General Terms and Conditions of Use of the server seal certificates issued by the YOUSIGN SAS – SIGN3 CA

v1.0.2 | Distribution: C1 - Public

VERSION HISTORY			
Version	**Purpose of the change**	**Date**	**Author**
1.0.2	Addition of the PKI Disclosure Statements (section general presentation) Addition of the qualified seal OID (section document identification) Update of the definition of the subscriber (section definitions) Addition of a paragraph on the CA's obligations (section CA obligations) Addition of the selection criteria for cryptographic modules for the qualified seal OID (section applicable audits and references)	May 14, 2025	Tony BELOT Tony DUFOUR
1.0.1	Changes to the obligations regarding certificate checking by users (sections obligations of the subject entity and of the legal representative and obligations of the subscriber and of the RCC)	Jun 28, 2024	Jean VERRONS
1.0.0	Addition of the definition of the term "subscriber" (section definitions) Introduction of the term "subject entity" and of the possible difference between that entity and the subscriber (sections definitions, type of certificates issued, conditions for obtaining a certificate, usage limitations, obligations of the subject entity and of the legal representative, obligations of the subscriber and of the RCC and obligations regarding certificate checking by users) Replacement of the notion of "holder" with more precise terms designating either the subscriber or its legal representative, or	Jul 13, 2023	Tony Belot

VERSION HISTORY			
Version	**Purpose of the change**	**Date**	**Author**
	the subject entity or the RCC (sections conditions for obtaining a certificate, obligations of the subject entity and of the legal representative and obligations of the subscriber and of the RCC) Clarification of the responsibilities of the subscriber (and of its RCC) and of the subject entity (and of its legal representative), as well as of their relationships (sections general presentation, obligations of the subject entity and of the legal representative, obligations of the subscriber and of the RCC, limitation of liability, personal data management and evidence agreement) Update of the links to the public documentation (sections type of certificates issued and reference documents) Alignment of the purpose of the certificates between the GTCU and the CP (section purpose of the certificates) Move of the arrangements for managing, storing, protecting and proving possession of the private key into the CP (section conditions for obtaining a certificate) Change of the term “server” to “application service” (section obligations of the subscriber and of the RCC) Move of the URLs to the CRLs and ARL into the CP (sections obligations regarding certificate checking by users and certificate status checking) Minor syntactic and formatting corrections		

VERSION HISTORY			
Version	**Purpose of the change**	**Date**	**Author**
0.0.1	Creation of the document, generated from the General Terms and Conditions of Use of the CA - YOUSIGN SAS - SIGN2 CA for seal certificates, version 1.0.1, with the following changes: • Change of the references to the Sign2 CA to Sign3, update of the OID and of the CRL addresses • Completion of the acronyms and addition of translations where applicable (section acronyms) • Addition of a section for the definitions (section definitions) • Clarification regarding the identification of the document (section document identification) • Addition of the applicable ETSI standard and certificate level (section document identification) • Update of the CA contact address (section general terms and conditions of use, subsection contact details of the Certification Authority) • Removal of the example of use of the certificates for a simple electronic signature by a natural person (section general terms and conditions of use, subsection purpose of the certificates) • Clarification and simplification of the roles of RCC and legal representative, move of the content of the registration record and of the accepted supporting documents into the CP (section general terms and conditions of use, subsection conditions for obtaining a certificate) • Addition of the systematic communication of the certificate to	Jun 23, 2023	Tony Belot

VERSION HISTORY			
Version	**Purpose of the change**	**Date**	**Author**
	the holder following its generation and removal of the possibility of subsequent requests (section general terms and conditions of use, subsection conditions for obtaining a certificate) • Clarification of the arrangements for storing, using and protecting private keys (section general terms and conditions of use, subsection conditions for obtaining a certificate) • Removal of the revocation channels by post and telephone, move of the detail of the revocation process into the CP (section general terms and conditions of use, subsection revocation arrangements) • Clarification of the service authorised to use the certificate (section general terms and conditions of use, subsection usage limitations) • Strengthening of the holder's obligations and clarification of the lead time required for certificate renewal operations (section general terms and conditions of use, subsection holder obligations) • Clarification of the limit of the exemption from damages (section general terms and conditions of use, subsection limitation of liability) • Removal of the subsection on compensation conditions (section general terms and conditions of use) • Removal of the reference to the CPS (section general terms and conditions of use, subsections		

VERSION HISTORY			
Version	**Purpose of the change**	**Date**	**Author**
	reference documents and applicable audits and references) • Update of the competent Court from Caen to Paris (section general terms and conditions of use, subsection applicable law and dispute resolution) • Review of the subsection content and addition of a pointer to the online Privacy Policy (section general terms and conditions of use, subsection personal data management) • Removal of the compliance check and clarification regarding the audit carried out regularly (section general terms and conditions of use, subsection applicable audits and references) • Various changes making the document easier to read		

Table of contents

1. Introduction

1.1. General presentation

This document sets out the GTCU of the server seal certificates issued by the Certification Authority `YOUSIGN SAS - SIGN3 CA`.

These GTCU are accepted by the subscriber and the subject entity during the request process. This document sets out the certificate management arrangements as well as the commitments and obligations of the various parties.

This document complies with the PKI Disclosure Statements template within the meaning of standard EN 319 411-1.

1.2. Document identification

This document is referenced by its title and its version number. This number may evolve independently of changes to the OID of the Certificate Policy.

This version of the GTCU applies to the following OIDs:

- `1.2.250.1.302.1.18.1.0` for certificates at LCP level of standard ETSI 319 411-1, used for server seal certificates issued for a legal person;
- `1.2.250.1.302.1.24.1.0` for qualified certificates at QCP-l level of standard ETSI 319 411-2 used for server seal certificates issued for the legal person Yousign SAS.

Items specific to a policy are preceded by the OID of that policy in square brackets. Several OIDs may be specified, in which case they are listed one after the other. Where an item applies to all the OIDs described in this document, either the tag `[all OIDs]` is used, or no tag is specified.

1.3. Acronyms

Acronym	Meaning	Translation
CA	Certification Authority	-
RA	Registration Authority	-
GTCU	General Terms and Conditions of Use	-
DN	Distinguished Name	-
CPS	Certification Practice Statement	-
DPO	Data Protection Officer	-
PKI	Public Key Infrastructure	-
ARL	Authority Revocation List	-
LCP	Lightweight Certificate Policy	-
CRL	Certificate Revocation List	-
OCSP	Online Certificate Status Protocol	-
OID	Object Identifier	-
CP	Certificate Policy	-
RCC	Responsable du Certificat de Cachet	Seal Certificate Manager
URL	Uniform Resource Locator	-

1.4. Definitions

Term	Meaning
Subscriber	[1.2.250.1.302.1.18.1.0] The subscriber is a legal person that is a customer of the company Yousign. A contractual relationship exists between the subscriber and the company Yousign. [1.2.250.1.302.1.24.1.0] The subscriber is the legal person Yousign SAS.

Term	Meaning
Subject entity	The subject entity is the legal person for which the certificate has been issued. That legal person is represented by a legal representative registered by the RA. The DN of the certificate makes it possible to identify that entity.
Responsable du Certificat de Cachet	The RCC is the natural person responsible for protecting the activation data of the private key corresponding to the certificate of the subject entity. By default, the RCC is a legal officer of the subject entity. Alternatively, the RCC may be a person appointed by a legal representative of the subject entity. In the latter case, the RCC may report hierarchically to the subject entity, or belong to another entity with which a contractual or regulatory relationship exists. The RCC may change during the validity period of the certificate (departure of the RCC from the entity, change of assignment and responsibilities within the entity, etc.) without calling into question the validity of the certificate.
User	A user is a natural or legal person having access to a signed file whose signature was generated by the private key of a certificate issued by the CA covered by these GTCU. It should be noted that no direct relationship exists between the company Yousign and a user.

2. General Terms and Conditions of Use

Contact details of the Certification Authority	Yousign SAS Yousign CA management 507, rue de Suède et de Norvège 14000 Caen authority@yousign.com
Type of certificates issued	The GTCU apply to the certificates specified in the paragraph document identification. The certificates are issued to an RCC who is a formal representative of the Subscriber to the Yousign service and

	who is responsible for the management and deployment of these certificates. The certificates issued by the CA are server seal certificates, issued on behalf of a subject entity identified in the certificate. The certificates are issued through the following certification chain: • Root CA: `YOUSIGN SAS - ROOT2 CA` • Issuing CA: `YOUSIGN SAS - SIGN3 CA` The certificates of the certification chain are available at the following address https://yousign.com/fr-fr/documentation-technique-des-certifications.
Purpose of the certificates	The certificates issued by the CA are server seal certificates making it possible to guarantee the authenticity and integrity of data.
Conditions for obtaining a certificate	The RCC must submit a formal request to the RA. The registration record is described in the CP. The certificate produced is communicated to the RCC following its generation and remains subsequently accessible in each signed document. Possession of the private key must be proven in accordance with the method described in the CP.
Renewal arrangements	The renewal process corresponds to a new certificate request.
Revocation arrangements	A request for revocation of a certificate must be made by email, to the address given in the section "Contact details of the Certification Authority". A revocation request form must be completed and signed by the requester. The process for handling the revocation request is documented in the CP.
Usage limitations	The use of a server private key and of the associated certificate is strictly reserved for the seal creation service stipulated in the registration record. The certificates have a validity period of three (3) years. The

	corresponding private keys are destroyed at the end of that period with no possibility of recovery. Yousign retains for seventeen (17) years the logs and audit trails relating to the issuance and use of the private keys associated with the certificates.

CA obligations	`[all OIDs]`
	The CA is responsible for:
	● the validation and publication of the CP and of these GTCU of the CA;
	● compliance with the CP and with these GTCU.
	
	`[1.2.250.1.302.1.24.1.0]`
	The CA is responsible for:
	● in the event of a major incident (loss, compromise or theft of the private key of the certificates, for example), reporting the incident to ANSSI within 24 hours.

Obligations of the subject entity and of the legal representative	The subject entity, represented by its legal representative, shall comply with the following requirements: ● have a contractual, hierarchical or regulatory relationship with the subscriber; ● undertake to provide the information and supporting documents required in the registration record, up to date and valid; ● check that the content of the certificate provided is correct; ● deploy the certificate only under the conditions of use laid down by the CP and reproduced in these GTCU, complying with the usage limitations; ● consent to any successful authentication with the electronic seal service being presumed to have been carried out with the agreement of the RCC and of the subject entity; ● undertake to notify the CA without undue delay when one of the following grounds for revocation is established: ○ an error (whether intentional or not) has been detected in the registration record or in the certificate; o the information appearing in the certificate no longer complies with the identity or the intended

	use stated in the certificate, this before the normal expiry of the certificate; ○ the activation data is suspected of compromise, compromised, lost, stolen or revoked. • refrain from using the certificate as soon as the activation data, the private key or the CA is suspected of compromise, compromised, lost, stolen or revoked; • undertake to check the status of the certificate issued through the CRLs published by the CA; • consent to the retention by the RA and the CA of the information in the registration record and in the management of the keys and of the certificate.
Obligations of the subscriber and of the RCC	The subscriber, represented by the RCC, shall comply with the following requirements: • have a contractual, hierarchical or regulatory relationship with the subject entity; • undertake to obtain the formal agreement of a legal representative of the subject entity prior to any certificate request; • undertake to provide the information and supporting documents required in the registration record, up to date and valid; • check that the content of the certificate provided is correct; • tacitly accept the certificate issued by the CA as soon as it is provided by the RA; • ensure the confidentiality of the activation items enabling the application service to access the electronic seal service; • consent to any successful authentication with the electronic seal service being presumed to have been carried out with the agreement of the RCC and of the subject entity; • use the certificate only with the agreement of the subject entity, within the framework agreed with the subject entity and within the usage limitations laid down by the GTCU; • undertake to notify the CA without undue delay when one of the following grounds for revocation is established: ○ an error (whether intentional or not) has been detected in the registration record or in the certificate;

	○ the information appearing in the certificate no longer complies with the identity or the intended use stated in the certificate, this before the normal expiry of the certificate; ○ the activation data is suspected of compromise, compromised, lost, stolen or revoked. ● refrain from using the certificate as soon as the activation data, the private key or the CA is suspected of compromise, compromised, lost, stolen or revoked; ● undertake to notify the RA prior to any invalidation of the role of the known RCC; ● undertake to check the status of the certificate issued through the CRLs published by the CA; ● request the renewal of the certificate at least three (3) months before its expiry; ● consent to the retention by the RA and the CA of the information in the registration record and in the management of the keys and of the certificate.
Obligations regarding certificate checking by users	Users of the certificates must: ● check and comply with the use for which a certificate was issued; ● for each certificate of the certification chain, from the certificate of the subject entity up to the CA YOUSIGN SAS – ROOT2 CA, verify the digital signature of the CA issuing the certificate concerned and check the validity of that certificate (validity dates, revocation status); ● check and comply with the obligations of certificate users set out in the CP. The CRLs are published at the URLs given in the certificates and restated in the CP.
Certificate status checking	Should the CA be revoked, for example following a compromise of its private key, the revocation information is made available in an ARL published at the URLs given in the certificates and restated in the CP.
Limitation of liability	Yousign may not be held liable for any unauthorised or non-compliant use of the authentication data, the certificates, the CRLs, or any other equipment or software made available. Yousign disclaims liability for any damage resulting from errors or inaccuracies affecting the information contained in the certificates, where such errors or inaccuracies result

	directly from the erroneous nature of the information provided by the subscriber or the subject entity. In any event, and to the strictest extent permitted by applicable law, Yousign shall not be liable for the payment of damages of any nature whatsoever, whether direct, material, commercial, financial or non-material, arising from the performance hereof.
Reference documents	The Certificate Policy of the CA `YOUSIGN SAS - SIGN3 CA` for server seals is available at the following address: https://yousign.com/fr-fr/documentation-technique-des-certifications.
Language	These GTCU have been drawn up in several languages, including French. The language of interpretation shall be French in the event of any contradiction or dispute as to the meaning of a term or a provision.
Applicable law and dispute resolution	These GTCU are governed by and interpreted in accordance with French law. In the event of a dispute between the parties arising from the interpretation, application and/or performance of the contract, and failing an amicable agreement between the aforementioned parties, exclusive jurisdiction is granted to the courts of Paris.
Personal data management	Yousign undertakes to comply with the applicable laws and regulations concerning the management of personal data, in particular European Regulation No 2016/679 of 27 April 2016 known as the "General Data Protection Regulation" (GDPR). The subscriber and the subject entity are informed that the issuance of electronic certificates involves the processing of personal data by Yousign. They are invited to consult the Privacy Policy for further information on how their personal data is processed and on how to exercise their rights.
Applicable audits and references	`[all OIDs]` Yousign operates a Yousign Technical Steering Committee. A technical security audit is carried out at least annually. The audits are carried out internally by Yousign staff or in the form of an engagement with information systems security

	specialists having recognised expertise in the field of information systems security. [1.2.250.1.302.1.24.1.0] The cryptographic module used by Yousign is qualified by ANSSI. The certificates comply with standard ETSI 319 411-2 at QCP-l level and are qualified, within the meaning of the eIDAS Regulation, by ANSSI.
Evidence agreement	For each electronic seal applied, Yousign, the subscriber and the subject entity agree that the items contained in: ● the registration record, such as: ○ the identification items of the subscriber and of its RCC; ○ the identification items of the subject entity and of its legal representative; ○ the supporting documents provided; ● the evidence record, such as: ○ the processes used to apply the electronic seal to the documents (authentication process, for example); ○ the electronic seal certificate; ○ the time-stamping items; ○ a set of computer logs; shall be admissible before the courts and shall constitute evidence of the data and items they contain as well as of the authentication processes they express. The registration record and the evidence record will be archived and time-stamped by Yousign.