Certificate and timestamp authority

General Conditions of Use - YOUSIGN SAS - SIGN2 CA

Export at 05/01/2021

Creator : Kevin Dubourg - 03/04/2020

last change : Yves Rocha - 28/12/2020

Diffusion : C1 - Public

Summary:

1 - Version history

Version	Purpose of the revision	Date	Author
1.1.4	Acronyms update Modification of the contact email address of the certificate authority Update of "Liability limit" and "Management of personal data" clauses Addition of the "Language" clause "Dispute Resolution" and "Applicable Law" clauses grouped together in the same clause	21 déc. 2020	Yves Rocha
1.1.3	Template modification	18 août 2020	Florent Eudeline
1.1.2	Document creation	3 avr. 2020	Antoine Louiset

2 - Introduction

2.1 - General presentation

This document defines the general conditions of use of the certificates issued in agreement with the electronic signature process from the Certificate Authority « YOUSIGN SAS - SIGN2 CA ».

These general conditions of use are accepted by the certificate's holder during the signature process. This document aims to review briefly the demands that are respected by the Certificate Authority and they are more defined in CA's certification policy « YOUSIGN SAS - SIGN2 CA ».

The certificate's holder is a natural person.

If the certificate's holder signs on behalf of a legal person, he declares that he is authorized to represent and legally bind this legal person for whom the electronic signature process is implemented.

2.2 - Document identification

This document is referenced by its version number.

This number is to be changed disregarding the OID from the certification policy.

This GCU version applies to the following OID:

- OID : 1.2.250.1.302.1.5.1.0 for LCP level certificates of ETSI 319 411-1 standard,
- OID : 1.2.250.1.302.1.6.1.0 for generated certificates with at least an identifying factor from the holder from a RA member from Yousign,
- OID : 1.2.250.1.302.1.8.1.0 for generated certificates with at least an identifying factor from the holder from a RA external to Yousign.

The relevant elements of OID will be preceded by OID in square brackets : [OID]. Several OID can be specified, they are separated with a semicolon.

2.3 - Acronyms

CA	Certificate Authority
CP	Certification Policy
CRL	Certification Revocation List
DCP	Declaration of Certification Process
DPO	Data Protection Officer
GCU	General Conditions of Use
LCP	Lightweight Certificate Policy

OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
SMS	Short Message Service
URL	Uniform Resource Locator

3 - General Conditions of Use

Certificate Authority's contact	Gestion de l'AC Yousign Yousign SAS 8 allée Henri Pigis 14000 CAEN authority@yousign.com
Type of issued certificates	GCU apply to certificates detailed in paragraph Identification of document. The certificates issued by the CA are signature certificates for Yousign users in agreement with the electronic signature process of Yousign. They are ephemeral certificates generated by the CA on the behalf of the holder during the signature process. These certificates can't be used for any other purpose. The certificates are issued following this certification chain: YOUSIGN SAS – ROOT2 CA | YOUSIGN SAS – SIGN2 CA The certificates from the certification chain are available at the following address https://yousign.fr/fr/public/document.
Certificates' subjects	The certificates issued by the CA are aimed at natural persons. These certificates data are stored in a security module under the CA control and can only be used during the signature transaction.

Procedures	The certificate's holder is a natural person. [OID : 1.2.250.1.302.1.5.1.0] The holder registration is issued by YOUSIGN that validates the holder's identity with an ID, his email address and/or his phone number. [OID : 1.2.250.1.302.1.6.1.0 ; 1.2.250.1.302.1.8.1.0] The initial validation of the holder identity is obtained: the RA validates at least one holder identification's criteria. Here is a non-exhaustive list of criteria that can be verified: unique code sent by email, unique code sent by SMS, ID validation, photo of the signatory. ***Identity Validation of a person to obtain a certificate*** [OID : 1.2.250.1.302.1.5.1.0] The registration of the holder requires his ID validation, an existing email address and/or a phone number. Identity documents allowed are : • national ID, • passport, • residence permit. To do so, we are going through this following process : • use of a unique URL; • verification of the ID sent by the holder ; • an authentication code is sent (this code enables the authentication of a holder to validate a signature) ; Once the future holder has clicked on the unique URL, has downloaded his ID which is verified instantaneously and has given us the authentication code, his identity is validated. [OID : 1.2.250.1.302.1.6.1.0 ; 1.2.250.1.302.1.8.1.0] The future holder's registration requires the verification of an identity parameter. The identification can be executed in different ways. Here is a non-exhaustive list of criteria that can be verified: unique code sent by email, unique code sent by SMS, ID validation, photo of the signatory. To do so, we are going through this following process : • use of a unique URL; • signatory's identification through chosen system ; Once the future holder has clicked on the unique URL, has filled the identification requirements, his identity is validated. ***Method to access the private key and use the signature certificate*** The private key is entirely managed, stored and protected by the infrastructure Yousign. Nevertheless, we have implemented technical and organizational tools in order to make sure that the private key will be exclusively used by the holder. In no case may this key be used by Yousign on its own behalf or on the behalf of someone else. The private key is logically related to the holder and he is the only one to know the activation data.

	Indeed, to use his private key, the holder will have to authentify via two channels : • via obtaining a unique URL ; • via an authentication code. It should be noted that obtaining the unique URL is transparent for the holder as it is either transmitted by email when the holder clicks on the button allowing access to the documents to be signed or transparently if the signature process is embedded in a third-party application managed by the Yousign client. Our technical architecture allows the private key to be used provided that the authentication code is entered by the user. Moreover, a signature made via the CA « YOUSIGN SAS - SIGN2 CA » is valid only if the PKI Yousign can attest of a standard procedure for a signature request via system log files and traces. These system log files and traces are archived for 17 years.
Renewal modalities	There is no renewal modalities process.
Revocation modalities	You can apply for a certificate revocation by email or phone. Here is the procedure : • Revocation by phone: the user can contact Yousign by phone to apply for a certificate revocation. To do so, Yousign will be checking his identity. The holder will be asked two random questions about his identity. These questions are based on the information Yousign owns. The validation will be effective, following another confirmation from another channel than the phone. For instance, we can send him a confirmation link at his email address. • Revocation by email: the user can contact Yousign by email to apply for a certificate revocation. To do so, Yousign will be checking his identity. The holder will be asked two random questions about his identity. These questions are based on the information Yousign owns. The validation will be effective, following another confirmation from another channel than the email. For instance, we can : • Send him a code on his phone • Call him to get a confirmation A certificate revocation can only occur during the validity period of the contract, that is, the 15min following the certificate generation. This extremely short period makes the revocation process difficult to apply with the associated CP.
Restrict use	Delivered certificates can only be used for signatures transactions provided by Yousign infrastructure. The holder's certificates have a 15-minute validity period. The matching private keys have a life duration similar to a signature process. System log files and traces about certificate issuance and private key usage are archived for 17 years.

Holders' obligations	The holder must: • Provide correct and updated information when applying for the certificate creation or renewal ; • Protect his authentication data ; • Accept these general conditions of use ; • Check that provided data from the certificate of the signed document are correct ; • Ask for his certificate renewal within a reasonable time before the expiration date; • Immediately apply for revocation of his certificate to Yousign in case of any compromise or compromise suspicion of his authentication data. The acceptance of the certificate issued by the CA is tacit as soon as the signature has been made via the signature system of Yousign. Before using it, the holder can refuse the certificate generation by interrupting the signature process. If the bi-key had already been generated, a technical process would automatically destroy it.
Obligations of certificates' verification by users	The certificates' users must : • Verify and respect the use for which the certificate has been generated ; • For every certificate of the certification chain, from the holder's certificate to the CA « YOUSIGN SAS – ROOT2 CA », check the digital signature from the CA that has issued the specific certificate and check the certificate validity (validity period, revocation status); the users can use a signed file for these verifications. The certificate content can be verified and monitored. • Verify and respect the obligations of certificates users of the CP.
Liability limit	Yousign may not, under no circumstances, be considered liable for any unauthorized or non-compliant use of authentication date, certificates, CRL, as well as any other existing equipment or software made available. Yousign declines responsibility for any damage resulting from errors or inaccuracies in the information contained in the certificates, when these errors or inaccuracies result directly from the erroneous nature of the information communicated by the holder. In any event, Yousign shall not be liable for the payment of damages of any nature whatsoever, whether direct, material, commercial, financial or moral, as a result of the execution hereof.
Documentaries' references	The Certification Policy of the CA « YOUSIGN SAS – SIGN2 CA » can be found at the following link : https://yousign.fr/fr/public/document. The CPS is available upon request to the CA using the contact information provided above.
Compensation conditions	No subject
Language	In the event any translation of this general conditions of use is prepared for convenience or any other purpose, the provisions of the French version shall prevail.

Applicable law and dispute resolution	These general conditions of use are governed and interpreted in accordance with French Law. 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 courts of Caen (France).
Management of personal data	Yousign undertakes to comply with the laws and regulations in force regarding the protection of personal data, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (known as the General Data Protection Regulation or GDPR). The holder is informed that the issuance of electronic certificates and the execution of the electronic signature process presupposes the implementation by Yousign of personal data processing to which the holder consents, in accordance with Yousign's privacy policy available at https://yousign.com/privacy. The holder is informed that the communication of his data is mandatory and necessary to take into account his request and the execution of the electronic signature process. The holder has a right to access, rectify or delete information concerning him, as well as a right to oppose the processing of the data by contacting Yousign's DPO at dpo@yousign.com.
Audits	Certificate Authority «YOUSIGN SAS - SIGN2 CA» is compliant, for certificates issued with the 1.2.250.1.302.1.5.1.0 policy, with LCP level of ETSI 319 411-1 standard. Yousign enforces a Technical Direction Board. This one performs validation of the conformity between DCP and CP. A conformity control is processed during the commissioning and after any significant change. Moreover, an audit will be organized every year. Audits are processed internally by qualified staff or by external companies recognized in the electronic signature area. In the context of obtaining certifications for the PKI infrastructure, audit is executed by an external company duly accredited.
Evidence convention	For each electronic signature performed, Yousign and the holder agree that : • the identification elements used in order to proceed with the electronic signature of the documents, i.e. the surname and first name of the holder, the personal telephone number used, his e-mail address, the Electronic Signature Certificate, the supporting documents, • the time stamping elements, • the processes used to electronically sign documents (entering the security code sent by sms for example), • the evidence file containing a set of computer traces, are admissible in court and demonstrate the data and elements they contain and the authentication procedures they express. This file will then be archived and time-stamped by the third-party archiver.

Archiving with a third-party archiver	When the Yousign's client subscribed to the option of archiving electronically signed documents, these will be archived with a third party archiver (CDC ARKHINEO), under conditions that guarantee security and integrity over time, in accordance with the requirements of Article 1367 of the Civil Code.