Certificate and timestamp authority

Terms and conditions YOUSIGN SAS - SIGN2 CA

Export at 23/04/2020

Creator : Sylvain Rossi - 06/03/2020

last change : Sylvain Rossi - 06/03/2020

Diffusion :

Summary:

1 - Versions

Version	Description	Date	Author
1.0.0	Initial version	06 Mar 2020	Sylvain Rossi

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
ICA	Intermediate Certificate Authority
IDS	Intrusion Detection System
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PDS	Public Disclosure Statements
PKI	Public Key Infrastructure

Acronym	Signification
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
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

Terms	Signification
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
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.

Terms	Signification
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 Public Disclosure Statements (PDS) 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.

2.3 - Document identification

This document corresponds to the Public Disclosure Statements (PDS) of the Certification Authority "YOUSIGN SAS - QUALIFIED SEAL2 CA" whose the CP's identifications is the foillow: **2.250.1.302.1.13.1.0**.

Other, more explicit elements (name, version number, date of update) also make it possible to identify it.

3 - Terms and conditions

These Terms and conditions are based on the model provided for in appendix A of standard EN 319411-1 (version 1.1.1).

3.1 - 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

3.2 - Type of certificates, management certificates procedures, restriction of usage

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"

These are qualified seal certificates enabling sealing operations to be carried out using electronic seals.

These certificates are issued to a Seal Certificate Officer (SCO) who is a natural person representative of the Subscriber to the Yousign seal service and who is responsible for the management and implementation of these certificates.

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

Attribute	Description	Include
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.

The SCO is in charge of configuring or having the configuration allowing access to the infrastructure made available by Yousign. Each access to the seal certificate is authenticated.

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.

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.

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.

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.

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.

Please ask your Confluence administrator to update the license for the MultiExcerpt App for Confluence **.**
Admin Info: The error is: license EXPIRED
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.

Please ask your Confluence administrator to update the license for the MultiExcerpt App for Confluence **.**
Admin Info: The error is: license EXPIRED

3.3 - 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.

3.4 - Subscribers obligations

Subscriber takes into account the following requirements:

- Obligation to provide up-to-date and valid identity data during the registration process,
- Implement the signing certificate respecting the limits of liability in force and in particular to ensure the confidentiality of authentication and activation data allowing the server under the responsibility of the SCO to access the electronic seal service,
- Obligation to notify the CA when one of the following causes of revocation is established:

  - the information contained in the certificate is no longer in accordance with the identity or the intended use in the certificate, this before the normal expiration of the certificate,
  - an error (intentional or not) was detected in the registration dossier,
  - the private key is suspected of being compromised, is compromised or is lost (possibly the associated activation data),
  - the authentication and activation data to authorize access to the sealed certificate have been compromised or suspected of being compromised,
- Obligation to check the status of the certificate issued through the CRL published by the CA and the OCSP service implemented,
- Use the certificate under the terms and conditions of use provided for by the CA and included in these Terms

3.5 - CA obligations

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.

3.6 - Checking of certificate status

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 the CP in force.

CA makes available to users an updated CRL, published on the Internet on the site:

- http://crl.yousign.fr/crl/yousignsasqualifseal2ca.crl
- http://crl2.yousign.fr/crl/yousignsasqualifseal2ca.crl
- http://crl3.yousign.fr/crl/yousignsasqualifseal2ca.crl

Yousign also implements an OCSP service accessible at the following address: http://ocsp.yousign.fr

CRLs include the X.509 "ExpiredCertsOnCRL" extension and maintain all serial number of revoked certificates, even those who have expired.

OCSP responder uses the ArchiveCutOff extension as specified in IETF RFC 6960, with the archiveCutOff date set to start validity date of the CA's certificate and maintain the ocsp response after the CA's termination.

If the OCSP's request concerns a serial number not issued by the corresponding CA, OCSP server answers the status "unknown". If the serial number is issued by the corresponding CA, OCSP answers are compliant with IETF RFC 6960.

Before the CA's termination, Yousign will provide:

- A last CRL containing a nextUptade date to 99991231235959Z,

- All OCSP responses pre-generated for each certificate issued and containing an end validity date to 99991231235959Z

If Yousign terminates the activity of its CA, it undertakes to keep available the CRLs and the pre-generated OCSP responses.

3.7 - Limits of waranty and responsabilities

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.

3.8 - Certificate Policies

CP describing the requirements that the CA has to respect is published on the following website: http://yousign.fr/fr/public/document and is identified by the followin OID: 1.2.250.1.302.1.13.1.0.

3.9 - Confidentiality of professional data

3.9.1 - 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.

3.9.2 - Information not classified as confidential

Not applicable.

3.9.3 - 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.

3.10 - Insurance cover

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

3.11 - 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.

3.12 - Audit and certifications

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

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

Certificates issued contain the following qualified fields:

- esi4- qcStatement-1 = id-etsi-qcsQcCompliance
- esi4- qcStatement-6 = id-etsi-qct-eseal