yousign

General Terms and Conditions of Use of the YOUSIGN SAS - QUALIFIED SIGNATURE CA

v1.2.5 | Distribution: C1 - Public

VERSION HISTORY			
Version	**Purpose of the change**	**Date**	**Author**
1.2.5	Change of the corporate name from Yousign to Youtrust (section General presentation and throughout the document); Redesign of the holder registration journey (section Types of certificates, validation procedures and usage restrictions); Removal of the services **[In-person face-to-face]**: OID 1.2.250.1.302.1.11.1.0 and **[Remote face-to-face]**: OID: 1.2.250.1.302.1.15.1.0; Generalisation of the "PVID" terminology towards multi-provider wording; Change of the registered office address (section Contact point).	Jul 2, 2026	Tony DUFOUR
1.2.4	Change of the lifetime of holder certificates to 60 minutes (previously 15 minutes).	Jan 23, 2024	Tony DUFOUR
1.2.3	Layout change	Oct 3, 2023	Sid Ahmed Remmide
1.2.2	Completion of the acronyms and addition of translations where applicable (section acronyms) Update of the postal address (section general terms and conditions of use, subsection contact point) Replacement of the term “customer” with “holder” (section general terms and conditions of use, subsection types of certificates, validation procedures and usage restrictions) Addition of a reference to the Certificate Policy describing the revocation process and removal of information redundant with it (section general terms and conditions of	May 9, 2023	Adrien Van Den Branden Tony Belot

	use, subsection types of certificates, validation procedures and usage restrictions) Addition of obligations for the holder relating to the safekeeping and sharing of the authentication private key (section general terms and conditions of use, subsection holder obligations) Addition of links to the CRLs of YOUSIGN SAS - QUALIFIED SIGNATURE CA (section general terms and conditions of use, subsection certificate status checking) Clarification of the limit of the exemption from damages (section general terms and conditions of use, subsection limitation of liability) Renaming of the subsection (section general terms and conditions of use, subsection confidentiality) Removal of the local reference to the applicable laws and regulations (section general terms and conditions of use, subsection confidentiality) Replacement of the competent courts of Caen with those of 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) Minor corrections of spelling and wording		
1.2.1	Removal of the qualified field `esi4-qcStatement-5` from the section general terms and conditions of use, subsection audit and certification	Jan 27, 2023	Sid Ahmed Remmide
1.2.0	Addition of a provision on the acceptance of these GTCU by signatories as a	Jan 4, 2023	Tony Belot

	condition for obtaining a certificate (section general presentation) Referencing of the various certificate policies according to the OID (section document identification) Addition of the term QSCD (section acronyms) Update of the postal address of the company Yousign (section general terms and conditions of use, subsection contact point) Addition of qualified certificates for qualified electronic signature, of QCP-n-qscd type, with OID 1.2.250.1.302.1.16.1.0 (section general terms and conditions of use, subsections types of certificates, validation procedures and usage restrictions and applicable agreements and certification practices) Addition of the obligation for the holder to register an authentication means in the case of OID 1.2.250.1.302.1.11.1.0 (section general terms and conditions of use, subsection types of certificates, validation procedures and usage restrictions) Addition of the UID attribute in the DNs in the case of OID 1.2.250.1.302.1.16.1.0 (section general terms and conditions of use, subsection types of certificates, validation procedures and usage restrictions) Change of the component responsible for comparing the surname and given name provided by the RA (section general terms and conditions of use, subsection types of certificates, validation procedures and usage restrictions) Clarification of the retention period for holder registration records (section general terms and conditions of use, subsection usage limitations)		

	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 terms and conditions of use, subsection holder obligations) Addition of the applicable documents relating to the PVID (section general terms and conditions of use, subsection applicable agreements and certification practices) Addition of the qualifications and certifications applicable to the Remote QSCD and to the PVID (section general terms and conditions of use, subsection audit and certification) Addition of certificate levels and of additional qualified fields (section general terms and conditions of use, subsection audit and certification) Correction of typographical errors in the additional qualified fields (section General Terms and Conditions of Use, subsection Audit and certification)		
1.1.1	Addition of the publication addresses for the CA revocation information, for example in the event of its compromise (section certificate status checking)	Jul 28, 2022	Tony Belot
1.1.0	Change of the layout Addition of the remote face-to-face Update of the "Personal data management" clause with regard to the holder's rights Certificate checking supplemented in connection with the eIDAS Trusted List Update and completion of the holder's obligations Correction of the CRL publication URLs Clarification of the contact details for sending revocation requests	May 27, 2022	Tony Belot

1.0.4	Update of the acronyms Change of the contact email address of the certification authority Update of the "Limitation of liability" clause Addition of the "Personal data management" and "Language" clauses	Dec 21, 2020	yves.rocha@yousign.com
1.0.3	Update of Certificate status checking. Clarification on the OCSP response.	Sep 22, 2020	Kévin Dubourg
1.0.2	Layout change	Aug 18, 2020	Florent Eudeline
1.0.1	Update of the holder's responsibilities and addition of a signature test during holder registration	Nov 2, 2018	Antoine Louiset
1.0.0	Creation of the document	Sep 25, 2018	Antoine Louiset

Table of contents

1. Introduction

1.1. General presentation

The company Youtrust is an Electronic Certification Service Provider (ECSP) which provides its customers, and uses for its own purposes, services involving electronic certificates and in particular an electronic signature.

In this context, this document constitutes the General Terms and Conditions of Use of the certificates issued by the Certification Authority "YOUSIGN SAS - QUALIFIED SIGNATURE CA". This document sets out the certificate management arrangements as well as the commitments and obligations of the various parties.

The certificate holder explicitly accepts these General Terms and Conditions of Use during the certificate request phase. Failing this, no certificate may be issued to the holder by the Certification Authority "YOUSIGN SAS - QUALIFIED SIGNATURE CA".

The company Youtrust was named Yousign until 01/07/2026, the date on which its corporate name was amended in the Trade and Companies Register (RCS) without any change of SIREN number. As a result, the Certification Authorities bear the name Yousign and retain a correct identifier of the legal entity Youtrust.

1.2. Document identification

These "General Terms and Conditions of Use" relate to the CA "YOUSIGN SAS - QUALIFIED SIGNATURE CA", which issues certificates in accordance with its Certificate Policy.

The certificate profiles are identified by their respective OIDs:

- **[Qualified signature]** : OID 1.2.250.1.302.1.16.1.0

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

1.3. Acronyms

Acronym	Meaning	Translation
CA	Certification Authority	-
RA	Registration Authority	-
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	French National Cybersecurity Agency
GTCU	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	Prestataire de Vérification d'Identité à Distance	Remote Identity Verification Provider
QCP-n	Policy for EU qualified certificate issued to a natural person	-
QSCD	Qualified Signature Creation Device	-

2. General Terms and Conditions of Use

These GTCU are based on the template set out in Annex A of standard EN 319 411-1 (version 1.3.1).

Contact point	Youtrust Yousign CA management 36 rue de Saint Petersbourg 75008 Paris authority@yousign.com
Types of certificates, validation procedures and usage restrictions	The certificates covered by these GTCU are issued by the following Certification Authority chain: ● Root CA: "YOUSIGN SAS - ROOT2 CA" ○ Issuing CA: "YOUSIGN SAS - QUALIFIED SIGNATURE CA" The CA issues ephemeral qualified certificates, used in accordance with the process, for remote qualified electronic signature or advanced electronic signature within the meaning of the eIDAS Regulation. Qualified certificates for remote qualified electronic signature are issued following an initial remote identity verification. The holder's private key is generated and used within a remote qualified signature creation device (Remote QSCD). The holder may register a strong authentication means, compliant with the requirements applicable to electronic identification means at substantial level, allowing new remote qualified electronic signature certificates to be obtained. These certificates bear OID 1.2.250.1.302.1.16.1.0 and, where rules apply specifically to this type of certificate, they are identified in this document by the marker **[Qualified signature]**. The certificates may only be used within the framework of the signature service offered by Youtrust, to sign a document or a message in all areas where a signature is required for validity or evidentiary purposes, and in particular: ● electronic signature by a holder, followed by verification of that signature by a public administration or a company by electronic means; ● electronic signature by a holder, followed by verification of that signature by a natural person.

In addition to the authenticity and integrity of the data thus signed, such an electronic signature evidences the signatory's consent to the content of that data. A qualified electronic signature is furthermore presumed reliable and is equivalent, under the eIDAS Regulation, to a handwritten signature.

The holder is a natural person.

The DNs are constructed as follows:

Attribute	Description	Presence
CN	commonName: Surname and given name of the holder	Yes
SN	surname: Surname of the holder	Yes
GN	givenName: Given name of the holder	Yes
OI	organizationIdentifier: Identifier of the entity to which the holder is linked, using the eIDAS syntax: NTRFR-<SIREN number>	Only where there is a link with a legal entity
OU	organizationUnit: Identifier of the entity to which the holder is linked, using the RGS syntax: 0002 <SIREN number>	
O	organizationName: Name of the entity to which the holder is linked	
C	countryName: Country of Youtrust's registration authority, always equal to FR (France)	Yes
SerialNumber	serialNumber: Date and time at which certificate generation was started.	Yes

UID	userIdentifier: Transaction identifier of the signatory within the Youtrust infrastructure.	[Qualified signature] only

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 particular feature, test certificates issued by the CA "YOUSIGN SAS - QUALIFIED SIGNATURE CA" follow the same processes as nominal production certificates.

The use of a qualified certificate requires a process for verifying the holder's identity.

1. **Case of validation with a physical identity document**

Initial validation of the holder's identity is carried out on the RA's website during a remote face-to-face session. The remote verification process comprises the following steps:

- the holder connects to the RA's website via a unique link received at their email address, and must ensure that they have a smartphone equipped with a camera;
- the RA displays to the holder the identity information used for their certificate request:
  - surname and given name;
  - email address;
- the holder confirms having 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 consents to signing the certificate request form drawn up on that 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 receipt of an SMS;
	• the remote identity verification is carried out by a certified PVID provider (involving validation by a human operator), and includes the following steps:
	  ○ the holder accepts the GTCU and the privacy policy of the PVID service and consents to the processing of their biometric data so that the PVID can ascertain their identity;
	  ○ the holder ensures that they have a smartphone meeting the requirements set out by the PVID;
	  ○ the holder presents to the camera a valid official identity document from among the following:
	  ○ the identity card;
	  ○ the passport;
	  ○ the residence permit;
	  and follows the successive instructions given by the PVID;
	  ○ the PVID checks the validity and authenticity of the document presented and extracts the holder's identity information from it;
	  ○ the PVID asks the holder to present their face to the camera and to follow the instructions given to them 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 returns the result of the identity verification to the RA. The PVID's final verdict is sent asynchronously, after the items have been checked by a human operator. **2. Case of identity validation using an electronic identification means** Initial validation of the holder's identity is carried out on the website or mobile application of the electronic identification means provider. The remote verification process comprises the following steps: ● the holder must already hold an active electronic identification means supported by the RA; ● the holder connects to the RA's website via a unique link received at their email address; ● the RA displays to the holder the identity information used for their certificate request: ○ surname and given name; ○ email address; ● the holder confirms having 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 consents to signing the certificate request form drawn up on that basis; ● the holder is redirected to a web page or an application belonging to the electronic identification means provider; ● the holder must authenticate with the electronic identification means provider; ● the electronic identification means provider returns the result of the identity verification to the RA.

	The RA then archives the signed certificate request form, the signed GTCU and the evidence of the holder's identity verification. Following this initial identity verification, the holder may register an authentication means that will subsequently allow them to obtain new qualified certificates for qualified signature without repeating the initial identity verification. In the absence of such a means, the signatory will have to carry out a new initial identity verification at their next qualified electronic signature. The identity information contained in the ephemeral certificate generated for each signature is that validated during the remote face-to-face session. This information remains valid for a maximum period of 3 years before the holder is required to have the identity information validated again; this period must be shortened in line with the expiry date of the identity document or of the electronic identification means presented when the authentication means was issued. It is the holder's responsibility to request an update of the identity information if it were to become out of date before the 3-year period elapses. The holder must submit a request for revocation of their authentication means in the following cases: ● their private key is suspected of compromise, is compromised or is lost (together, where applicable, with the associated activation data); ● their authentication means for authorising a signature transaction has been compromised or is suspected of compromise. A revocation request guarantees to the holder that no new signature will be permitted with their current authentication means.
Usage limitations	The certificates issued may only be used for signature transactions handled by the Youtrust infrastructure. Holder certificates have a validity period of 120 minutes. The corresponding private keys have a lifetime equivalent to the duration of the signature process. Youtrust retains holder registration records for 10 years (20 years for certificates issued as part of an electronic signature process initiated by a Youtrust customer established in Italy).

	Youtrust retains for 17 years the logs and audit trails relating to the issuance and use of holders' private keys.
Holder obligations	The holder shall comply with the following requirements: ● undertake to provide up-to-date and valid identity items during the registration process; ● comply with the obligations relating to the remote identity verification service imposed by the remote identity verification provider; ● 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 GTCU; ● accept the retention by the CA of the information in the registration record and in the management of their signature keys; ● undertake to use the strong authentication means initially enrolled by the RA; ● use the signature certificate in compliance with the prescribed usage limitations; ● in order to guarantee sole control of their signature private key and where an authentication means is registered, the holder must: ○ configure robust authentication on their phone (PIN code or password, with a limit on the number of unlocking attempts); ○ never lend their phone, including to a trusted person; ○ 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 Youtrust; ○ in the event of permanent transfer of the phone to a third party (sale, assignment, etc.), apply the measures recommended by the phone manufacturer to reset it and contact Youtrust for revocation of the identity; ○ keep their phone up to date by installing the software updates offered by its manufacturer and by the operating system publisher; ○ install on the phone only applications published on the official stores of the operating system, avoid potentially dangerous applications (including jailbreak tools), and keep the installed applications up to date;

	○ keep their authentication private key and any other information relating to their identity confidential on their phone; ○ not share their authentication private key or any other information relating to their identity on another phone or device, even where that other phone or device belongs to the holder or to another person, including a trusted person. Any signature created after authentication on the phone is presumed to have been made by the holder who registered that 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 grounds for revocation is established: ○ the information appearing in their certificate no longer complies with the identity or the intended use stated in the certificate, this before the normal expiry of the certificate; ○ an error (whether intentional or not) has been detected in their registration record; ○ the holder's private key is suspected of compromise, is compromised or is lost (together, where applicable, with the associated activation data); ○ their authentication means for authorising a signature transaction has been compromised or is suspected of compromise; ● undertake to check the status of the signature certificate issued through the CRLs published by the CA and the OCSP service implemented; ● use the signature certificate under the conditions of use laid down by the CP and reproduced in these GTCU.
CA obligations	Youtrust is responsible for: ● the validation and publication of the CA's CP, CPS and GTCU; ● the compliance of the certificates issued with the CP; ● compliance with all security principles by the various components, and the related controls; ● in the event of a major incident (loss, suspected compromise, compromise or theft of the certificate management private key, for example), reporting the incident to ANSSI (supervision-eIDAS@ssi.gouv.fr).

	Youtrust is liable for any harmful consequence resulting from its own failure to comply with this document. Unless it can demonstrate that it has committed no intentional fault or negligence, Youtrust 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 registration; ● the issuance of the certificate was not subject to verification that the holder possessed the corresponding private key; ● the CA did not have the revocation of a certificate recorded and did not publish that information in accordance with its commitments. Youtrust is not liable for damage caused by a use of the certificate exceeding the limits set for its use. Should the CA cease its activity, the certificates issued that are still within their validity period will be revoked. Lastly, Youtrust accepts liability in the event of fault or negligence in the precautions to be taken as regards the confidentiality of the personal data entrusted to it by holders.
Certificate status checking	The user of a certificate is required to check the status of the certificates, including those in the corresponding chain of trust. The CA makes an up-to-date CRL available to users, 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 Youtrust also operates 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 “ExpiredCertsOnCRL” extension and retains the serial numbers of all revoked certificates, including those that have expired.

	The OCSP service implements the "archive cutoff" extension, as provided for by 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 query for a serial number not issued by the CA, the OCSP server will return the status "unknown" in the corresponding response. If the OCSP request contains a query for a serial number issued by the CA, the OCSP response will comply with the IETF standards RFC 6960. The certificates issued by the CA are qualified certificates under the eIDAS Regulation. This should be verified on the basis of the Trusted List issued by ANSSI at https://www.ssi.gouv.fr/eidas/TL-FR.xml. That list must in particular include the CA certificate and its qualification status. Should the CA be revoked, for example following a compromise of its private key, the revocation information is published in an ARL accessible at: ● http://crl.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl2.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl3.yousign.fr/crl/yousignsasroot2ca.crl In the event of the end of life of the CA, Youtrust will generate: ● a final CRL whose expiry date will be set to the value 99991231235959Z; ● a final OCSP response will be pre-generated for each certificate issued, containing an end-of-validity date set to the value 99991231235959Z. If Youtrust ceases the CA's activity, it undertakes to keep the CRLs and the pre-generated OCSP responses available.
Limitation of liability	Youtrust 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. Youtrust 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 holder.

	In any event, and to the strictest extent permitted by applicable law, Youtrust 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.
Applicable agreements and certification practices	The certificate policies describing the requirements that the CA intends to comply with are published at https://yousign.fr/fr/public/document, The service policy and the terms of use of the remote identity verification service of Youtrust's partner are applicable.
Confidentiality	The information regarded as confidential is at least the following: • the CA's internal procedures; • the private keys of the CA, of the components and of the certificate holders; • the activation data associated with the private keys of the CA and of the holders; • all PKI secrets; • the event logs of the PKI components; • the holder registration records; • the grounds for revocation, unless the holder expressly agrees otherwise. Youtrust applies security procedures to guarantee the confidentiality of this information. Youtrust undertakes to comply with the applicable laws and regulations.
Insurance policy	Youtrust certifies that it holds an insurance policy covering its professional civil liability. It undertakes to keep this insurance policy in force throughout the duration of its professional activity.
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	Youtrust 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 holder is informed that the issuance of electronic certificates and the performance of the electronic signature process involve the processing of personal data by Youtrust. The holder is invited to consult the Privacy Policy for further information on how their personal data is processed and on how to exercise their rights.
Audit and certification	The cryptographic module used by Youtrust for the CA and for the advanced electronic signature is qualified by ANSSI. The qualified electronic signature creation device is a remote qualified signature creation device ("Remote QSCD"), qualified under the eIDAS Regulation. The remote identity verification service is certified by ANSSI at the substantial or high level of assurance. The certificates comply with standard ETSI 319 411-2 and are qualified, within the meaning of the eIDAS Regulation, by ANSSI. The certificates are of QCP-n-qscd level. The certificates contain the following qualified fields: • esi4-qcStatement-4 = id-etsi-qcs-QcSSCD • esi4-qcStatement-1 = id-etsi-qcs-QcCompliance • esi4-qcStatement-6 = id-etsi-qct-esign