yousign

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

v1.0.0 | Distribution: C1 – Public

VERSION HISTORY			
Version	**Purpose of the modification**	**Date**	**Author**
1.0.0	Addition of the definition of the term 'subscriber' (definitions section) Introduction of the term 'subject entity' and the possible difference between that entity and the subscriber (sections on definitions, type of certificates issued, how to obtain, limits on use, obligations of the subject entity and the authorised representative, obligations of the subscriber and the SCM and obligations in relation to the verification of certificates by users) Replacement of the notion of 'holder' by more precise terms designating either the subscriber or its lawfully appointed representative or the subject entity or the SCM (sections on how to obtain, obligations of the subject entity and the authorised representative and obligations of the subscriber and the SCM) Clarification of the responsibilities of the subscriber (and its SCM) and the subject entity (and its lawfully appointed representative) and their relationship (sections on general presentation, obligations of the subject entity and the authorised representative, obligations of the subscriber and the SCM, limit on liability, management of personal data and agreement on proof) Updating of links to public documentation (type of certificates issued and documentary references sections) Alignment of the purpose of certificates between the GCU and the CP (purpose of the certificates section) Moving the management, storage, protection and proof of possession of the	13 juil. 2023	Tony Belot

VERSION HISTORY			
Version	**Purpose of the modification**	**Date**	**Author**
	private key in the CP (how to obtain section) Change of the term ‘server’ to ‘application service’ (obligations of the subscriber and the SCM section) Relocation of URLs to CRLs and RCACLs in the CP (sections on obligations in relation to the verification of certificates by users and verification of certificate status) Minor syntax and formatting corrections		
0.01	Creation of the document, generated from the General Conditions of Use for the Yousign S.A.S. - Sign2 Certification Authority (CA) for seal certificates, version 1.0.1, with the following modifications: ● Modification of Sign2 CA references for Sign3, update of Object Identifier (OID) and CRL addresses ● Acronyms completed and translations added where necessary (acronyms section) ● Addition of a section for definitions (definitions section) ● Details of document identification (document identification section) ● Addition of the applicable ETSI standard and certificate level (document identification section) ● Update of the CA contact address (in the general conditions of use section under the heading Certification Authority contact) ● Deletion of the example of the use of certificates for a simple electronic signature by an individual (in the general conditions of use section under the purpose of certificates heading) ● Clarification and simplification of the roles of SCM and legal manager, relocation of the content of the	23 juin 2023	Tony Belot

VERSION HISTORY			
Version	**Purpose of the modification**	**Date**	**Author**
	registration file and the supporting documents accepted in the CP (general conditions of use section under the how to obtain heading) ● Addition of systematic communication of the certificate to the holder following its generation and deletion of the possibility of subsequent requests (general conditions of use section under the how to obtain heading) ● Clarification of the terms and conditions for storing, using and protecting private keys (general conditions of use section under the how to obtain heading) ● Removal of channels for revocation by letter and telephone, relocation of details of revocation process moved in the CP (general conditions of use section under the revocation conditions heading) ● Clarification of the service authorised to use the certificate (general conditions of use section under the limits of use heading) ● Reinforcement of the holder's obligations and clarification of the deadline for renewing certificates (general conditions of use section under the holder obligations heading) ● Clarification of the limit of exemption from damages and interest (general conditions of use section under the limitation of liability heading) ● Removal of the heading on compensation conditions (general conditions of use section) ● Removal of the reference to the DCP (general conditions of use section under the documentary references and applicable audits and references headings)		

VERSION HISTORY			
Version	**Purpose of the modification**	**Date**	**Author**
	• Update of court jurisdiction from Caen to Paris (general conditions of use section under the applicable law and dispute resolution heading) • Review of the content of the heading and addition of a pointer to the online Privacy Policy (general conditions of use section under the personal data management heading) • Removal of the compliance check and clarification of the audit carried out on a regular basis (general conditions of use section under the applicable audits and references heading) • Various changes to make the document easier to read		

Table of contents

1. Introduction

1.1. General presentation

This document defines the General Conditions of Use (GCU) of server seal certificates issued by the Certification Authority `YOUSIGN SAS - SIGN3 CA`.

These GCU are accepted by the subscriber and the subject entity during the request process. This document sets out the terms and conditions for managing certificates and the commitments and obligations of the various parties.

1.2. Document identification

This document is referenced by its title and version number. This number is subject to change independently of changes to the OID in the Certification Policy.

This version of the GCU applies to OID `1.2.250.1.302.1.18.1.0` for ETSI standard 319 411-1 LCP level certificates that are used in the context of seal certificates issued to a legal entity.

1.3. Acronyms

Acronym	Meaning
CA	Certification Authority
CP	Certification Policy
CRL	Certificates Revoked List
DCP	Declaration of Certification Practices
DN	Distinguished Name
DPO	Data Protection Officer
GCU	General Conditions of Use
KMI	Key Management Infrastructure

Acronym	Meaning
LCP	Lightweight Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object Identifier
RA	Registration Authority
RCACL	Revoked Certification Authority Certificates List
SCM	Seal Certificate Manager
URL	Uniform Resource Locator

1.4. Definitions

Term	Meaning
Seal Certificate Manager	The Seal Certificate Manager is the individual who is responsible for the protection of the private key activation data corresponding to the certificate of the subject entity. The SCM is, by default, an authorised representative of the subject entity. Alternatively, he can be a person nominated by the authorised representative of the subject entity. In the latter situation, the SM may have a hierarchical link with the subject entity or be attached to another entity with which a contractual or regulatory link exists. The SCM may change during the validity of the certificate (departure of the SCM from the entity, change of role and responsibilities within the entity, etc) without affecting the validity of the certificate.
Subject entity	The subject entity is the legal entity for which the certificate has been issued. Such a legal entity is represented by an authorised representative, registered by the RA. The DN of the certificate enables that entity to be identified.

Term	Meaning
Subscriber	The subscriber is a legal entity customer of Yousign. A contractual link exists between the subscriber and Yousign.
User	A user is an individual or legal entity with access to a signed file whose signature has been generated by the private key of a certificate issued by the CA covered by these GCU. Please note that there is no direct link between Yousign and a user.

2. General conditions of use

Contact details for the Certification Authority	Yousign S.A.S. Yousign CA Management 507 Rue de Suède et de Norvège 14000 Caen authority@yousign.com
Type of certificates issued	The GCU applies to the certificates specified in the document identification paragraph. The certificates are issued to an SCM, who is a formal representative of the Subscriber to the Yousign service and who is responsible for managing and implementing these certificates. Certificates issued by the CA are server seal certificates that are issued on behalf of a subject entity that is identified in the certificate.. Certificates are issued through the following certification chain: ● Root CA: Yousign S.A.S. - Root2 CA ● Issuing CA: Yousign S.A.S. - Sign3 CA Certificates for the certification chain are available at the following address https://yousign.com/technical-documentation-of-certifications.
Purpose of the certificates	The certificates issued by the CA are server seal certificates guaranteeing the authenticity and integrity of the data.

How to obtain	The SCM must make a formal request to the RA. The registration documents are described in the CP. The certificate produced is sent to the SCM once it has been generated and subsequently remains accessible in each signed document. The possession of the private key must be proved in compliance with the method described in the CP.
Renewal procedure	The renewal process corresponds to a new certificate application.
Revocation procedure	A certificate revocation request must be sent by email to the address given in the Certification Authority's contact details section. A revocation request form must be completed and signed by the requesting person. The revocation request processing procedure is documented in the CP .
Limits on use	The use of a server private key and the associated certificate is strictly reserved for the seal creation service stipulated in the registration documents. The certificates are valid for three (3) years. The corresponding private keys are destroyed at the end of that period with no possibility of recovery. Yousign keeps the logs and traces relating to the issuing and use of the private keys associated with certificates for seventeen (17) years.
Obligations of the subject entity and the authorised representative	The subject entity, represented by its lawfully appointed representative, takes the following requirements into account, namely it: ● has a contractual, hierarchical or regulatory link with the subscriber; ● undertakes to provide the information and justifications required in the registration documents that are up to date and valid; ● applies the certificate in compliance with the conditions of use provided for in the CP and repeated in these GCU, respecting the limits on use; ● agrees that any successful authentication for the electronic seal service is presumed to have been carried out with the agreement of the SCM and the subject entity;

	● undertakes to notify the CA, without undue delay, whenever any of the following causes for revocation are established: ○ an error (intentional or otherwise) has been detected in the registration documents or the certificate; ○ the information contained in the certificate no longer conforms to the identity or intended use of the certificate, before the normal expiry date of the certificate; ○ the activation data is suspected of having been compromised, lost, stolen or revoked. ● is prohibited from using the certificate where the activation data, the private key or the CA are suspected of having been compromised, lost, stolen or revoked; ● undertakes to check the status of the certificate issued via the CRLs published by the CA; ● agrees to the AE and the CA keeping the registration information, key and certificate management data.
Obligations of the subscriber and the SCM	The subscriber, represented by the SCM, takes the following requirements into account, namely it: ● has a contractual, hierarchical or regulatory link with the subject entity; ● undertakes to obtain the formal agreement of an authorised representative of the subject entity prior to requesting any certificate; ● undertakes to provide the information and justifications required in the registration documents that are up to date and valid; ● tacitly accepts the certificate issued by the CA once issued by the RA; ● ensures the confidentiality of the activation data enabling the application service to access the electronic seal service; ● agrees that any successful authentication from the electronic seal service is presumed to have been carried out with the consent of the SCM and the subject entity; ● uses the certificate only with the consent of the subject entity within the framework agreed between the subject entity and within the limits on use provided for in these GCU; ● undertakes to notify the CA, without undue delay, whenever any of the following causes for revocation are established:

	○ an error (intentional or otherwise) has been detected in the registration documents or the certificate; ○ the information contained in the certificate no longer conforms to the identity or intended use of the certificate, before the normal expiry date of the certificate; ○ the activation data is suspected of having been compromised, lost, stolen or revoked. ● is prohibited from using the certificate where the activation data, the private key or the CA are suspected of having been compromised, lost, stolen or revoked; ● undertakes to notify the RA prior to any invalidation of the role of the known SCM; ● undertakes to check the status of the certificate issued via the CRLs published by the CA; ● agrees to request the renewal of the certificate at least three (3) months before it expires; ● agrees to the AE and the CA keeping the registration information, key and certificate management data.
Obligations in relation to the verification of certificates by users	Certificate users must: ● verify and respect the use for which a certificate has been issued; ● for each certificate in the certification chain, from the holder's certificate to the `Yousign S.A.S. -` Root2 CA, verify the digital signature of the CA that issued the certificate in question and check the validity of that certificate (validity dates, revocation status); ● verify and respect the obligations of certificate users as expressed in the CP. CRLs are published at the URLs contained in the certificates, which can also be found in the CP.
Verification of certificate status	In the event of revocation by the CA, for example if its private key is compromised, the revocation information is provided in a RCACL that is published in the URLs contained in the certificates and that can also be found in the CP.
Limit on liability	Yousign cannot be held liable for any unauthorised or improper use of authentication data, certificates, CRLs or any other equipment or software made available. Yousign accepts no liability for any damage resulting from errors or inaccuracies in the information contained in the

	certificates where such errors or inaccuracies are the direct result of the erroneous nature of the information provided by the subscriber or the subject entity. In any event, and to the strict extent permitted by the applicable law, Yousign cannot be held liable for the payment of damages and interest of any nature whatsoever, whether direct, material, commercial, financial or moral as a result of the performance herein.
Documentary references	The Certification Policy of the Yousign S.A.S. - Sign3 CA for server seals is available at the following address: https://yousign.com/technical-documentation-of-certifications.
Language	These GCU have been drafted in several languages, including French. The language of interpretation will be French in the event of any contradictions or disputes over the meaning of a term or provision.
Applicable law and dispute resolution	These GCU are governed by and constructed 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 in the absence of an amicable agreement between the parties, the courts in Paris have exclusive jurisdiction.
Management of personal data	Yousign undertakes to comply with the applicable legislation and regulations on personal data management, in particular European Regulation 2016/679 of 27 April 2016, known as the 'General Data Protection Regulation' (GDPR). The subscriber and the subject entity are informed that the issuing of electronic certificates involves the processing of personal data by Yousign. They are invited to consult the Privacy Policy for more information on how their personal data is processed and how to exercise their rights.
Audits and applicable references	Yousign has set up a Yousign Technical Management Committee. A technical security audit is carried out at least once a year. The audits are carried out internally by Yousign staff or as a service provided by companies specialising in IT systems

	security and with recognised skills in the field of IT systems security.
Agreement on proof	For each electronic seal produced, Yousign, the subscriber and the subject entity accept that the information contained in: ● the registration documents, such as: ○ the identification details of the subscriber and its SCM; ○ the identification details of the subject entity and its lawfully appointed representative; ○ the supporting documents provided; ● the documents of proof, such as: ○ the procedures used to affix the electronic seal to documents (the authentication process, for example); ○ the electronic seal certificate; ○ time-stamping information; ○ a set of computer traces; are admissible in court and provide proof of the data and information they contain as well as the authentication procedures they express. The registration and proof documents will be archived and time-stamped by Yousign.