information

All the published information indicated above is public and can only be accessed in read-only.

Modification to published data is restricted to internal Yousign teams responsible for publishing documents on the publication space. A strong and nominative access control is implemented, respecting the Yousign password policy which complies with current regulatory requirements.

4 - Identification and authentication

4.1 - Naming

4.1.1 - Types of name

The names used in a certificate are described in accordance with standard RFC X.500

Certificates of SCO are described in accordance with standard RFC X.509. CA issuer and certificate's subject are identified by their Distinguished Name (DN) in accordance with standard X.501 and the eIDAS regulatory (see eIDAS) .DNs are constructed as follows:

Attribute	Description	Include
CN	commonName: Free name designating the application service identify by the certificate. The name must contain the official name of the entity	YES
OI	organizationIdentifier: SCO entity identifier structured in the form: NTRFR-<SIREN number>	YES
OU	organizationUnit: SCO entity identifier structured in accorance to the RGS syntax: 0002 <SIREN number>	YES
O	organization: Entity name	YES
C	country: Country where Yousign SAS is established. The value is always FR	YES

Test certificates issued by "YOUSIGN SAS - QUALIFIED SEAL2 CA" are directly identifiable by adding the prefix "TEST - " into the value of the attribute CN, for example:

CN = TEST – Service de cachet ENTITE,…

Apart from this specificity, the test certificates issued by the "YOUSIGN SAS - QUALIFIED SEAL2 CA" follow the same processes as the certificates issued in production mode.

4.1.2 - Need for use of explicit names

The DN chosen to designate the seal creation services in the certificates must be explicit. The identification of the entity to which this service is attached is mandatory.

4.1.3 - Pseudonyms for seal creation service

Not applicable.

4.1.4 - Rules for interpretation of the different name forms

The elements contained in chapter 3.1.1 provide explanations for correctly interpreting the different forms of names.

4.1.5 - Uniqueness of names

To ensure the uniqueness of the names, the RA checks that, for the entity identified in the DN's OI attribute, the service name provided in the CN field has not already been used for a separate service.

4.1.6 - Identification, authentication and role of registered trademarks

The RA reserves the right to suspend the generation of a certificate if the DN is likely to be linked or to prejudice any title or intellectual property right.

If a such event occurs, the RA will ask the SCO information and documents demonstrating the legitimacy of its DN. Otherwise, the SCO will have to request the generation of a new certificate with a modification of the DN to avoid the same case and resolve the litigation.

4.2 - Initial validation of the identity

The registration of a seal creation service for an entity to which a certificate must be issued is made by registering the corresponding SCO with the RA. The RA also validates the "legal person" identity of the SCO is affiliate.

The registration of a SCO, and the corresponding entity, is done directly with the RA during a physical face-to-face process.

4.2.1 - Method for proving possession of the private key

Not applicable, the certificate holder does not generate his private key.

The certificate holder's private key is completely generated, stored and protected by Yousign's PKI that's guarantee the SOC's sole control of this private key.

4.2.2 - Validation of the identity of an organisation

See #below

4.2.3 - Validation of the identity of a holder

4.2.3.1 - Registration of a SCO to a certificate to issue

Registration of the new SCO (natural person) representing an entity requires the identification of this entity and the identification of the corresponding natural person.

The new SCO submits registration documents completed, including:

- The certificate request form, dated less than 3 months, signed by an authorized representative of the entity,
- A mandate, dated less than 3 months, authorising the new SCO as being entitled to be SCO for the seal creation service for which the seal certificate must be issued. This mandate must be signed by a legal representative of the entity and co-signed, for acceptance, by the future SCO,
- For a company, any document, valid at the time of the certificate request (Kbis extract or SIREN/SIRET attestation or national trade registry certificate, ...), attesting the existence of the company and bearing its SIREN number, or, failing this, another document attesting the unique identification of the company which will appear in the certificate,
- For a company, any document attesting to the quality of the signatory of the certificate request,
- For an administration, a document, valid at the time of registration, delegating or subdelegating the authority responsible of the corresponding administrative organization,
- A valid proof of identity for the new SCO among the following proofs:
  o the identity card,
  o the passport,
  o the residence permit,

- The Terms and conditions of use in force signed by the new SCO.

The request form contains:

- The name of the seal creation service identified by this request,
- Name, SIREN/SIRET number and the postal address of the new SCO's entity,
- Surname and givenames of the new SCO, as they appear on the identity document presented with the request,
- Information from the identity document presented: type, number, validity date, issuing authority,
- Email address of the new SCO,
- A phone number to join the new SCO,
- The explicit acceptance by the new SCO of its obligations
- The commitment to the accuracy of the information submited into the form, and in particular data which will be included into the certificate
- The acceptance of the new SCO to the archiving by the CA of the information in the registration and management of the seal's key.

The RA performs the following operations during the face to face:

- Control of the completeness and signature of the request form by an authorized representative of the entity,
- Control of the validity of the mandate and its signature by an authorized representative of the entity and by the new SCO,
- Control of the proof documents produced by the company or the administration to which the new SCO is attached,
- Control of the signature by the new SCO of the Terms and conditions of use of the signature service,
- Validation of the identity proof of the new SCO by checking the original document,
- Control of the consistency of the information given in the request form with the proof documents.

After these checks have been successfully completed, the RA timestamps and signs the form, then records the request in the PKI.

The RA archives the request form, the Terms and conditions as well as the proof documents. The SCO obtains a copy of the form and the Terms and conditions of use.

The SCO provides to the RA the authentication certificate that will be used to connect to Yousign's seal creation service, which is part of the activation data for the client's seal private key.

4.2.3.2 - Registration of a new SCO for a seal certificate already issued

In the case of a change to a new SCO for a valid seal certificate, the new SCO must be registered as such by the CA in replacement of the old SCO.

Registration of the new SCO (natural person) representing an entity requires the identification of this entity and the identification of the corresponding natural person.

The new SCO submits registration documents completed, including:

- The SCO change form, dated less than 3 months, signed by an authorized representative of the entity,
- A mandate, dated less than 3 months, authorising the new SCO as being entitled to be SCO for the seal creation service for which the seal certificate must be issued. This mandate must be signed by a legal representative of the entity and co-signed, for acceptance, by the future SCO,
- For a company, any document, valid at the time of the certificate request (Kbis extract or SIREN/SIRET attestation or national trade registry certificate, ...), attesting the existence of the company and bearing its SIREN number, or, failing this, another document attesting the unique identification of the company which will appear in the certificate,
- For a company, any document attesting to the quality of the signatory of the certificate request,
- For an administration, a document, valid at the time of registration, delegating or subdelegating the authority responsible of the corresponding administrative organization,

- A valid proof of identity for the new SCO among the following proofs:
  o the identity card,
  o the passport,
  o the residence permit,
- The Terms and conditions of use in force signed by the new SCO.

The change form contains:

- The name of the seal creation service identified by this request,
- Name, SIREN/SIRET number and the postal address of the new SCO's entity,
- Surname and givenames of the new SCO, as they appear on the identity document presented with the request,
- Information from the identity document presented: type, number, validity date, issuing authority,
- Email address of the new SCO,
- A phone number to join the new SCO,
- The explicit acceptance by the new SCO of its obligations
- The commitment to the accuracy of the information submited into the form, and in particular data which will be included into the certificate
- The acceptance of the new SCO to the archiving by the CA of the information in the registration and management of the seal's key.

The RA performs the following operations during the face to face:

- Control of the completeness and signature of the change form by an authorized representative of the entity,
- Control of the validity of the mandate and its signature by an authorized representative of the entity and by the new SCO,
- Control of the proof documents produced by the company or the administration to which the new SCO is attached,
- Control of the signature by the new SCO of the Terms and conditions of use of the signature service,
- Validation of the identity proof of the new SCO by checking the original document,
- Control of the consistency of the information given in the request form with the proof documents.
- After these checks have been successfully completed, the RA timestamps and signs the form, then records the request in the PKI.

After these checks have been successfully completed, the RA timestamps and signs the form, then records the new SCO in the PKI.

The RA archives the request form, the Terms and conditions as well as the proof documents. The SCO obtains a copy of the form and the Terms and conditions of use.

4.2.4 - Non-verified holder information

The SCO email address is declared and certified to be correct by it. Yousign does not check this data.

4.2.5 - Validation of the applicant's authority

The proof documents presented for the link between of the natural person with the legal person are sufficient to authorize the SCO to request a certificate on behalf of its attachment entity.

4.2.6 - Cross-certification of a CA

Not applicable

4.3 - Identification and validation of an application to renew keys

4.3.1 - Identification and validation for a current renewal

The identification and control of the identity of the SCO for a renewal of the certificate near its end of validity is done in the same way as a new certificate request.

See chapter above.

4.3.2 - Identification and validation for a renewal after revocation

The identification and control of the identity of the SCO for a renewal of the certificate after its end of validity is done in the same way as a new certificate request. See chapter above.

4.4 - Identification and validation of a revocation application

The request for revocation of a certificate must be made by the SCO or, failing this, by a legal representative of the entity attached to the stamp certificate.

The identity of the applicant is verified by the RA:

- When the request is made by the SCO, Yousign submits a series of two random questions concerning his identity,
- When the request is made by the legal representative, he must submit a paper request containing the signed revocation request, the KBis of the company, a copy of the applicant's identity document and a mandate if he is not a legal entity official representative.

In both cases, a Yousign revocation operator contacts the requester directly to validate the willingness to revoke.

5 - Operational requirements concerning the life cycle of the certificates

5.1 - Certificate application

5.1.1 - Origin of a certificate application

The certificate request is signed by the legal representative of the entity, and supplied by the SCO to the RA.

5.1.2 - Process and responsibilities for establishing a certificate application

Registration and identity validation of the SCO and its affiliated entity are described in this chapter. The request file is prepared by the SCO. He makes an appointment with the RA in order to submit his document and validate his identity and the entity's identification during a physical face-to-face meeting.

The following information must at least be part of the certificate request (see chapter above):

- The name of the seal creation service to be used in the certificate,
- Personal data of the RCC,
- Entity identification data.

5.2 - Processing of a certificate application

5.2.1 - Execution of the processes of identification and validation of the application

The RA performs the following operations:

- Validation of the identity of the SCO,
- Validation of the identity of the entity,
- Validation of the consistency of the proof documents presented,
- Validation that the SCO knows the Terms and conditions applicable for the use of the certificate.

Once these operations have been carried out, the RA issues the request to generate the certificate and the key pair to the appropriate function of the PKI.

The RA archives the registration request securely.

5.2.2 - Acceptance or rejection of the application

In the event of rejection of the request, the RA informs the SCO of it by justifying the rejection.

5.2.3 - Certificate creation time

The CA makes it possible to process the certificate request within a reasonable time. However, there are no restrictions regarding the maximum or minimum duration of treatment.

5.3 - Issue of the certificate

5.3.1 - Actions of the CA concerning the issue of the certificate

Following the authentication of the origin and the verification of the integrity of the request coming from the RA, the CA triggers the processes of generation and preparation of the different elements of the SSCO: the key pair, and the associated certificate. From this moment, the Yousign signature device will be activated.

The process for generating the certificate is securely linked to the process for generating the key pair. The private key and the certificate are integrated into the cryptographic module of the PKI. The SCO has not physically the private key associated with its seal certificate.

The conditions for generating keys and certificates and the security measures to be observed are specified in this chapter and this chapter, in particular the separation of trusted roles (see chapter).

5.3.2 - Notification by the CA of the issue of the certificate to the holder

Once the key pair and the certificate have been generated, and the Yousign seal service of the SCO activated, the SCO will be informed by email.

5.4 - Acceptance of the certificate

5.4.1 - Process for accepting the certificate

The acceptance of a certificate issued by the CA is tacit from the first seal created via the Yousign system. The SCO can refuse the certificate before its first use if he detects an error in it. This action is treated as a revocation request and results in the destruction of the key pair. The CA keeps a record of the acceptance (creation of the first seal) of the certificate by the SCO. This acceptance will be time stamped.

5.4.2 - Publication of the certificate

The CA does not publish certificates issued for SCO. The certificate is available in each signed document or upon request from the SCO to CA.

5.4.3 - Notification by the CA to other entities of the issue of a certificate

The RA can check the status of the request and the certificate in the PKI system.

5.5 - Use of the key pair and the certificate

5.5.1 - Use of the private key and the certificate by SCO

The SCO private key and public key are stored in a cryptographic module within the Yousign PKI. These elements can only be used in the context of the use of the Yousign seal service by the SCO. Any other use is strictly prohibited.

In addition, only the SCO can use their private key and certificate as part of a signature. This usage restriction of the private key and the associated certificate by the SCO exclusively is controlled by an authentication system for each request to create a seal.

5.5.2 - Use of the public key and the certificate by the user of the certificate

Certificate users must strictly observe the authorized uses of certificates.
Otherwise, their responsibility could be engaged.

5.6 - Renewal of a certificate

In accordance with RFC 3647, the notion of “certificate renewal” corresponds to the issuance of a new certificate for which only the validity dates are modified, all the other information is identical to the previous certificate (including the public key of the server).

Regarding this CP, there can be no certificate renewal without renewal of the corresponding key pair. The CA generating the SCO key pairs, guarantees that a certificate corresponding to an existing key pairs cannot be renewed within the meaning of RFC 3647.

5.7 - Issue of a new certificate following a change of key pair

In accordance with RFC 3647, this chapter deals with the issue of a new seal certificate linked to the generation of a new key pair.

5.7.1 - Possible cause of change of key pair

The key pairs must be periodically renewed in order to minimize the possibility of cryptographic attacks. Thus the key pairs and the corresponding certificates will be renewed at least at a frequency of 3 years.

In addition, a key pair and a certificate can be renewed in advance, following the revocation of the certificate (see this chapter in particular for the different possible causes of revocation).

5.7.2 - Origin of an application for a new certificate

The initiation of the supply of a new seal certificate is at the initiative of the SCO. The process to be followed is identical to the initial request (see this chapter and this chapter).

5.7.3 - Procedure for processing an application for a new certificate

See this chapter

5.7.4 - Notification to the SCO of the creation of a new certificate

See this chapter

5.7.5 - Process for accepting the new certificate

See this chapter

5.7.6 - Publication of the new certificate

See this chapter

5.7.7 - Notification by the CA to other entities of the issue of a new certificate

See this chapter

5.8 - Modifying a certificate

Modification of an issued certificate is not authorized by this PC. If necessary, a new certificate must be issued after revocation of the old one.

5.9 - Revocation and Suspension of certificates

5.9.1 - Possible causes of a revocation

5.9.1.1 - Seal certificate

The following circumstances may cause the revocation of the seal certificate:

- The information of the server appearing in its certificate is no longer in accordance with the identity of the seal service or the intended use in the certificate (for example, modification of the name of the entity), this before the normal expiration of the certificate,
- The SCO did not respect the applicable terms and conditions of use of the certificate,

- The SCO and / or, where applicable, the entity did not respect their obligations indicated in the CP of the CA or the corresponding Terms and conditions,
- An error (intentional or not) was detected in the registration of the SCO,
- The private key of the service is suspected of compromission, is compromised or, is lost (possibly the associated activation data),
- The SCO authentication or key activation data has been compromised or suspected of being compromised,
- The SCO or an authorized entity (legal representative of the entity for example) requests the revocation of the certificate (in particular in the case of destruction or alteration of the private key of the service and / or its device),
- The definitive shutdown of the server or the end of activity of the SCO's entity to which the server is attached,
- The certificate "YOUSIGN SAS - QUALIFIED SEAL2 CA" is revoked, involving the revocation of all the SCO's certificates which have been issued by this CA,
- The scheduled end of use of the hash algorithm implemented,
- The end of activity of the CA.

When one of the above circumstances occurs and the CA is aware of it (it is informed of it or it obtains the information during one of its verifications, notably when a new certificate is issued), the corresponding certificate must be revoked.

5.9.1.2 - CA components certificate

The following circumstances may cause the revocation of a certificate of a component of the PKI (including a CA certificate for the generation of certificates and CRL/ARL):

- Suspicion of compromise, compromise, loss or theft of the component's private key,
- Decision to change the PKI component following the detection of non-compliance of the procedures applied within the component with those announced in the CPS (for example, following a negative qualification or compliance audit),
- End of activity of the entity operating the component.

5.9.2 - Origin of a revocation application

5.9.2.1 - Seal certificate

The following persons / entities can request the revocation of a seal certificate:

- The SCO of the stamp certificate,
- A legal representative of the entity,
- The CA issuing the certificate or one of its components (RA for example).

The SCO is informed of the persons / entities who can make a revocation request of its certificate in the Terms and conditions.

5.9.2.2 - CA components certificate

The revocation of a CA certificate can only be decided by the entity responsible for the CA, or by the judicial authorities via a court decision.
The revocation of other component certificates is decided by the entity operating the component concerned, which must inform the CA without delay.

5.9.3 - Procedure for processing a revocation application

5.9.3.1 - Revocation of a seal certificate

The identification and validation requirements for a revocation request are described in this chapter.

The request for revocation of a certificate can be initiated by phone or by email at the support service team. The revocation operator of Yousign opens a support ticket and provides the requester with the seal certificate revocation request form. The applicant must complete this form, sign it and then return a scanned copy to the support service team, the original to be sent by postal way to Yousign.

When the request is made by the SCO and the Yousign's revocation operator is in possession of this signed request, he calls back the SCO using the contact details provided when the certificate is requested (or when the SCO has changed). The Yousign's operator checks the identity of the requester by asking two random questions based on the confidential information in the possession of Yousign. The revocation request is validated once these verifications have been successfully completed.

When the request is made by a legal representative, he must send by post documents including the revocation certificate request, a KBis of the company, a copy of the applicant's identity card and a mandate if he is not the legal responsible. The Yousign's operator checks the documents and validates the request once the checks have been carried out.

The following information must be included in the certificate revocation request:

- The name of the applicant for revocation,
- Any information about the certificate to be revoked allowing to found quickly and without error (serial number, entity identifier, SCO identity, validity dates),
- The reason of revocation.

Once the request has been authenticated and checked, the revocation function revokes the corresponding certificate by changing its status, then communicates this new status to the certificate status information function.

The revocation information will be disseminated at least via a CRL signed by an entity designated by the CA.

The revocation applicant will be informed of the good treatment of the revocation request and of the effective revocation of the certificate. In addition, if the SCO is not the applicant, he will also be informed of the effective revocation of his certificate.

The entity is informed of the revocation of any SCO's certificate attached to it.

The operation is recorded in the event logs.

5.9.3.2 - Revocation of a certificate's component of the PKI

In the case of revocation of one of the certificates in the certification chain, the CA must inform all of the SCO concerned as soon as possible and by any means (and if possible in advance) that their certificates are no longer valid. For this, the CA must inform the SCO by explicitly indicating to them that their certificates are no longer valid because one of the certificates in the certification chain is no longer valid.

To facilitate the revocation of the CA certificate, it is signed by a higher root authority.

5.9.4 - Time granted to the SCO to make a revocation application

As soon as the SCO (or an authorized person) becomes aware that one of the possible causes of revocation, within its jurisdiction, is effective, it must formulate its request for revocation without delay.

5.9.5 - Time limit for CA to process a revocation application

5.9.5.1 - Revocation of a seal certificate

By its nature, a request for revocation must be dealt with urgently.

The revocation function is available 24 hours a day, 7 days a week.

Any request for revocation of a seal certificate will be processed within a period of less than 24 hours, this period is between the receipt of the authenticated revocation request and the provision of revocation information to users.

5.9.5.2 - Revocation of a certificate's component of the PKI

The revocation of a certificate of a PKI's component must be carried out as soon as detection of an event described in the possible causes of revocation for this type of certificate. The revocation of the certificate is effective when the serial number of the certificate is entered into the revocation list of the CA which issued the certificate, and this list is accessible for download.

The revocation of a CA signing certificate (signing of certificates and of CRL/ARL) will be carried out immediately, particularly in the case of compromise of the key.

5.9.6 - Requirements for verification of the revocation by the certificate users

The user of a seal certificate is required to check, before use, the status of the certificates of the entire corresponding certification chain. It may use the last published CRL or the OCSP service.

5.9.7 - Frequency of producing CRLs

CRLs are generated at least every 24 hours.

5.9.8 - Time limit for publication of an CRL

CRLs are published as soon as possible after their establishment. The maximum publication period will be 30 minutes.

The OCSP service takes into account the revocation of certificates without delay.

5.9.9 - Availability of an online system for checking the revocation and status of certificates

See this chapter.

5.9.10 - Requirements for online verification of the revocation of certificates by the certificate users

See here.

5.9.11 - Other sources of information on revocations

Not applicable.

5.9.12 - Specific requirements in the event the private key is compromised

For seal certificates, the entities authorized to request revocation are required to do so as soon as possible after becoming aware of the compromise of the private key.

For CA certificates, in addition to the requirements of this parapgraph, the revocation following a compromise of the private key will be the subject of information clearly published on the website www.yousign.fr. In addition, in the event of compromise of the CA's private key, the CA undertakes to immediately and definitively interrupt the use of its private key and its associated certificate.

In accordance with regulatory obligations on European trusted service providers, the national supervisory body will be informed of the compromise of a private CA key within 24 (twenty-four) hours.

5.9.13 - Possible causes of a suspension

Certificates suspension is not allowed by this CP.

5.10 - Certificate status information function

5.10.1 - Operational characteristics

Yousign provides certificate users the information needed to check and validate, prior to its use, the status of a certificate and of the entire corresponding certification chain (up to and including the CA Root certificate), that is to say also to verify the signatures of the certificates of the chain, the signatures guaranteeing the origin and the integrity of the CRL/ARL and the state of the certificate of the CA Root.

The CRL/ARL are published at the address specified in this chapter, and at the address contained in the certificates issued.

The OCSP service is available at http://ocsp.yousign.fr, which is also indicated in the certificates issued.

5.10.2 - Availability of the function

The certificate status information function (CRL and OCSP) is available 24 hours a day, 7 days a week.

This function has a maximum unavailability time per service interruption (breakdown or maintenance) of 4 hours and an annual availability rate of 99.9%.

5.11 - End of subscription

In the event of the end of the contractual / hierarchical / regulatory relationship between the CA and the server's attachment entity before the end of validity of the certificate, for any reason, the certificate must be revoked.

In addition, the CA must revoke a seal certificate for which there is no longer a SCO explicitly identified.

5.12 - Key escrow and recovery

CA private keys are not escrowed. In addition, SCO's private keys are not escrowed. Although they are stored in the cryptographic module of the Yousign's PKI for use, this should not be considered as escrow.

5.12.1 - Recovery policy and practices by key escrow

Not applicable.

5.12.2 - Recovery policy and practices by encapsulation of session keys

Not applicable.

6 - Non-technical security measures

The requirements described in this chapter comply with the RGS requirements and result from the risk analysis and the risk management strategy defined by the Yousign Technical Management Committee.

6.1 - Physical security measures

6.1.1 - Geographical situation and construction of sites

The Yousign certification services hosting sites are located in secure areas.

6.1.2 - Physical access

In order to avoid any loss, damage and compromise of the resources of the PKI and the interruption of the services of the CA, access to the areas of the various components of the PKI are controlled. Personels will need to authenticate and have the necessary rights to physically and logically access all of the PKI's resources and features.

All physical accesses are traced (video recording and monitoring of the opening of the bays).

6.1.3 - Electricity supply and air conditioning

Power supply and air conditioning protection systems are implemented to ensure the continuity of the services provided.

The materials used to perform the services are operated in compliance with the conditions defined by their suppliers and / or manufacturers.

6.1.4 - Exposure to water damage

Hosting site is provided in a non-floodable area.

6.1.5 - Fire prevention and protection

The fire prevention and protection means implemented by the CA are compliant with the requirements and commitments made by the CA in this CP, in terms of availability.

6.1.6 - Preservation of media

Media backups are performed daily. The sites in which the backups are kept are protected against the risk of fire and flooding. In addition, physical and logical accesses are protected and subject to rights management and strong authentication.

If paper documents are used, or removable media such as a CD, USB storage key, external hard drive or smart card, these will be kept in a safe accessible by the person responsible of the Technical Management.

6.1.7 - Deactivation of the media

The decommissioning of the various media varies according to their nature. Regarding paper documents, CDs, USB storage keys, smart cards, they will be shredded at the end of their life (end of use or obsolescence). The storage media will be emptied and then destroyed. The HSMs will be decommissioned following the manufacturer's instructions.

6.1.8 - Off-site backup

The PKI's components supports the functions of revocation and information on the status of certificates, have an off-site backup that allowing a rapid recovery of these functions after the occurrence of a disaster or an event seriously and lastingly affecting the provision of these services (destruction of the site, etc.). Backup and restore functions will be performed by authorized administrators in accordance with procedural security measures.

Off-site backups are performed in a secure environment with physical and logical access, and secured against the risk of fire and flooding.

6.2 - Procedural security measures

6.2.1 - Trusted roles

The Yousign Technical Committee implements the following roles:

- **Security officer**: The security officer is responsible for implementing the PKI security policy. He decides the physical access controls to the equipment of the component systems. He is authorized to examine the archives and is responsible for analyzing event logs in order to detect any incident, anomaly, attempted compromise, etc. He is responsible for certificate generation and revocation operations. This role is assigned to the head of the Technical Management Committee.
- **Application manager**: The application manager is responsible, within the component to which he is attached, for the implementation of the CP and CPS of the PKI of the application for which he is responsible. Its responsibility covers all the functions rendered by this application and the corresponding performances.
- **System engineer**: He is responsible for the start-up, configuration and technical maintenance of the component's IT equipment. It provides technical administration of the component's systems and networks.
- **Operator**: An operator within a component of the PKI realizes, in relation of his attributions, the system operations of the applications for the functions implemented by the component.
- **System auditor**: Designated person whose role is to regularly analyze the event logs in order to detect any incident, anomaly, attempted compromise, etc.

In addition to these trusdted roles, a CA distinguishes, as a trusted role, the roles of secret holder of CA's secrets. These secret share holders are responsible for ensuring the confidentiality, integrity and availability of the shares entrusted to them.

All persons operating a trusted role within the PKI will be notified, and will accept this role through the signing of a role acceptance agreement. The application manager will then train and educate the person obtaining a trusted role.

The functions of the PKI are subject to role-based access management. A strong authentication system is in place.

6.2.2 - Number of people required per task

Depending on the type of operation performed, the number and the quality of the personel to be respected, as actors or witnesses, may be different.

For security reasons, it is requested to distribute the sensitive functions among several people. This CP defines a certain number of requirements concerning this distribution, in particular for the operations linked to the cryptographic modules of the PKI (see this chapter).

6.2.3 - Identification and authentication for each role

All persons operating a trusted role within the Yousign's PKI must obtain prior authorization. All functions of the PKI are subject to authorization control based on strong authentication.

The application manager manages permissions. He will have to manage the list of authorizations according to the roles. In addition, he will have to assign the right role to each person. Finally, he is also responsible to issue the authentication data to the personnel. It will issue a certificate for authentication usage.

Each assignment of a role to a member of the PKI staff must be notified in writing. This role must be clearly mentioned and described in his job description.

6.2.4 - Roles requiring a separation of responsibilities

Several roles can be assigned to the same person, as long as the combination does not compromise the security of the functions implemented. However, there is a mandatory separation of the following roles: security manager and system engineer.

6.3 - Staff security measures

6.3.1 - Qualifications, competencies and authorisations required

All personnel working within PKI components are subject to a non-disclosure agreement with Yousign.

The staff working within Yousign's PKI, will hold a position corresponding to their professional skills. Staff in a trusted role (security manager, application manager, system engineer or system auditor) must have the expertise appropriate to their role and be familiar with the security procedures in force within the PKI.

CA informs all those involved in trusted roles:

- Its responsibilities relating to the services of the PKI,
- Procedures related to system security and personnel control, with which it must comply.

6.3.2 - Procedures for background checks

Yousign ensures the honesty of its personnel working within a PKI component by implementing means respecting the legal framework and the regulations in force. In particular, this personnel with a trusted role has not committed any crime offence in contradiction with their responsabilities. They must provide Yousign with a copy of bulletin no. 3 from their criminal records. People in a trusted role must not suffer from conflicts of interest prejudicial to the impartiality of their tasks. These verifications will be carried out before being assigned to a trusted role.

6.3.3 - Initial training requirements

Staff are trained in the software, hardware and internal operating and security procedures that they implement and that they must respect, corresponding to the component within which they operate.

6.3.4 - Continuing training requirements and frequency of courses

The personnel concerned will be informed and will have adequate training prior to any development in systems, procedures, organization, etc. depending on the nature of these developments.

Staff are regularly (annually) trained in state-of-the-art IT security practices and are trained in the management and treatment of security incidents.

6.3.5 - Frequency and sequence of rotations between different assignments

This CP does not make any requirements.

6.3.6 - Penalties in the case of unauthorised actions

The associated sanctions and disciplinary procedures are defined in the internal authorization conditions and the IT charter provided to all Yousign employees. These are more or less important depending on the impact that an unauthorized action can have.

6.3.7 - Requirements for staff of external service providers

No external service provider can have a trusted role within the Yousign's PKI. If an external service provider must access on a component of the PKI, this is done with the prior agreement of the security manager, and under his supervision. All interventions carried out are logged.

6.3.8 - Documentation provided to staff

The personnel have adequate documentation concerning the operational procedures and the specific tools that they implement as well as the general policies and practices of the component within which they work. In particular, he must be given the security policies impacting him.

6.4 - Procedures for audit data constitution

Type of event to be recorded

Concerning the systems linked to the functions which are implemented within the PKI, it logs the events as described below, in electronic form. Logging is automatic, from the start of a system and without interruption until the shutdown of this system.

- Creation / modification / deletion of user accounts (access rights) and corresponding authentication data (passwords, certificates, etc.),
- Start and stop of computer systems and applications,
- Activity events (logs) of firewalls and routers,
- Logging events: start and stop of the logging function, modification of logging parameters, actions taken following a failure of the logging function,
- Login / logout of users with trusted roles, and the corresponding unsuccessful attempts.

Other events are collected, by electronic and/or manual means. These are those relating to security and which are not produced automatically by computer systems, in particular:

- Actions for maintenance and configuration changes of the systems, which are logged in an electronic document and/or paper signed and time-stamped,

- Changes made to personnel, which are recorded in an electronic document and/or paper signed and time-stamped,
- Actions to destroy and reset media containing confidential information (keys, activation data, SCO personal information, ...), which are logged in an electronic document and/or paper signed and time stamped.

In addition to these logging requirements common to all components and functions of the PKI, specific events to the different functions of the PKI must also be logged, including:

- Receipt of a certificate request (initial and renewal),
- Validation / rejection of a certificate request,
- Events related to signature keys and CA certificates (generation (key ceremony), backup / recovery, revocation, renewal, destruction, ...),
- Generation of SCO's certificates,
- Transmission of certificates to SCO,
- Publication and updating of information related to the CA (CP, CA certificates, Terms and conditions of use, etc.),
- Receipt of a revocation request,
- Validation / rejection of a revocation request,
- Generation and publication of CRLs.

Each record of a log must contain at least the following fields:

- King of event,
- Name of the author or identification of the starting system,
- Event timestamp (the exact time of significant CA events concerning the environment, key management and certificate management must be recorded),
- Event result (succesfull and unsuccessful).

Accountability for an action is applicable to the person, entity or system that performed it. The name or identification of the author must appear explicitly in one of the fields in the event log.

In addition, depending on the type of event, each record should also contain the following fields:

- Recipient of the operation,
- Name of the requester of the operation or reference of the system making the request,
- Name of the people present (if this is an operation requiring several people),
- Cause of the event,
- Any information specifying the event (for example, for the generation of a certificate, the serial number of this certificate).

In the case of manual entry, the entry must be made, in general, on the same working day as the event.

6.4.1 - Frequency of processing the event logs

See here.

6.4.2 - Period for the preservation of event logs

Event logs are kept on site for a maximum of 90 days. They are archived at least within a period of 3 months.

6.4.3 - Protection of event logs

On site, event logs are only made available to trusted roles.

6.4.4 - Backup procedure for the event logs

All event logs are backed up daily.

6.4.5 - System for collecting event logs

The collection of event logs is done through a log centralization system.

6.4.6 - Notification of the record of an event to the event manager

No notification is issued following the recording of an event.

6.4.7 - Vulnerabilities assessment

Yousign performs or has performed a vulnerability analysis. To do this, several elements are analyzed:

- An analysis of physical access, in order to detect any unauthorized intrusion,
- A complete analysis of event logs for detection of event or operation failure is performed continuously. Staff with a trusted role are notified by email when an anomaly is detected,
- Automatic analysis with a vulnerability management tool. A weekly scan is performed and a report sent to staff in a trusted role.

6.5 - Data archiving

6.5.1 - Types of data to be archived

Archiving means are put in place by the CA. This archiving ensures the perenity of logs made up by the different components of the PKI.

Archiving data are the followings:

- Binaries and configuration files of components,
- CP,
- CPS,
- Certificates, CRL, ARL as issued or published,
- Commitments signed by the head of the Technical Management Committee,
- Logs of the different components of the PKI,
- Registrations,
- Acceptance of certificate by SCO.
- Archive retention period

6.5.2 - Archive retention period

6.5.3 - Certificate request

All accepted certificate request documents will be archived for 10 years to provide proof of certification in legal procedures.

The retention period for registration documents must be informed to the SCO.

During this period of opposability of the documents, the certificate request data must be able to be presented by the CA when requested by the competent authorities.

This data must enable the real identity of the natural persons named in the certificate issued by the CA to be found.

6.5.3.1 - Certificates, CRL and ARL issued by CA

Seal and CA certificates, as well as the CRL/ ARL produced, must be archived for at least 10 years after their expiration.

6.5.3.2 - Event logs

Event logs identified in this chapter will be archived for 17 years after their generation. Archiving will be done in a secure environment, ensuring data integrity over time.

6.5.4 - Protection of the archives

During all the time of their conservation, the archives, and their backups, will:

- Be protected in integrity,
- Be accessible only to authorized persons,
- Could be re-read and exploited during the entire archiving period.

6.5.5 - Archive backup procedure

Archiving is carried out either automatically or manually by authorized personnel. Archives iare encrypted in AES256 and then sent off-site in a secure environment. These archives are duplicated on several separate datacenters to guarantee their availability.

6.5.6 - Data timestamping requirements

Each event contains the precise date and time of completion. Daily archives are time stamped using a cryptographic process.

Components in charge of the revocation function are synchronized daily with a UTC time source.

6.5.7 - Archive collection system

Yousign's archive collection systems are internal.

6.5.8 - Archive recovery and verification procedure

Archives can be recovered within a maximum of 2 working days. Only people in a trusted role can perform the operations of recovery and verification of archives.

6.6 - Changing CA keys

The CA cannot generate a certificate whose end date is later than the expiration date of the corresponding CA certificate. For this, the period of validity of this CA certificate must be greater than the validity of the certificates it signs.

Regarding the expiry date of this certificate, its renewal will be requested within a period at least equal to the lifetime of the certificates signed by the corresponding private key.

As soon as a new CA key pair is generated, only the new private key will be used to sign certificates.

The previous certificate remains usable to validate the certificates issued under this key until all the certificates signed with the corresponding private key have expired.

6.7 - Recovery after compromise and disaster

6.7.1 - Procedure for recovery and processing of incidents and compromises

The Yousign's PKI has implemented procedures and means for reporting and dealing with incidents, in particular through awareness and training its staff and by analyzing the various event logs. These procedures and means must make it possible to reduce damage due to security incidents and malfunctions.

In the case of a major incident, such as loss, suspected compromise, compromise, theft of the CA's private key, the triggering event is the observation of this incident at the PKI level. The person in charge of the Technical Committee must be informed immediately. He will have to treat the anomaly. If he considers the incident to have a serious level of severity, he will request an immediate revocation of the certificate. If it occurs, it will publish the certificate revocation information urgently, immediately if it is possible. He will do so via the Yousign public site, via email notification to all customers.

If one of the algorithms, or associated parameters, used by the CA or its SCO becomes insufficient for its intended remaining use, then the person in charge of the Technical Committee will publish the information via the public site and notify by e-mail all of Yousign's customers. All relevant certificates will then be revoked.

In accordance with regulatory obligations on European trusted service providers, the national supervisory body will be informed of any security incident affecting the CA and its services within 24 (twenty-four) hours.

6.7.2 - Recovery procedure in the event of corrupted computer resources (equipment, software and/or data)

Hosting site of Yousign has a business continuity plan to meet the availability requirements of the various functions of the PKI expected from this CP, the commitments of the CA in its own CP especially with regard to functions related to the publication and / or revocation of certificates.

Yousign has a procedure for resetting the software environment.

This plan will be tested at least once every 2 years.

6.7.3 - Recovery procedures in the event of compromise of the private key of a component

The compromise of a component key is treated in the component continuity plan (see this chapter) as a disaster.

If a CA key is compromised, the corresponding certificate will be immediately revoked (see this chapter).

In addition, CA respects the following commitments:

- Inform all SCO,
- Indicate that certificates and revocation status information issued using this CA key may no longer be valid,
- Inform the national supervisory body within twenty-four hours (see this chapter).

6.7.4 - Business continuity capabilities after a disaster

Yousign's PKI has the necessary means to ensure the continuity of activities in accordance with the requirements of this CP (see this chapter).

6.8 - End of life of PKI

One or more components of the PKI may have to cease their activity or transfer it to another entity for various reasons.

CA makes the necessary to cover costs to meet these minimum requirements in the event that the CA is bankrupt or for other reasons is unable to cover these costs on its own, as far as possible, depending on the constraints of the applicable bankruptcy law.

The transfer of activity is defined as the end of activity of a component of the PKI that does not affect the validity of the certificates issued prior to the transfer considered and the continuity of this activity organized by the CA in collaboration with the new entity.

The cessation of activity is defined as the end of activity of a component of the PKI having an impact on the validity of the certificates issued prior to the cessation concerned.

The CA will communicate to the contact point identified on http://ssi.gouv.fr, the main steps of the action plan implementing the technical and organizational means intended to treat a cessation of activity or to organize the transfer activity. In particular, CA will present the means put in place for archiving (keys and information relating to certificates) in order to ensure directly or to make ensure this function over the entire period initially planned in its CP. CA will communicate to ANSSI, according to the different components of the PKI concerned, the modalities of the changes that have occurred. CA will measure the impact and make an inventory of the consequences (legal, economic, functional, technical, communication, etc.) of this event. CA will keep ANSSI informed of any obstacle or additional delay encountered during this process.

6.8.1 - Transfer of activity or termination of activity affecting a CA's component

To ensure a constant level of confidence during and after such events, the CA:

- Establishes procedures whose objective is to ensure a constant service in particular in the field of archiving (in particular, archiving of seal certificates and information relating to certificates),
- Ensures the continuity of the revocation (taking into account a request for revocation and publication of the CRL and ARL), in accordance with the availability requirements for its functions defined in this CP. Otherwise, the Government's applications will refuse certificates issued by CAs whose valid CRLs are no longer accessible, even if the seal certificate is still valid,
- To the extent that the planned changes may have an impact on commitments for SCO or certificate users, the CA must notify them as soon as necessary.

6.8.2 - Termination of activity affecting the CA

The cessation of activity can be total or partial (for example: cessation of activity for a given family of certificates only). The partial cessation of activity will be gradual so that only the obligations referred to below are to be performed by the CA, or a third-party entity which continues activities, when the last certificate issued expires.

In the event of a complete cessation of activity, the CA or, if this is impossible, any entity which would be substituted for it by the effect of a law, a regulation, a decision of justice or an agreement previously concluded with this entity, must ensure the revocation of certificates and the publication of CRL/ARL in accordance with the commitments made in its CP.

CA takes the following measures in the event of separation from service:

- Notification of affected entities,
- The transfer of its obligations to other parties,
- Management of revocation status for unexpired certificates that have been issued.

When the service is stopped, the CA will take the following measures:

- Refrain from transmitting the private key that enabled him to issue certificates,
- Take all necessary measures to destroy it or render it inoperative,
- Revoke his certificate,
- Revoke all the certificates that CA signed and that are still valid,
- Inform (for example by receipt) all SCO of certificates revoked or to be revoked, as well as their affiliated entity if applicable.

7 - Technical security measures

The requirements described in this chapter comply with the RGS requirements and result from the risk analysis and the risk management strategy defined by the Yousign Technical Management Committee.

7.1 - Generation and installation of key pairs

7.1.1 - Key pairs generation

7.1.1.1 - CA's keys

The generation of the CA keys is carried out in a secure environment (see this chapter). CA signing keys are generated and implemented in a cryptographic module that complies with the requirements of this chapter for the security level considered.

The generation of CA keys is carried out in perfectly controlled way, by personnel in trusted roles (see this chapter), during “key ceremonies”. These ceremonies are realized according to the procedure previously defined and validated by the Technical Management Committee.

The initialization of the PKI and/or the generation of the CA keys is accompanied by the generation of PKI secret shares. These parts of secrets are authentication data making it possible to manage and manipulate, after the key ceremony, the CA private keys, in particular, to be able to subsequently initialize new cryptographic modules with the CA keys.

These secret shares are stored on a smart card. The same holder cannot hold more than one share of secrets from the same CA at any given time. Each share of secrets is under sole control of the corresponding holder.

The key ceremony is carried out by two internal Yousign people in trusted roles. In addition, a witness validates the proper implementation of the ceremony.

7.1.1.2 - Seal's certificate keys

The generation of seal keys is carried out in a secure environment (see this chapter).

The seal key pairs are generated directly in a seal creation device that complies with the requirements of this chapter. This device is a cryptographic module which complies with the requirements of this chapter and is owned by Yousign.

7.1.2 - Transmission of the private key to its owner

The private key is not transmitted to the SCO or its entity. It is stored by the PKI within a cryptographic module.

7.1.3 - Transmission of the public key to the CA

The SCO public key is technically transmitted to the CA following the process of generating the key pair, in the cryptographic module. This is done through a message in PKCS#10 format signed by the server private key.

7.1.4 - Transmission of the CA's public key to the certificate users

The CA public key is wrapped in a certificate signed by the root CA. Its distribution is accompanied by the digital fingerprint of the certificate as well as a declaration that it is indeed a public key of the CA.

The CA public key, and the corresponding information (certificate, digital fingerprints, declaration of belonging) can easily be retrieved by certificate users, on the publication service of Yousign (see this chapter).

7.1.5 - Key sizes

CA keys have these characteristics:

- Algorithm used: RSA.
- Minimum key size: 4096 bits.

The keys to the stamp and OCSP certificates have these characteristics:

- Algorithm used: RSA.
- Minimum key size: 2048 bits.

7.1.6 - Checking the generation and quality of the parameters of key pairs

The device used for generating key pairs is a cryptographic module conforming to the requirements of this chapter, configured and operated in accordance with the recommendations of its supplier, which guarantees the quality of the key pairs generated.

7.1.7 - Key usage objectives

The use of a private CA key and associated certificate is strictly limited to signing certificates, CRL/ARL (see this chapter).

The use of a private seal key and associated certificate is strictly for the seal creation service (see this chapter).

7.2 - Security measures for the protection of private keys and for cryptographic modules

7.2.1 - Security standards and controls for cryptographic modules

The cryptographic modules, used by the CA and the seal creation service, for the generation and implementation of their signature keys, are cryptographic modules meeting the requirements of this chapter. Yousign uses certified HSMs and ensures their security, physical and software aspect. Yousign hosts this equipment in controlled access areas protected against power outages, floods and fires.

Yousign ensures the safety of HSMs during their installation, during the key ceremony, during their use, until their end of life.

7.2.2 - Control of private keys by several persons

The control of the CA private keys is ensured by trusted roles (holders of PKI secret shares) and with a tool implementing the secret's sharing. There are 3 secret holders for each CA, who are given these secrets on a smart card during the key ceremony. We use an “M of N” sharing secret algorithm: a quorum of 2 holders out of 3 is necessary to authorize an operation on the keys.

Control of the SCO private key is under its sole control. Yousign does not have the elements to access and use the private key of a server during the signing process. The technical process ensures that only the private key generated for the server during the signing process is used.

7.2.3 - Private key escrow

CA and SCO private keys are not escrowed.

7.2.4 - Emergency copy of the private key

CA and seal private keys are backed up, either in a cryptographic module conforming to the requirements of this chapter, or outside a cryptographic module but in this case in an encrypted form and with an integrity control mechanism. The encryption used offers a level of security equivalent to or higher than the storage within the cryptographic module and, in particular, uses an algorithm, a key length and an operating mode capable of resist attacks by cryptanalysis for at least the duration of life of the key thus protected.

Encryption and decryption operations are carried out inside the cryptographic module in such a way that the CA and seal private keys are at anytime in a clear way outside the cryptographic module.

Control of encryption/decryption operations must comply with the requirements of this chapter.

7.2.5 - Private key archiving

CA and seal private keys are never archived.

7.2.6 - Transfer of the private key to/from the cryptographic module

Generation of CA and seal private keys is done within the cryptographic module.

Transfer to/from the cryptographic module is only done for the generation of backup copies. This is done in encrypted form, in accordance with the requirements of this chapter.

7.2.7 - Storage of the private key in the cryptographic module

Storage of CA and seal private keys is carried out within a cryptographic module meeting the requirements of this chapter and this chapter for the level of security considered.

However, in the case of backups, storage can be carried out outside a cryptographic module subject to compliance with the requirements of this chapter.

Yousign implements means to guarantee that the CA and seal private keys are not compromised during their storage or their transport.

7.2.8 - Method of activating the private key

Activation of CA's private keys will be done in a cryptographic module and will be controlled via activation data (see this chapter). For the CA, secret share holders must be present in order to carry out the activation.

The activation of the private seal key is linked to the signing process and requires authentication of the SCO (see this chapter).

The technical architecture of the Yousign seal creation service only allows the use of a private key if the authentication data is entered by the SCO. In addition, a signature made by "YOUSIGN SAS - QUALIFIED SEAL2 CA" is only valid if the Yousign's PKI can proof to the lifecycle of a signature request with a set of logs, and traces which are documented.

7.2.9 - Method of deactivating the private key

Deactivation of the CA and seal private CA keys in the cryptographic module is automatic as soon as the environment of the module changes: stop or disconnection, disconnect the operator, etc.

These deactivation conditions must make it possible to comply the requirements defined in this chapter for the level of security considered.

7.2.10 - Method of destruction of private keys

At the normal or anticipated (revocation) end of the life of a CA or seal private key, it is systematically destroyed, along with any copy and any element allowing it to be reconstituted.

7.2.11 - Security assessment level of the cryptographic module

Cryptographic modules used by Yousign are modules qualified at the high level by ANSSI.

7.3 - Other aspects of key pair management

7.3.1 - Public key archiving

CA public keys are archived for 12 years after the corresponding certificates have expired.

7.3.2 - Lifespan of key pairs and certificates

The key pairs and certificates of CAs have a lifespan of 10 years maximum.

The end of validity of a CA certificate must be later than the end of the life of the seal certificates it issues.

Key pairs and seal certificates have a maximum lifespan of 3 years.

7.4 - Activation data

7.4.1 - Generation and installation of activation data

7.4.1.1 - CA keys

Generation and installation of activation data for a cryptographic module is done during the initialization and customization phase of this module. Activation data is stored on smart cards. These cards are provided to secret share holders who must store them securely, protecting them from theft, damage, and unauthorized use.

7.4.1.2 - Seal keys

The activation data for seal private key consists of the client's SSL authentication private key on the one hand, and a secret known only to the SCO on the other. This secret is submitted by in a session authenticating the client with its private SSL authentication key on the Yousign signature service.

7.4.2 - Protection of activation data

7.4.2.1 - CA keys

Secret share holder is responsible for ensuring the confidentiality, integrity and availability of the activation data.

7.4.2.2 - Seal keys

SCO is the only one to know the secret for activating the private key, associated with the seal and the SCO. He is responsible for protecting this secret. He also guarantees the protection of the client's private SSL authentication key. The request to create a seal is made in an HTTPS session with mutual authentication, which protects the confidentiality of the data exchanged.

7.4.3 - Other aspects related to the activation data

Not applicable.

7.5 - Computer systems security measures

7.5.1 - Technical security requirements specific to the computer systems

PKI implements a series of measures and means to guarantee a high level of security:

- Strong authentication of system users with user role management based
- Management of sessions (disconnection after a period of inactivity, access to files controlled by role and user name)
- Implementation of antivirus and antimalware
- Periodic review of staff skills about computer systems
- Regular monitoring to detect any attempt to access computer systems
- Security monitoring ensuring the regular application of IT system security patches, and taking critical vulnerabilities into account within 48 hours
- Computer systems hardening policy
- Network protection

7.5.2 - Security assessment level of the computer systems

Not applicable.

7.6 - Security measures related to the development of the systems

7.6.1 - Measures related to security management

All developments made by Yousign and impacting the PKI are documented and carried out through a process in order to ensure their quality.

The configuration of the PKI components system as well as any modifications and upgrades are documented and checked.

In addition, Yousign operates a closed separation between the development, test, pre-production and production environments. This ensures a quality production process.

7.6.2 - Security assessment level of the life cycle of the systems

Any significant upgrade of a system of a PKI's component must be tested and validated before deployment. These operations are carried out by trusted roles.

7.7 - Network security measures

CAs subject to this CP are online and are deployed in a physically secure environment and periodically audited. Network protection devices (firewalls, intrusion detection systems (IDS), VPN) contribute to network security. Flows that are not explicitly authorized are prohibited by default.

The IT systems administration network is logically separate from the operating network. Administration stations, specifically secured, are dedicated to system administration.

Redundancy of access to services exposed on the Internet is ensured.

The configuration of network equipment is periodically audited. Penetration tests are performed periodically.

7.8 - Timestamping / dating system

"YOUSIGN SAS - QUALIFIED SEAL2 CA" produces a time stamp on all the archived elements.

See this chapter.

8 - Certificates and CRL profiles

8.1 - Certificates profiles

8.1.1 - Root CA certificate

Basic field	Value
Version	2

Basic field	Value
Serial number	Defined by PKI
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS - ROOT2 CA,OU=794513986, O=YOUSIGN SAS, L=CAEN,ST=CALVADOS,C=FR
Validity	20 years
Subject	CN=YOUSIGN SAS - ROOT2 CA, OU=794513986, O=YOUSIGN SAS, L=CAEN,ST=CALVADOS,C=FR
Key length	4096 bits

Extension field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	Hash sha1 of issuer field
Subject Key Identifier	Y	N	Hash sha1 of subject field
Key usage	Y	Y	certSign crlSign
CRL Distribution Points	Y	N	http://crl.yousign.fr/crl/yousignsasroot2ca.crl http://crl2.yousign.fr/crl/yousignsasroot2ca.crl http://crl3.yousign.fr/crl/yousignsasroot2ca.crl
Basic Constraints	Y	Y	CA:true Pathlength : any

8.1.2 - "YOUSIGN SAS - QUALIFIED SEAL2 CA"

Basic field	Value
Version	2
Serial number	Defined by PKI
Signature	SHA256WithRSA

Basic field	Value
Issuer	CN=YOUSIGN SAS - ROOT2 CA,OU=794513986, O=YOUSIGN SAS, L=CAEN,ST=CALVADOS,C=FR
Validity	10 years
Subject	CN=YOUSIGN SAS – QUALIFIED SEAL2 CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Key length	4096 bits

Extension field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	Hash sha1 of issuer field
Subject Key Identifier	Y	N	Hash sha1 of subject field
Key usage	Y	Y	certSign crlSign
CRL Distribution Points	Y	N	http://crl.yousign.fr/crl/yousignsasroot2ca.crl http://crl2.yousign.fr/crl/yousignsasroot2ca.crl http://crl3.yousign.fr/crl/yousignsasroot2ca.crl
Basic Constraints	Y	Y	CA:true Pathlength : any
Authority Information Access	Y	N	http://crl.yousign.fr/yousignsasroot2ca.crt http://crl2.yousign.fr/yousignsasroot2ca.crt http://crl3.yousign.fr/yousignsasroot2ca.crt

8.1.3 - Seal certificate

Basic field	Value
Version	2
Serial number	Defined by PKI

Basic field	Value
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS – QUALIFIED SEAL2 CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Validity	3 years
Subject	see this chapter
Key length	2048 bits

Extension field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	Hash sha1 of issuer field
Subject Key Identifier	Y	N	Hash sha1 of subject field
Key usage	Y	Y	digitalSignature
Extended Key Usage	Y	N	MS Document Signing Adobe PDF Signing
Certificate Policies	Y	N	1.2.250.1.302.1.13.1.0 URI: http://yousign.fr/fr/public/document
CRL Distribution Points	Y	N	http://crl.yousign.fr/crl/yousignsasqualifseal2ca.crl http://crl2.yousign.fr/crl/yousignsasqualifseal2ca.crl http://crl3.yousign.fr/crl/yousignsasqualifseal2ca.crl
Basic Constraints	Y	Y	CA: false

Extension field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Information Access	Y	N	CA certificate: http://crl.yousign.fr/yousignsasqualifseal2ca.crt http://crl2.yousign.fr/yousignsasqualifseal2ca.crt http://crl3.yousign.fr/yousignsasqualifseal2ca.crt OCSP service: http://ocsp.yousign.fr
qcStatements	Y	N	esi4- qcStatement-1 = id-etsi-qcsQcCompliance esi4- qcStatement-6 = id-etsi-qct-eseal

8.1.4 - OCSP certificate

Basic field	Value
Version	2
Serial number	Defined by PKI
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS – QUALIFIED SEAL2 CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Validity	5 years
Subject	CN=OCSP Service *N* Yousign QUALIFIED SEAL2 CA, SERIAL NUMBER=<*certificate generation timestamp*>, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR *N* is a number fixed by Yousign
Key length	2048 bits

Extension field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	Hash sha1 of issuer field
Subject Key Identifier	Y	N	Hash sha1 of subject field

Extension field	Mandatory (Y/N)	Critical (Y/N)	Value
Key usage	Y	Y	digitalSignature
Extended Key Usage	Y	N	id-kp-OCSPSigning
Certificate Policies	Y	N	1.2.250.1.302.1.14.1.0 URI: http://yousign.fr/fr/public/document
id-ocsp-nocheck	Y	N	NULL
CRL Distribution Points	Y	N	http://crl.yousign.fr/crl/yousignsasqualifseal2ca.crl http://crl2.yousign.fr/crl/yousignsasqualifseal2ca.crl http://crl3.yousign.fr/crl/yousignsasqualifseal2ca.crl
Basic Constraints	Y	Y	CA: false
Authority Information Access	Y	N	CA certificate: http://crl.yousign.fr/yousignsasqualifseal2ca.crt http://crl2.yousign.fr/yousignsasqualifseal2ca.crt http://crl3.yousign.fr/yousignsasqualifseal2ca.crt

8.2 - CRL profiles

Basic field	Value
Version	1
Signature	SHA256WithRSA
Issuer	CN=YOUSIGN SAS – QUALIFIED SEAL2 CA, OU=0002 794513986, O=YOUSIGN SAS, OI=NTRFR-794513986, C=FR
Validity	7 days

Basic field	Value
Revoked Certificates	Serial Number Revocation Date

Extension field	Mandatory (Y/N)	Critical (Y/N)	Value
Authority Key Identifier	Y	N	Hash sha1 of issuer field
CRL number	Y	Y	PKI defined sequence number

8.3 - OCSP responder

8.3.1 - OCSP request

OCSP requests accepted are those which respect the format described by RFC 6960. The OCSP service ignores the signature if it is present.

The expected requests are of the form:

Field	Comments	Attended value
Version	Request version format	0 (version 1)
requestorName	Name of the request's issuer	Empty or ignored
requestList • reqCert • singleRequestExtensions	List of certificate to check	One or more certificate identification number are accepted Extension values are ignored
requestExtensions	Extensions	Only the nonce extension is taken into account, others are ignored

Accepted fingerprint algorithms for certificate identifiers are SHA-1, SHA-256, SHA-384 and SHA-512.

8.3.2 - OCSP responses

OCSP responses accepted are those which respect the format described by RFC 6960. Responses are signed by the service unless an error has occurred (request rejected or processing failure).

The responses are of the form BasicOCSPResponse:

Field	Comments	Attended value
Version	Request version format	0 (version 1)
requestorID	Name of the OCSP responder	Hash sha1 of subject responder certificate field
producedAt	Response generation timestamp	Generation timestamp to the second
responsesList • certID • certStatus • revocationDate • thisUpdate	Status of certificate to check	Current status of the certificate (thisUpdate is the current date) revocationDate is provided but not the revocation reason.
responseExtensions	Extensions Archive CutOff	Nonce extension provide into the request is returned. CA validity start date

9 - Compliance audit and other assessments

Audits and evaluations concern, on the one hand, those carried out to obtain an eIDAS qualification certificate (according to a process described in ANSSI_PSCO) and, on the other hand, those that must be carried out by the CA to ensure that all of its PKI's requirements is in compliance with the commitments it makes and the practices it declares in this document.

The contents of this chapter only concerns audits and assessments of the CA's responsibility in order to ensure the proper functioning of its PKI.

9.1 - Frequency and/or circumstances of the assessments

A check for compliance with the CP at the time of the operational implementation of the system and when any significant modification is made, is conducted by means of an annual internal audit.

9.2 - Identities: qualification by the assessors

Audits are carried out either internally by Yousign staff, or by subcontractors. In all cases, Yousign undertakes to mandate people with the security skills required to audit and check the compliance of the system.

9.3 - Relationship between assessors and assessed entities

Assesors are either internal staff of Yousign, or auditors under a service contract.

9.4 - Scope of the assessments

Compliance checks point to a component of the PKI (specific checks) or to the entire architecture of the PKI (periodic checks) and aim to verify compliance with commitments and practices (operational procedures, resources, etc.) defined in this document.

To do this, the auditors will present for approval to the Technical Management Committee the list of components and procedures that will be audited.

9.5 - Actions taken as a result of the assessments

On completion of the compliance checks, the audit team provides the CA with an opinion rated "pass, fail or to be confirmed". According to the opinion delivered, the consequences of the check are as follows:

- In the case of a fail, and depending on the importance of the non-conformities, the audit team issues recommendations to the CA which may be the cessation (temporary or final) of activity, the revocation of the component's certificate, the revocation of all certificates issued since the last positive check, etc. It is up to the CA to decide which measures to apply and must comply with its internal security policies,
- In the case of a "to be confirmed", the audit team identifies and ranks the non-conformities; it is then up to the CA to propose a schedule for the resolution of the non-conformities; a re-test will then make it possible to remove the non-conformities identified,
- In the case of a pass, the CA confirms that the inspected component complies with the requirements of the CP.

10 - Other professional and legal problems

10.1 - Fees

10.1.1 - Certificate and renewal fees

Not applicable.

10.1.2 - Certificate access fees

Not applicable.

10.1.3 - CRL access fees

CRL access is free.

10.1.4 - Refund policy

Not applicable.

10.2 - Financial liability

10.2.1 - Insurance cover

CA applies reasonable levels of insurance and has taken out liability insurance for this purpose icovering its professional activity.

10.2.2 - Other resources

Not applicable.

10.2.3 - Cover and guarantee concerning the user entities

Not applicable.

10.3 - Confidentiality of professional data

10.3.1 - Scope of the confidential information

The information considered confidential is at least the following:

- The internal procedures of the CA,
- The private keys of the CA, components and certificates,
- The activation data associated with the CA and seal private keys,
- All the secrets of the PKI,
- The event logs of the PKI components,
- Registrations,
- The causes of revocation, unless expressly agreed to by the SCO.

10.3.2 - Information not classified as confidential

Not applicable.

10.3.3 - Responsibilities in terms of protection of confidential information

Yousign applies security procedures to guarantee the confidentiality of the information identified in this chapter.
Yousign undertakes to comply with the laws and regulations in force on French territory.

10.4 - Protection of personal data

10.4.1 - Personal data protection policy

Yousign undertakes to comply with the laws and regulations in force in France, in particular the General Data Protection Regulations (see GDPR).

10.4.2 - Personal information

The information considered personal is at least the following:

- The reasons for revoking seal certificates (which are considered confidential unless expressly agreed to by the SCO),
- The SCO registration,
- The activation data of the private key.

10.4.3 - Non-personal information

Not applicable.

10.4.4 - Liability in terms of personal data protection

Refer to the laws and regulations in force on French territory.

10.4.5 - Notification of and consent to use of personal data

In accordance with the laws and regulations in force on French territory, personal information provided by the SCO to the CA is not disclosed or transferred to a third party except in the following cases: prior consent of the SCO, judicial decision or other legal authorization.

10.4.6 - Conditions for disclosing personal information to the judicial or administrative authorities

Refer to the laws and regulations in force on French territory.

10.4.7 - Other circumstances for disclosing personal information

Not applicable.

10.5 - Intellectual and industrial property rights

All intellectual property rights held by Yousign are protected by the laws and regulations in force.

Users have no intellectual property rights on all elements implemented by Yousign to ensure its PKI functions.

Violation of trademarks and services, logos and models, distinctive signs, copyright (for example: software, web pages, databases, original texts, ...) is penalized by the Code of Intellectual property.

Yousign holds all intellectual property rights on the personal information contained in the seal certificates issued by the CA and for which Yousign is the owner.

10.6 - Contractual interpretations and guarantees

The obligations common to the components of the PKI are as follows:

- Protect and guarantee integrity and confidentiality of their secret and / or private keys,
- Respect the usage purpose of their cryptographic keys (public, private and / or secret) during their issue and with tools specified in the requirements set by in this CP and the documents resulting therefrom,
- Respect and apply the practices specified in the document and the responsibilities linked,
- Accept the audit compliance appointed by the CA (see this chapter),
- Respect the agreements or contracts which link parties together or to the SCO,
- Document their internal operating procedures,
- Implement the means (technical and organizational) necessary for the performance of the services to which they undertake under conditions by guaranteeing quality and safety.

10.6.1 - Certificate Authority

Obligations of Yousign's CA are as follows:

- Validate and publish the CP,
- Declare the conformity of the certificates issued under conditions of this CP,
- Ensure compliance with all security principles by the all components of the PKI, and related controls.

Unless it can be shown that CA has not committed any intentional fault or negligence, Yousign is responsible for damage caused to users if:

- The information contained in the certificate does not correspond to the registration data,

- Yousign did not register the revocation of a certificate, and did not publish this information in accordance with its commitments.

10.6.2 - Registration Authority

See this chapter.

10.6.3 - SCO

SCO are responsible to:

- Provide accurate and up-to-date information when requesting or renewing the certificate,
- Protect their authentication data,
- Respect the Terms and conditions of use of the Yousign sealing service,
- Inform the CA of any modification concerning the information contained in its certificate,
- Request the renewal of their certificates with a reasonable time before their expirations,
- Make, without delay, a revocation request of their certificates to Yousign in the event of compromise or suspicion of compromise of their authentication data.

10.6.4 - Users

Certificate users must:

- Check and respect the certificate purpose,
- For each certificate in the certification chain, from the seal certificate to the root certificate, verify the digital signature of the CA issuing the corresponding certificate and check the validity of this certificate (validity dates, revocation status),
- Check and comply with the obligations of certificate users described in this CP.

10.6.5 - Other parties

Not applicable.

10.7 - Limit of warranty

Not applicable.

10.8 - Limit of liability

Yousign may not be deemed liable for the unauthorised or non-compliant use of activation data, the certificates, CRLs and any other equipment or software provided.

Yousign rejects liability for errors or inaccuracies in the information contained in the certificates, when these errors or inaccuracies result directly from incorrect information sent by the SCO.

In addition, tothe limitations of French law in force, Yousign cannot be held responsible for:

- Financial loss,
- Data loss,
- Indirect damage linked to the use of a certificate,
- Other damage.

In this context, Yousign's liability will be limited, all generative facts and for all damages combined, to the amount paid to Yousign for access to the seal service, within limits of law in force.

10.9 - Indemnities

Not applicable.

10.10 - Termination and early end of validity of the CP

10.10.1 - Validity period

This document is applicable until the expiry of the last certificate issued under the terms of this CP. A new version of the CP becomes applicable on a date indicated in the description document published by Yousign.

10.10.2 - Early end of validity

The application of the CP can be interrupted in the event of the end of the CA's life (see this chapter).

10.10.3 - Effects of the end of validity and clauses that remain applicable

Not applicable.

10.11 - Amendments to the CP

10.11.1 - Amendment procedures

10.11.1.1 - Decision

The updating of this CP is done under the control of the Technical Management Committee. The events that may require an evolution of the document can be the following:

- Major evolution of the registration process of SCO or management of certificates,
- Integration of new regulatory conditions applicable to the service,
- Major modification of the technical architecture,
- End or loss of certification or qualification from the Certification Authority.

10.11.1.2 - Operational procedure

The CP amendment procedure includes the following actions:

- Organization of a Yousign Technical Management Committee,
- Analysis of the scope and impacts of the modifications,
- Contact with the certified auditor body that issued the CA compliance attestation, and if necessary the supervisory body ANSSI, to ensure the admissibility of the changes made and the conditions to maintain the certifications and qualifications obtained,
- Identification of the people involved to make the changes,
- Implementation (technical, organizational, legal) of the changes decided,
- Updates of associated documents,
- Update the OID if necessary,
- Make of an internal audit, and if necessary external, on the parties affected by the modifications,
- Publication of associated information (see this chapter),
- Commissioning of the modifications made,
- Archiving of old versions of documents (Policy, Terms and conditions of Use, etc.).

10.11.2 - Amendment process and reporting period

When any significant change affecting the CP, Yousign will inform the SCO through a press release published through its website. If necessary, communication by post can be made.

10.11.3 - Circumstances in which the OID must be changed

The OID of the CP being registered into the certificates which CA issues, any evolution of this CP having a major impact on the certificates already issued (for example, increased requirements in terms of registration of SCO, which cannot therefore apply to certificates already issued) must result in an evolution of the OID, so that users can clearly distinguish which certificates correspond to which requirements.

In particular, the OID of the CP must evolve when a major change (and which will be indicated as such, in particular by an evolution of the OID of this CP) intervenes in the requirements of this CP applicable to the family of certificates considered.

10.12 - Provisions concerning conflict resolution

In the event of a dispute between the parties arising from the interpretation, application and / or execution of the contract and in the absence of an agreement between the above parties, exclusive jurisdiction is attributed to the Commercial Court of Caen.

10.13 - Jurisdiction

See this chapter.

10.14 - Compliance with legislation and regulations

The laws and regulations applicable to this CP are, in particular, those indicated in this chapter.

10.15 - Miscellaneous provisions

10.15.1 - Overall agreement

Not applicable.

10.15.2 - Transfer of activities

Not applicable.

10.15.3 - Consequences of a non-valid clause

Not applicable.

10.15.4 - Application and cancellation

Not applicable.

10.15.5 - Force majeure

All situations normally deemed to constitute a case of force majeure by the French courts are considered as such under the terms of this document, especially an unpredictable, unavoidable and overwhelming event.

10.15.6 - Other provisions

Not applicable.

11 - Annex 1: Security requirements of the CA cryptographic module

11.1 - Security objectives requirements

The cryptographic module, used by the CA to generate and implement its signature keys (for the generation of electronic certificates, CRL/ARL), as well as, for the generation of seal key pairs, meets the requirements of following security:

- Guarantee that the generation of the seal key pairs is carried out exclusively by authorized users and guarantee the cryptographic robustness of the generated key pairs,
- Ensure the confidentiality of private keys and the integrity of private and public keys,
- Ensure the confidentiality and integrity of the CA's private signature keys throughout their life cycle, and ensure their safe destruction at the end of their life,
- Is able to identify and authenticate its users,
- Limit access to its services according to the user and the role assigned to him,
- Is capable of carrying out a series of tests to check that it is operating correctly and to enter a safe state if it detects an error,
- Allow the creation of a secure electronic signature, to sign the certificates generated by the CA, which does not reveal the CA's private keys and which cannot be falsified without knowledge of these private keys,
- If a backup and restore function for the CA's private keys is offered, guarantee the confidentiality and integrity of the backed up data and require at least double control of the backup and restore operations,
- If the cryptographic module of the CA detects attempts at physical alteration, this will enter a safe state.

The cryptographic module is deployed according to the recommendations of its security target for the qualification of the material. Communication with the cryptographic module is carried out on an encrypted channel after mutual authentication.

11.2 - Certification requirements

The cryptographic module used by Yousign is qualified to the high level by the ANSSI.

12 - Annex 2: Security requirements of the seal creation device

12.1 - Security objectives requirements

The Yousign seal creation device meets the following security requirements:

- Guarantee that the generation of the seal key pairs is carried out exclusively by authorized users and guarantee the cryptographic robustness of the generated key pairs,
- Detect anomalies during the initialization, personalization and operation phases and have secure means for destroying the private key in the event of re-generation of the private key,

- Ensure the confidentiality and integrity of the private keys,
- Ensure the cryptograhic association between private and public keys,
- Is capable of carrying out a series of tests to check that it is operating correctly and to enter a safe state if it detects an error,
- Allow the creation of a secure seal certificate which does not reveal the seal private keys and which cannot be falsified without knowledge of these private keys,
- Ensure the seal function for the legitimate SCO only and protect the private key against any use by third parties,
- Guarantee the authenticity and integrity of the public key when it is exported from the device.

12.2 - Certification requirements

The cryptographic module used by Yousign is qualified to the high level by the ANSSI.