Terms of Service - YOUSIGN SAS - SIGN2 CA

1-Introduction

1.1 General presentation

This document defines the general conditions of use of the certificates issued in agreement with the digital signature process from the Certifying 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 Certifying 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 authorized to represent and legally bind this legal person for whom the signature process is implemented.

1.2 Identification of document

This document is referenced by its version number: 1.1.0.

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 of ETSI 319 411-1 standard,
- OID : 1.2.250.1.302.1.6.1.0 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 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.

1.3 Acronyms

CA	Certificate Authority

RA	Registration Authority
GCU	General Conditions of Use
DCP	Declaration of Certification Process
PKI	Public Key Infrastructure
LCP	Lightweight Certificate Policy
OID	Object Identifier
CP	Certification Policy
CRL	Certificate Revocation List

2-General conditions of use

Certifying Authority's contact	Yousign SAS 8 allée Henri Pigis 14000 CAEN contact@yousign.fr
Type of issued certficates	GCU apply to certificates detailed in paragraph 1.2. The certificates issued by the CA are signature certificates for Yousign users in agreement with the digital 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 AC | YOUSIGN SAS – SIGN2 AC 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[1] ;

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 ;

[1] Authentication code: this code enables the authentication of a holder to validate a signature.

	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. 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 AC » 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 10 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 : o Send him a code on his phone o 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 existing Certification Policy.
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 10 years.
Holders’ obligations	The holder must: • Provide correct and updated information when applying for the certificate creation or renewal ; • Protect his authentication data ; • Accept the terms of service of signature Yousign ; • 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 AC », 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 accepts no responsibility with non-authorized use or noncompliant use of authentication date, certificates, des LCR, and every other existing equipment or software. Yousign accepts no responsability with damages from mistakes or inaccurate information among certificates data, when mistakes or inaccurate information come from the holder who provided the information. Moreover, in accordance with french law restrictions, Yousign accepts no responsibility with: • Financial loss ; • Data loss ; • Consequential damage when using a certificate ; • Any other damage. In every instance, Yousign responsability will be limited, whatever the cause of damage, to the sum payed to Yousign for accessing the signature service and that, with respecting the full extent of the applicable law.
Documentaries' references	The Certification Policy of the CA « YOUSIGN SAS – SIGN2 AC » can be found at the following link : https://yousign.fr/fr/public/document Certification Practice Statements can be obtained on demand using CA contact info.
Compensation conditions	No subject.
Applicable law	The present Certification Policy is governed by French law. In case of litigation between parts and failing amicable agreement, exclusive jurisdiction is attributed to the Caen Court.
Management of personal data	The holder is informed that issuance of certificates and execution of signature system assume the processing of personal data which the holder accepts. Yousign is responsible of this process. The holder is informed that communication is compulsory and necessary to take account his demand and to execute the process of signature. The holder is entitled to access, change, correct and delete this information.

	Personal data will not be transferred to third party, except companies responsible to implementation of Yousign's solutions with Yousign. Yousign undertakes to ensure its users the highest level of confidentiality and security of the information provided.
Audits	Certification 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 digital signature area. In the context of obtaining certifications for the PKI infrastructure, audit is executed by an external company duly accredited.