yousign

GENERAL TERMS AND CONDITIONS OF USE OF AC YOUSIGN SAS – QUALIFIED SIGNATURE CA

v1.2.4 | Diffusion: C1 – Public

VERSION HISTORY			
Version	**Subject of the modification**	**Date**	**Author**
1.2.4	Modified holders certificates lifetime to 60 minutes (15 minutes before).	2024-01-23	Tony DUFOUR
1.2.3	Page layout modification	2023-10-03	Sid Ahmed Re...
1.2.2	Completion of acronyms and addition of translations where necessary (section acronyms) Postal address update (section general conditions of use, see contact point) Replacement of the term "customer" by "holder" (section general conditions of use, see types of certificates, validation procedures and usage restrictions) Addition of a reference to the Certification Policy describing the revocation process and removal of information redundant with it (section general conditions of use, see types of certificates, validation procedures and usage restrictions) Addition of obligations for the holder relating to the storage and sharing of the private authentication key (section general conditions of use, see holder undertakings) Addition of the CRL links to YOUSIGN SAS - QUALIFIED SIGNATURE CA (section general conditions of use, see verification of the certificate status) Clarification of the limit of the exemption from damages (section general conditions of use, see limitation of liability) Renaming the section (section general conditions of use, see confidentiality) Removal of the local reference for applicable legislation and regulations	2023-05-09	Adrien Van De... Tony Belot

	(section general conditions of use, see confidentiality) Change of the competent court from Caen to Paris (section general conditions of use, see applicable law and dispute resolution) Review of the content of the section and addition of a pointer to the online Privacy Policy (section general conditions of use, see personal data management) Minor spelling and wording corrections		
1.2.1	Deletion of the qualified field `esi4-qcStatement-5` from the section general conditions of use, see audit and certification	2023-01-27	Sid Ahmed Re…
1.2.0	Addition of a notion concerning the acceptance of these GCU by the signatories, as a condition for obtaining a certificate (section general presentation) Referencing the various certification policies according to the OID (section identification of the document) Addition of the term QSCD (section acronyms) Update of Yousign's postal address (section general conditions of use, see contact point) Addition of qualified electronic signature certificates, type QCP-n-qscd, with the OID 1.2.250.1.302.1.16.1.0 (section general conditions of use, see types of certificates, validation procedures and usage restrictions and applicable agreements and certification practices) Addition of the obligation for the holder to register a means of authentication in the case of OID 1.2.250.1.302.1.11.1.0 (section general conditions of use, see types of certificates, validation procedures and usage restrictions)	2023-01-04	Tony Belot

	Adding the UID attribute to DNs in the case of the OID 1.2.250.1.302.1.16.1.0 (section general conditions of use, see types of certificates, validation procedures and usage restrictions) Modification of the component responsible for comparing the first names and last names supplied by the RA (section general conditions of use, see types of certificates, validation procedures and usage restrictions) Clarification of the retention period for holder registration files (section general conditions of use, see usage limits) Addition of holder obligations for OIDs 1.2.250.1.302.1.15.1.0 and 1.2.250.1.302.1.16.1.0 (section general conditions of use, see holder undertakings) Addition of applicable documents relating to the PVID (section general conditions of use, see applicable agreements and certification practices) Addition of qualifications and certifications applicable to Remote QSCD and to the PVID (section general conditions of use, see audit and certification) Addition of certificate levels and additional qualified fields (section general conditions of use, see audit and certification) Correction of typographical errors in additional qualified fields (section general conditions of use, see audit and certification)		
1.1.1	Addition of addresses for distributing CA revocation information e.g. in the event of the CA being compromised (section verification of the certificate status)	2022-07-28	Tony Belot
1.1.0	Modification of the page layout Addition of remote face-to-face	2022-05-27	Tony Belot

	Update of the "Personal data management" clause concerning the holder's rights Certificate verification completed in connection with the eIDAS Trusted List Updating and completion of the holder's undertakings URLs for publishing CRL corrected Clarification of contact details for sending revocation requests		
1.0.4	Update of acronyms Modification of the certification authority's contact email address Update of the "Limitation of liability" clause Addition of "Personal data management" and "Language" clauses	2020-12-21	yves.rocha@y...
1.0.3	Certificate status check updated. Clarification of the OCSP response.	2020-09-22	Kévin Dubourg
1.0.2	Page layout modification	2020-08-18	Florent Eudeli...
1.0.1	Updating of holder responsibilities and addition of a signature test during holder registration	2018-11-02	Antoine Louiset
1.0.0	Document creation	2018-09-25	Antoine Louiset

Table of contents

1. Introduction

1.1. General presentation

Yousign is an Electronic Certification Service Provider (ECSP) which provides its customers and for its own use services involving electronic certificates and in particular an electronic signature.

In this context, this document sets out the General Conditions of Use of the certificates issued by the Certification Authority "YOUSIGN SAS - QUALIFIED SIGNATURE CA". This document sets out the modalities for the management of the certificates as well as the undertakings and obligations of the different parties.

The certificate holder explicitly accepts these General Terms and Conditions of Use when requesting a certificate. Otherwise, no certificate can be issued by the Certification Authority "YOUSIGN SAS - QUALIFIED SIGNATURE CA".

1.2. Identification of the document

These "Terms and Conditions of Use" relate to the CA "YOUSIGN SAS - QUALIFIED SIGNATURE CA" which issues certificates according to its Certificate Policy dealing with the following certificate profiles identified by their respective OIDs:

- **[Physical face-to-face]**: OID 1.2.250.1.302.1.11.1.0
- **[Remote face-to-face]**: OID 1.2.250.1.302.1.15.1.0
- **[Qualified signature]**: OID 1.2.250.1.302.1.16.1.0

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

1.3. Acronyms

Acronym	**Meaning**
CA	Certification Authority
RA	Registration Authority
ANSSI	French National Cybersecurity Agency (in French "*Agence*

Acronym	Meaning
	Nationale de la Sécurité des Systèmes d'Information")
TCU	General Terms and Conditions of Use
DN	Distinguished Name
CPS	Certification Practice Statement
DPO	Data Protection Officer
eIDAS	electronic IDentification, Authentication and trust Services
PKI	Public Key Infrastructure
ARL	Authority Revocation List
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
OID	Object Identifier
CP	Certificate Policy
PVID	Trusted Remote Identity Verification (in French "*Prestataire de Vérification d'Identité à Distance*")
QCP-n	Policy for EU qualified certificate issued to a natural person
QSCD	Qualified Signature Creation Device

2. General Conditions of Use

These TCU are based on the model provided by Annex A of the norm EN 319 411-1 (version 1.3.1).

Contact point	Yousign SAS CA management Yousign 507 rue de Suède et de Norvège

	14000 Caen authority@yousign.com
Types of certificates, validation procedures and usage restrictions	The certificates covered by these TCU are issued by the following Certification Authority chain: - Root AC: « YOUSIGN SAS - ROOT2 CA » - Issuing AC: « YOUSIGN SAS - QUALIFIED SIGNATURE CA » The CA issues ephemeral qualified certificates, used according to the process, for remote qualified electronic signature or advanced electronic signature as defined in the eIDAS Regulation. Qualified certificates for remote qualified electronic signature are issued after an initial remote identity verification performed on the RA's website. The holder's private key is generated and used in a remote qualified signature creation device (Remote QSCD). The holder can register a strong authentication means, complying with the requirements of the electronic identification means of substantial level, allowing to obtain new remote qualified electronic signature certificates. These certificates have the OID 1.2.250.1.302.1.16.1.0, and where rules specifically apply to this type of certificate, they are identified in this document as **[Qualified signature]**. Qualified certificates for advanced electronic signatures are issued in one of the following ways: - after an initial identity check in a physical face-to-face with an operator of the RA. During this face-to-face meeting, the holder registers a means of strong authentication enabling them to sign subsequently. These certificates carry the OID 1.2.250.1.302.1.11.1.0, and when rules specifically apply to this type of certificate, they are identified in this document by the mention **[Physical face-to-face]**; - after an initial remote face-to-face identity verification of a substantial or high level according to the eIDAS regulation, on the RA's website. These certificates carry the OID 1.2.250.1.302.1.15.1.0, and where rules specifically apply to this type of certificate, they are identified in this document by the mention **[Remote face-to-face]**. Certificates can only be used within the framework of the signature service offered by Yousign, to sign a document or a message in all areas for which a signature is required as validity or proof and in particular:

- electronic signature by a holder, followed by verification of said signature by an administration or a company by electronic means;
- electronic signature by a holder, followed by verification of said signature by a natural person.

Said electronic signature provides, in addition to the authenticity and integrity of the data thus signed, the manifestation of the signatory's consent to the content of these data. The qualified electronic signature is moreover presumed reliable and is deemed equivalent to a handwritten signature pursuant to the eIDAS Regulation.

The holder may be a natural person or, for certain certificates issued in **[Physical face-to-face]**, a natural person acting on behalf of a legal person.

The DN are constructed as follows:

Attribute	**Description**	**Presence**
CN	commonName: Last name and first name of the holder	Yes
SN	surname: Last name of the holder	Yes
GN	givenName: First name of the holder	Yes
OI	organizationIdentifier: Identifier of the entity with which the holder is linked, according to the eIDAS syntax : NTRFR-<SIREN number>	Only in the case of a link with a legal person
OU	organizationUnit : Identifier of the entity with which the holder is linked, according to the RGS syntax : 0002 <SIREN number>	
O	organizationName : Name of the entity with which the holder is connected	
C	countryName : Country of the Yousign registration authority,	Yes

	always equal to FR (France)	
SerialNumber	serialNumber : Date and time when the certificate generation was started	Yes
UID	userIdentifier: Transaction identified of the signatory in the Yousign infrastructure.	[Qualified signature] only

The test certificates issued by the CA “YOUSIGN SAS – QUALIFIED SIGNATURE CA” are immediately identifiable by the addition of the prefix “TEST –”in the value of the CN attribute, for example:
CN = TEST – Jean DUPONT,…

Apart from this specificity, the test certificates issued by CA “YOUSIGN SAS - QUALIFIED SIGNATURE CA” follow the same processes as nominal production certificates.

The implementation of a qualified certificate requires a verification process of the identity of the holder.

[Physical face-to-face]
This process takes place during a face-to-face meeting with an operator of the RA Yousign. The holder must prepare an application which contains the following elements:

- he certificate request form, signed by the holder and dated less than 3 months ago;
- the general terms and conditions of use in force, signed by the holder;
- a copy of a valid proof of identity of the holder among the following documents:
  - identity card;
  - passport;
  - residence permit;
- only for an application relating to a legal person:
  - for a company, any document, valid at the time of the certificate application, demonstrating the existence of the company and bearing its SIREN number, or, failing that, another document demonstrating the unique identification of the company which will appear in the certificate;
  - for a company, any document demonstrating the signatory's capacity to request a certificate on behalf of their company;
  - for an administration, a document, valid at the time of registration, delegating or subdelegating the

    - authority responsible of the administrative structure;
    - for a company or an administration, the certificate request form must be signed by an authorised representative of the legal entity in addition to the signature of the holder.

The request form for a certificate shall include:

- the type of certificate requested;
- the last name and first name of the holder, as they appear on the identity document submitted with the request;
- information from the identity document submitted: type, number, validity date, issuing authority;
- the email address of the holder;
- a phone number to contact the holder;
- the commitment to the accuracy of the information on the form, and in particular that which will be included in the certificate.

The RA performs the following operations during the face-to-face meeting

- verification of the completeness and signature by the future holder of the certificate request form;
- verification that the future holder has signed the general terms and conditions of use of the signature service;
- validation of the identity of the future holder through the verification of the original of the identity document and the conformity of its copy;
- verification of the consistency of the information provided in the certificate request form with the identity document;
- in the case of a request relating to a legal person:
    - verification of the validity of additional supporting documents;
    - verification of the signature by the legal person on the application.

The verification of the email address of the holder is carried out during the holder account creation process on the Yousign service.

During this initial process, the operator submits a document for the holder to sign electronically. This allows the operator to directly ensure that the identity information contained in the certificate is up to date.

Once the identity validation is obtained, the holder implements a strong authentication means. This means is enrolled by Yousign to allow the holder to strongly authenticate themselves in view of expressing their consent during the signature process. The identity information carried

in the ephemeral certificate is that which was initially validated by the RA operator. This information remains valid for a period of 3 years until the holder is required to re-validate the identity information.
It is the responsibility of the holder to request an update of the identity information if it ends up being out-of-date before the 3-year period.

The holder cannot renew their certificate, each signature transaction generates a new ephemeral qualified certificate.

[Remote face-to-face]
The initial validation of the identity of the holder is performed on the RA's website during a remote face-to-face meeting. The remote verification process includes the following steps:

- the holder connects to the RA website via a unique link that they has received on their email address, and must ensure that they have a mobile device equipped with a camera or that they carry out the signature process directly from a mobile device equipped with a camera;
- the RA displays to the holder the identity information used for the certificate request:
    - first name and last name;
    - email address;
- the holder confirms that they have read the general terms and conditions of use in force and agrees to sign them without reservation;
- the holder confirms the accuracy of the information presented and agrees to sign the certificate request form established on this basis;
- if the holder is not on a mobile device, they are asked to continue their identification on a mobile device (equipped with a camera), via a QR code to be scanned or via the reception of an SMS;
- remote identity verification is carried out by a certified PVID provider, and includes the following steps:
    - the holder accepts the terms and conditions and the privacy policy of the PVID and consents to the processing of their biometric data so that the PVID can verify their identity;
    - the holder presents the camera with a valid official identity document chosen among the following:
        - identity card;
        - passport;
        - residence permit;

      and follows the successive instructions given by the PVID;

    - the PVID verifies the validity and authenticity of the document presented, and extracts the identity information of the holder;
    - the PVID asks the holder to present their face to the camera and to follow the instructions given dynamically;
    - the holder follows the successive instructions given by the PVID;
    - the PVID ensures that the holder's face matches the photograph on the identity document;
    - the PVID sends the results of the identity verification back to the RA. The final PVID ruling is sent asynchronously, after the elements have been verified by a human operator;
- the remote identity verification service verifies that the last name and the first name extracted from the presented identity document correspond to those assumed for the requestor.

During a remote face-to-face meeting, the holder cannot make a request in relation to a legal entity.

The advanced electronic signature of the certificate application form and the TCU will be applied to the documents after generation of the holder certificate, following the final ruling of the PVID.

The certificate request form includes:

- the type of certificate requested;
- the last name and first name of the holder
- the e-mail address of the holder;
- a confirmation that the last name, first name and e-mail address are correct;
- acceptance of the General Conditions of Use;
- information from the identity document presented, such as its type, number, expiry date, etc.

The RA then archives the signed certificate request form, the signed TCU and the proof of the verification of the holder's identity.

[Qualified signature]

The initial validation of the identity of the holder is performed remotely on the RA's website. The process includes the following steps:

- the holder connects to the RA's website via a unique link that they have received on their email address;
- the holder selects the remote identity verification method that they are able to use chosen among the proposed methods (all with a substantial or high level of guarantee);

	● the RA displays to the holder the identity information used for the certificate application: ○ first name and last name; ○ e-mail address; ● the holder confirms that they have read the general terms and conditions of use in force and agrees to sign them without reservation; ● the holder confirms the accuracy of the information provided and agrees to sign the certificate request form based on this information; ● the holder follows the instructions for carrying out the remote identity verification, depending on the method chosen. Where applicable, a valid official identity document may be required, including the following: ○ identity card; ○ passport; ○ residence permit; ● the remote identity verification service verifies that the last name and first name extracted from the presented identity document correspond to those assumed for the requestor. During a remote identity verification, the holder cannot make a request in relation to a legal entity. The qualified electronic signature of the certificate request form and the TCU will be placed on the documents after the generation of the holder certificate, following successful identity verification. The certificate request form shall include: ● the type of certificate requested; ● the last name and first name of the holder ● the email address of the holder; ● a confirmation that the last name, first name and email address are correct; ● acceptance of the General Conditions of Use; ● information from the presented identity document, such as its type, number, expiry date, etc. The RA then archives the signed certificate request form, the signed TCU and the proof of verification of the holder's identity. Following this initial identity verification, the holder can register a means of authentication which will enable them to obtain new qualified signature certificates at a later date without repeating the initial identity verification. In its absence, the signatory will have to perform a new initial identity verification at the time of their next qualified electronic signature. The identity information carried in the ephemeral certificate generated at each signature is the one validated by the remote face-to-face. This information

	remains valid for a maximum of 3 years until the holder is obliged to re-validate the identity information, this period being reduced in accordance with the expiry date of the identity document or the electronic means of identification presented at the time of issuance of the means of authentication. It is the responsibility of the holder to request an update of the identity information if it ends up being out-of-date before the 3-year period. The holder must request the revocation of their means of authentication in the following cases: ● their private key is suspected of being compromised, is compromised or is lost (possibly the associated activation data); ● their means of authentication to authorise a signature transaction has been compromised or are suspected of being compromised. **[Physical face-to-face] and [Remote face-to-face]** The revocation request must be made by the holder themselves or potentially by an authorised representative in the case of a certificate issued in connection with a legal entity. It must be sent to the CA by postal mail or by email to the contact point identified above. The request must include a copy of the requestor's identity document and, if applicable, the documents justifying their authority over the certificate. The CA processes the request within 24 hours if the certificate has not expired at the time the revocation is processed. **[Qualified signature]** The revocation request must be performed by the holder themselves, who must contact the CA in accordance with the procedure documented in the CP: the CA verifies the identity of the holder by remote face-to-face verification. The CA processes the request within 24 hours if the certificate has not expired at the time the revocation is processed. **[Physical face-to-face] and [Qualified signature].** A revocation request guarantees the holder that no new signatures will be allowed with their current means of authentication.
Usage limits	The issued certificates can only be used for signature transactions provided by the Yousign infrastructure.

	Holder certificates are valid for 60 minutes. The corresponding private keys have a lifetime equivalent to the duration of the signature process. Yousign keeps the registration records of the holders for 10 years (20 years for certificates issued in the context of an electronic signature process initiated by a Yousign customer established in Italy). Yousign keeps logs and traces concerning the issuance and use of holder private keys for 17 years.
Holder undertakings	The holder takes the following undertakings: ● provide up-to-date and valid identity details during the registration process; ● **[Physical face-to-face]** and **[Qualified signature]**: comply with the obligations relating to the remote identity verification service imposed by Yousign's PVID partner; ● tacitly accept the certificate issued by the CA by validating the creation of the signature, after validation of the request form and acceptance of the TCU; ● accept the storage by the CA of the information in the registration and management file for its signature keys; ● agree to use the strong authentication method initially enrolled by the CA; ● use the signature certificate in compliance with the specified limits of use; ● **[Qualified signature]**: guarantee exclusive control of their private signature key and in the event of registration of a means of authentication, the holder must: ○ set up strong authentication on their phone (PIN code or password, with a limit on the number of attempts to unlock it); ○ never lend their phone, even to someone they trust; ○ in the event of loss or theft, apply the measures recommended by the phone manufacturer (remote wiping, for example) and revoke the identity by contacting Yousign; ○ if the phone is permanently transferred to a third party (sale, transfer, etc.), apply the measures recommended by the phone manufacturer to reset the phone and contact Yousign to revoke the identity; ○ keep their phone up-to-date, by installing software upgrades proposed by the phone manufacturer and by the operating system publisher; ○ only install applications on the phone that are published in the official operating system stores, avoid potentially dangerous applications (including

	jailbreak tools), and keep installed applications up-to-date; o keep their private authentication key confidential on their phone as well as any other information relating to their identity; o not share their private authentication key or any other information relating to their identity with another phone or device, even if said other phone or device belongs to the holder or to another person, including a trusted person. Any signature made after authentication on the phone is presumed to have been made by the holder who registered the phone. The principle of non-repudiation does not allow the holder to deny having signed. ● undertake to notify the CA when one of the following causes for revocation is established: o the information contained in their certificate no longer conforms to the identity or intended use of the certificate, before the normal expiry date of the certificate; o an error (intentional or not) has been detected in its registration file; o the holder's private key is compromised, suspected of being compromised or lost (possibly with the associated activation data); o the means of authentication for authorising a signature transaction have been compromised or are suspected of having been compromised; ● undertake to verify the status of the signature certificate issued through the CRL published by the CA and the OCSP service as implemented; ● use the signature certificate in accordance with the conditions of use set out in the CP and in these TCU.
CA obligations	Yousign is responsible for: ● the validation and the publication of the CP, CPS and the TCU of the CA; ● compliance of certificates issued pursuant to the CP; ● compliance with all security principles by the various components and the related controls; ● in the event of a major incident (loss, suspected compromission, compromission or theft of a certificate management private key, for example), to report the incident to ANSSI (supervision-eIDAS@ssi.gouv.fr). Yousign is liable for any damages resulting from its failure to comply with this document. Unless it can be shown that Yousign has not committed any intentional or negligent fault,

	Yousign is liable for any damage caused to any natural or legal person who reasonably relies on the certificates issued in each of the following cases: ● the information contained in the certificate does not correspond to the information provided at the time of registration; ● the issuance of the certificate did not give rise to verification of the possession of the corresponding private key by the holder; ● the CA has not recorded the revocation of a certificate and published this information in accordance with its obligations. Yousign is not liable for any damage derived from the use of the certificate exceeding the limits set for its use. If the CA ceases to operate, certificates issued and still within their validity period will be revoked. Finally, Yousign is liable in the event of fault or negligence in the precautions to be taken in terms of the confidentiality of personal data entrusted to it by holders.
Verification of the certificate status	Certificate users must verify the status of certificates, including those in the corresponding chain of trust. The CA provides users with an up-to-date CRL, which is published on the Internet at: ● http://crl.yousign.fr/crl/yousignsasqualifsignca.crl ● http://crl2.yousign.fr/crl/yousignsasqualifsignca.crl ● http://crl3.yousign.fr/crl/yousignsasqualifsignca.crl Yousign also implements an OCSP service accessible at the following address: http://ocsp.yousign.fr. This information is available seven days a week, twenty-four hours a day, with an availability of 99.7% over one month. The CRL contains the extension “ExpiredCertsOnCRL” and retains the serial numbers of all revoked certificates, even those that have expired. The OCSP service implements the "archive cutoff" extension, as provided for in RFC 6960, with a date identical to the start date of validity of the CA certificate and keeps the revocation status of the certificate available after its expiry. If the OCSP request contains a request for a serial number not issued by the CA, then the OCSP server will set the

	corresponding response status to "unknown". If the OCSP request contains a request for a serial number issued by the CA, the OCSP response will comply with the standards IETF RFC 6960. The certificates issued by the CA are qualified certificates pursuant to the eIDAS regulation. This can be verified on the basis of the Trusted List issued by ANSSI under https://www.ssi.gouv.fr/eidas/TL-FR.xml. This list must in particular include the CA certificate and its qualification status. If the CA is revoked, for example following the compromission of its private key, the revocation information is published in a ARL accessible on: ● http://crl.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl2.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl3.yousign.fr/crl/yousignsasroot2ca.crl If the CA is no longer valid, Yousign will generate: ● a final CRL with an expiry date set to 99991231235959Z; ● a final OCSP response will be pre-generated for each certificate issued, containing an expiry date set to 99991231235959Z. If Yousign ceases its CA activity, it undertakes to keep the CRL and pre-generated OCSP responses available.
Limitation of liability	Yousign cannot be held liable for unauthorised or improper use of authentication data, certificates, CRL 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 when these errors or inaccuracies result directly from the erroneous nature of the information communicated by the holder. In any event, and to the fullest 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 moral, as a result of the execution of these TCU.
Applicable agreements and certification practices	Certification policies setting out the requirements to which the CA intends to adhere are published at the following address https://yousign.fr/fr/public/document, under the OID 1.2.250.1.302.1.11.1.0, 1.2.250.1.302.1.15.1.0 and 1.2.250.1.302.1.16.1.0.

	[Physical face-to-face] and **[Qualified signature]**: The service policy and the terms of use of the remote identity verification service of Yousign's partner PVID are applicable.
Confidentiality	Information considered confidential includes at least the following: ● CA internal procedures; ● private keys of the CA, the component and the certificate holders; ● Activation data associated with the CA and certificate holder private keys; ● all PKI secrets; ● event logs of the PKI components; ● holder registration files; ● reasons for revocation, except with the explicit agreement of the holder. Yousign applies security procedures to guarantee the confidentiality of this information. Yousign undertakes to comply with applicable legislation and regulations.
Insurance policy	Yousign certifies that it holds an insurance policy guaranteeing its professional civil liability. It undertakes to maintain this insurance policy in force for the duration of its professional activity.
Language	These TCU have been drafted in several languages, including French. The language of interpretation will be French in the event of a contradiction or dispute over the meaning of a term or provision.
Applicable law and dispute resolution	These TCU are governed by and construed 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 Paris courts shall have exclusive jurisdiction.
Personal data management	Yousign undertakes to comply with the legislation and regulations in force related to 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 holder is informed that the issuance of electronic certificates and the execution of the electronic signature process involve the processing of personal data by Yousign. The holder is invited to consult the Privacy Policy for more

	information on how their personal data is processed and how to exercise their rights.
Audit and certification	The cryptographic module used by Yousign for the CA and the advanced electronic signature is qualified by ANSSI. The qualified electronic signature creation device is a qualified remote signature creation device ("Remote QSCD"), qualified under the eIDAS regulation. The remote identity verification service is certified by ANSSI at the substantial guarantee level in accordance with the PVID standard. The certificates comply with the ETSI 319 411-2 standard and are qualified under the eIDAS regulation by ANSSI. The certificates issued contain the following qualified fields: ● esi4-qcStatement-1 = id-etsi-qcs-QcCompliance ● esi4-qcStatement-6 = id-etsi-qct-esign **[Physical face-to-face]** and **[Remote face-to-face]**: The certificates are of the QCP-n level. **[Qualified signature]:** The certificates are of the QCP-n-qscd level. The certificates contain the following additional qualified field: ● esi4-qcStatement-4 = id-etsi-qcs-QcSSCD