



Condiciones Generales de Uso de la AC YOUSIGN SAS - QUALIFIED SIGNATURE CA

v1.2.5 | Difusión: C1 – Público

Este documento es propiedad exclusiva de Youtrust.



HISTORIAL DE VERSIONES			
Versión	Objeto de la modificación	Fecha	Autor
1.2.5	Modificación de la razón social de Yousign a Youtrust (sección Presentación general y conjunto del documento); Rediseño del recorrido de registro del titular (sección Tipos de certificados, procedimientos de validación y restricciones de uso); Supresión de los servicios [Cara a cara físico]: OID 1.2.250.1.302.1.11.1.0 y [Cara a cara a distancia]: OID: 1.2.250.1.302.1.15.1.0; Generalización de la terminología "PVID" hacia un vocabulario multiproveedor; Cambio de la dirección del domicilio social (sección Punto de contacto).	2 jul. 2026	Tony DUFOUR
1.2.4	Cambio del periodo de vigencia de los certificados de los titulares a 60 minutos (15 minutos anteriormente).	23 ene. 2024	Tony DUFOUR
1.2.3	Modificación de la maquetación	3 oct. 2023	Sid Ahmed Remmide
1.2.2	Completado de los acrónimos y adición de las traducciones cuando proceda (sección acrónimos) Actualización de la dirección postal (sección condiciones generales de uso, apartado punto de contacto) Sustitución del término "cliente" por "titular" (sección condiciones generales de uso, apartado tipos de certificados, procedimientos de validación y restricciones de uso) Adición de una referencia a la Política de Certificación que describe el proceso de revocación y supresión de la información redundante con esta (sección condiciones generales de uso, apartado tipos de	9 may. 2023	Adrien Van Den Branden Tony Belot



	certificados, procedimientos de validación y restricciones de uso) Adición de obligaciones para el titular relativas a la conservación y a la comunicación de la clave privada de autenticación (sección condiciones generales de uso, apartado obligaciones de los titulares) Adición de los enlaces a las LCR de YOUSIGN SAS - QUALIFIED SIGNATURE CA (sección condiciones generales de uso, apartado comprobación del estado de los certificados) Precisión en cuanto al límite de la exoneración de daños y perjuicios (sección condiciones generales de uso, apartado limitación de responsabilidad) Cambio de nombre del apartado (sección condiciones generales de uso, apartado confidencialidad) Supresión de la referencia local a la legislación y a la normativa vigentes (sección condiciones generales de uso, apartado confidencialidad) Sustitución de los tribunales competentes de Caen por los de París (sección condiciones generales de uso, apartado legislación aplicable y resolución de conflictos) Revisión del contenido del apartado y adición de un enlace a la Política de Privacidad en línea (sección condiciones generales de uso, apartado gestión de los datos de carácter personal) Correcciones menores de faltas de ortografía y de formulación		
1.2.1	Supresión del campo cualificado esi4-qcStatement-5 de la sección condiciones generales de uso , apartado auditoría y certificación	27 ene. 2023	Sid Ahmed Remmide



1.2.0	Adición de una previsión en cuanto a la aceptación de las presentes CGU por los firmantes, como condición para la obtención de un certificado (sección presentación general) Referencia a las distintas políticas de certificación según el OID (sección identificación del documento) Adición del término QSCD (sección acrónimos) Actualización de la dirección postal de la sociedad Yousign (sección condiciones generales de uso, apartado punto de contacto) Adición de los certificados cualificados de firma electrónica cualificada, de tipo QCP-n-qscd, con el OID 1.2.250.1.302.1.16.1.0 (sección condiciones generales de uso, apartados tipos de certificados, procedimientos de validación y restricciones de uso y acuerdos aplicables y prácticas de certificación) Adición de la obligación para el titular de registrar un medio de autenticación en el caso del OID 1.2.250.1.302.1.11.1.0 (sección condiciones generales de uso, apartado tipos de certificados, procedimientos de validación y restricciones de uso) Adición del atributo UID en los DN en el caso del OID 1.2.250.1.302.1.16.1.0 (sección condiciones generales de uso, apartado tipos de certificados, procedimientos de validación y restricciones de uso) Modificación del componente responsable de la comparación de los apellidos y el nombre facilitados por la AR (sección condiciones generales de uso, apartado tipos de certificados, procedimientos de validación y restricciones de uso) Precisión del periodo de conservación de los expedientes de registro de los titulares	4 ene. 2023	Tony Belot
-------	--	-------------	----------------------------



	(sección condiciones generales de uso, apartado límites de utilización) Adición de las obligaciones de los titulares para los OID 1.2.250.1.302.1.15.1.0 y 1.2.250.1.302.1.16.1.0 (sección condiciones generales de uso, apartado obligaciones de los titulares) Adición de los documentos aplicables en relación con el PVID (sección condiciones generales de uso, apartado acuerdos aplicables y prácticas de certificación) Adición de las cualificaciones y certificaciones aplicables al Remote QSCD y al PVID (sección condiciones generales de uso, apartado auditoría y certificación) Adición de los niveles de certificado y de los campos cualificados adicionales (sección condiciones generales de uso, apartado auditoría y certificación) Corrección de errores tipográficos en los campos cualificados adicionales (sección Condiciones Generales de Uso, apartado Auditoría y certificación)		
1.1.1	Adición de las direcciones de publicación de la información de revocación de la AC, por ejemplo en caso de compromiso de esta (sección comprobación del estado de los certificados)	28 jul. 2022	Tony Belot
1.1.0	Modificación de la maquetación Adición del cara a cara a distancia Actualización de la cláusula "Gestión de los datos de carácter personal" en lo relativo a los derechos del titular Comprobación del certificado completada en relación con la Trusted List eIDAS Actualización y completado de las obligaciones del titular	27 may. 2022	Tony Belot



	Corrección de las URL de publicación de las LCR Precisión de los datos de contacto para el envío de las solicitudes de revocación		
1.0.4	Actualización de los acrónimos Modificación de la dirección de correo electrónico de contacto de la autoridad de certificación Actualización de la cláusula "Limitación de responsabilidad" Adición de las cláusulas "Gestión de los datos de carácter personal" y "Idioma"	21 dic. 2020	yves.rocha@yousign.com
1.0.3	Actualización de Comprobación del estado de los certificados. Precisión sobre la respuesta OCSP.	22 sept. 2020	Kévin Dubourg
1.0.2	Modificación de la maquetación	18 ago. 2020	Florent Eudeline
1.0.1	Actualización de las responsabilidades del titular y adición de una prueba de firma durante el registro del titular	2 nov. 2018	Antoine Louiset
1.0.0	Creación del documento	25 sept. 2018	Antoine Louiset



Índice

1. Introducción	6
1.1. Presentación general	6
1.2. Identificación del documento	7
1.3. Acrónimos	7
2. Condiciones Generales de Uso	8



1. Introducción

1.1. Presentación general

La sociedad Youtrust es un Prestador de Servicios de Certificación Electrónica (PSCE) que presta a sus clientes y utiliza para su propio uso servicios que implican certificados electrónicos y, en particular, una firma electrónica.

En este marco, el presente documento constituye las Condiciones Generales de Uso de los certificados expedidos por la Autoridad de Certificación «YOUSIGN SAS – QUALIFIED SIGNATURE CA». Este documento expone las modalidades de gestión de los certificados así como los compromisos y las obligaciones de las distintas partes.

El titular del certificado acepta expresamente estas Condiciones Generales de Uso en la fase de solicitud del certificado. En caso contrario, la Autoridad de Certificación «YOUSIGN SAS – QUALIFIED SIGNATURE CA» no podrá expedirle ningún certificado.

La sociedad Youtrust se denominó Yousign hasta el 01/07/2026, fecha en la que su denominación social se modificó en el Registro Mercantil (RCS) sin cambio del número SIREN. Por ello, las Autoridades de Certificación llevan el nombre de Yousign y conservan un identificador correcto de la persona jurídica Youtrust.

1.2. Identificación del documento

Las presentes «Condiciones Generales de Uso» se refieren a la AC «YOUSIGN SAS – QUALIFIED SIGNATURE CA», que expide certificados conforme a su Política de Certificación.

Los perfiles de certificado se identifican mediante sus respectivos OID:

- **[Firma cualificada]** : OID 1.2.250.1.302.1.16.1.0

Otros elementos, más explícitos (nombre, número de versión, fecha de actualización), permiten asimismo identificarlo.



1.3. Acrónimos

Acrónimo	Significado	Traducción
AC	Autoridad de Certificación	-
AR	Autoridad de Registro	-
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	Agencia Nacional francesa de Seguridad de los Sistemas de Información
CGU	Condiciones Generales de Uso	-
DN	Distinguished Name	Nombre distintivo
DPC	Declaración de Prácticas de Certificación	-
DPO	Data Protection Officer (Delegado de Protección de Datos)	-
eIDAS	electronic IDentification, Authentication and trust Services	Identificación electrónica y servicios de confianza
ICP	Infraestructura de Clave Pública	-
LRA	Lista de Revocación de Autoridades	-
LCR	Lista de Certificados Revocados	-
OCSP	Online Certificate Status Protocol	Protocolo de verificación en línea del estado de certificados
OID	Object Identifier	Identificador de objeto
PC	Política de Certificación	-
PVID	Prestataire de Vérification d'Identité à Distance	Proveedor de verificación de identidad a distancia
QCP-n	Policy for EU qualified certificate issued to a natural person (política para los certificados cualificados expedidos a una persona física)	-
QSCD	Qualified Signature Creation Device	Dispositivo cualificado de creación de firma electrónica



2. Condiciones Generales de Uso

Las presentes CGU se basan en el modelo previsto en el anexo A de la norma EN 319 411-1 (versión 1.3.1).

Punto de contacto	Youtrust Gestión de la AC Yousign 36 rue de Saint Petersburg 75008 Paris authority@yousign.com
Tipos de certificados, procedimientos de validación y restricciones de uso	Los certificados cubiertos por las presentes CGU son emitidos por la siguiente cadena de Autoridad de Certificación: • AC Raíz: «YOUSIGN SAS – ROOT2 CA» ◦ AC Emisora: «YOUSIGN SAS – QUALIFIED SIGNATURE CA» La AC expide certificados cualificados efímeros, utilizados según el proceso, para la firma electrónica cualificada a distancia o la firma electrónica avanzada en el sentido del Reglamento eIDAS. Los certificados cualificados para la firma electrónica cualificada a distancia se entregan tras una verificación inicial de identidad a distancia. La clave privada del titular se genera y se utiliza en un dispositivo cualificado de creación de firma a distancia (Remote QSCD). El titular puede registrar un medio de autenticación fuerte, conforme a los requisitos de los medios de identificación electrónica de nivel sustancial, que permite obtener nuevos certificados de firma electrónica cualificada a distancia. Estos certificados llevan el OID 1.2.250.1.302.1.16.1.0 y, cuando determinadas reglas se aplican específicamente a este tipo de certificado, se identifican en el presente documento mediante la mención [Firma cualificada]. Los certificados solo pueden utilizarse en el marco del servicio de firma ofrecido por Youtrust, para firmar un documento o un mensaje en todos los ámbitos para los que se exige una firma a efectos de validez o de prueba y, en particular:



- firma electrónica por un titular y posterior comprobación de esa firma por una administración o una empresa por vía electrónica;
- firma electrónica por un titular y posterior comprobación de esa firma por una persona física.

Además de la autenticidad y la integridad de los datos así firmados, dicha firma electrónica manifiesta el consentimiento del firmante en cuanto al contenido de esos datos. La firma electrónica cualificada se presume además fiable y es equivalente, en virtud del Reglamento eIDAS, a una firma manuscrita.

El titular es una persona física.

Los DN se construyen de la siguiente manera:

Atributo	Descripción	Presencia
CN	commonName: apellidos y nombre del titular	Sí
SN	surname: apellidos del titular	Sí
GN	givenName: nombre del titular	Sí
OI	organizationIdentifier: identificador de la entidad con la que el titular está vinculado, según la sintaxis eIDAS: NTRFR- <número de SIREN>	Únicamente en caso de vínculo con una persona jurídica
OU	organizationUnit: identificador de la entidad con la que el titular está vinculado, según la sintaxis RGS: 0002 <número de SIREN>	
O	organizationName: nombre de la entidad con la que el titular está vinculado	



	C	countryName: país de la autoridad de registro de Youtrust, siempre igual a FR (Francia)	Sí
	SerialNumber	serialNumber: fecha y hora de inicio de la generación del certificado.	Sí
	UID	userIdentifier: identificador de transacción del firmante en la infraestructura de Youtrust.	Únicamente [Firma cualificada]
Los certificados de prueba emitidos por la AC «YOUSIGN SAS – QUALIFIED SIGNATURE CA» son identificables de inmediato por la adición del prefijo «TEST – » en el valor del atributo CN, por ejemplo: CN = TEST – Jean DUPONT,... Al margen de esta particularidad, los certificados de prueba emitidos por la AC «YOUSIGN SAS – QUALIFIED SIGNATURE CA» siguen los mismos procesos que los certificados de producción nominal. La utilización de un certificado cualificado requiere un proceso de verificación de la identidad del titular. 1. Caso de la validación con un documento de identidad físico La validación inicial de la identidad del titular se realiza en el sitio web de la AR durante un cara a cara a distancia. El proceso de verificación a distancia comprende las siguientes etapas: • el titular se conecta al sitio de la AR mediante un enlace único recibido en su dirección de correo electrónico y debe asegurarse de disponer de un teléfono inteligente equipado con cámara;			



	• la AR muestra al titular los datos de identidad utilizados para su solicitud de certificado: ◦ apellidos y nombre; ◦ dirección de correo electrónico; • el titular confirma haber tomado conocimiento de las condiciones generales de uso vigentes y acepta firmarlas sin reserva; • el titular confirma la exactitud de los datos presentados y consiente en firmar el formulario de solicitud de certificado elaborado sobre esa base; • si el titular no se encuentra en un dispositivo móvil, se le pide continuar su identificación en un dispositivo móvil (equipado con cámara), mediante un código QR que debe escanear o mediante la recepción de un SMS; • la verificación de identidad a distancia es realizada por un prestador PVID certificado (que implica una validación por un operador humano) e incluye las siguientes etapas: ◦ el titular acepta las CGU y la política de privacidad del servicio PVID y consiente el tratamiento de sus datos biométricos para que el PVID pueda cerciorarse de su identidad; ◦ el titular se asegura de disponer de un teléfono inteligente que cumpla los requisitos expuestos por el PVID; ◦ el titular presenta a la cámara un documento oficial de identidad en vigor entre los siguientes justificantes: ◦ el documento nacional de identidad; ◦ el pasaporte; ◦ el permiso de residencia;
--	---



	y sigue las instrucciones sucesivas facilitadas por el PVID; ○ el PVID comprueba la validez y la autenticidad del documento presentado y extrae de él los datos de identidad del titular; ○ el PVID pide al titular presentar su rostro a la cámara y respetar las instrucciones que se le facilitan dinámicamente; ○ el titular sigue las instrucciones sucesivas facilitadas por el PVID; ○ el PVID se asegura de que el rostro del titular corresponde a la fotografía que figura en el documento de identidad; ○ el PVID devuelve el resultado de la verificación de identidad a la AR. El veredicto final del PVID se envía de manera asíncrona, tras la comprobación de los elementos por un operador humano. 2. Caso de la validación de una identidad mediante un medio de identificación electrónica La validación inicial de la identidad del titular se realiza en el sitio o en la aplicación móvil del proveedor del medio de identificación electrónica. El proceso de verificación a distancia comprende las siguientes etapas: ● el titular debe disponer previamente de un medio de identificación electrónica admitido por la AR y activo; ● el titular se conecta al sitio de la AR mediante un enlace único recibido en su dirección de correo electrónico; ● la AR muestra al titular los datos de identidad utilizados para su solicitud de certificado:
--	--



	○ apellidos y nombre; ○ dirección de correo electrónico; ● el titular confirma haber tomado conocimiento de las condiciones generales de uso vigentes y acepta firmarlas sin reserva; ● el titular confirma la exactitud de los datos presentados y consiente en firmar el formulario de solicitud de certificado elaborado sobre esa base; ● el titular es redirigido a una página web o a una aplicación perteneciente al proveedor del medio de identificación electrónica; ● el titular debe autenticarse ante el proveedor del medio de identificación electrónica; ● el proveedor del medio de identificación electrónica devuelve el resultado de la verificación de identidad a la AR. La AR archiva entonces el formulario de solicitud de certificado firmado, las CGU firmadas así como las pruebas de la verificación de identidad del titular. Tras esta verificación inicial de identidad, el titular puede registrar un medio de autenticación que le permitirá obtener posteriormente nuevos certificados cualificados de firma cualificada sin repetir la verificación inicial de identidad. En su defecto, el firmante deberá realizar una nueva verificación inicial de identidad en su siguiente firma electrónica cualificada. Los datos de identidad incluidos en el certificado efímero generado en cada firma son los que se validaron mediante el cara a cara a distancia. Estos datos siguen siendo válidos durante un periodo máximo de 3 años antes de que el titular esté obligado a volver a validar los datos de identidad; este periodo deberá reducirse en concordancia con la fecha de caducidad del documento de identidad o del medio de identificación electrónica presentado en el momento de la entrega del medio de autenticación. Es responsabilidad del titular solicitar una actualización de los datos de identidad si estos dejaran de estar actualizados antes del periodo de 3 años.
--	---



	El titular debe presentar una solicitud de revocación de su medio de autenticación en los siguientes casos: • se sospecha que su clave privada está comprometida, está comprometida o se ha perdido (eventualmente junto con los datos de activación asociados); • su medio de autenticación para autorizar una transacción de firma ha sido comprometido o se sospecha que lo ha sido. Una solicitud de revocación garantiza al titular que no se permitirá ninguna nueva firma con su medio de autenticación actual.
Límites de utilización	Los certificados expedidos solo pueden utilizarse para las transacciones de firma gestionadas por la infraestructura de Youtrust. Los certificados de los titulares tienen un periodo de validez de 120 minutos. Las claves privadas correspondientes tienen un periodo de vida equivalente a la duración del proceso de firma. Youtrust conserva durante 10 años los expedientes de registro de los titulares (20 años para los certificados expedidos en el marco de un proceso de firma electrónica iniciado por un cliente de Youtrust establecido en Italia). Youtrust conserva durante 17 años los registros y las trazas relativos a la expedición y a la utilización de las claves privadas de los titulares.
Obligaciones de los titulares	El titular tiene en cuenta los siguientes requisitos: • obligarse a facilitar datos de identidad actualizados y válidos durante el proceso de registro; • respetar las obligaciones relativas al servicio de verificación de identidad a distancia impuestas por el prestador de verificación de identidad a distancia; • aceptar tácitamente el certificado emitido por la AC validando la creación de la firma, tras la validación del formulario de solicitud y la aceptación de las CGU; • aceptar la conservación por parte de la AC de los datos del expediente de registro y de gestión de sus claves de firma; • obligarse a utilizar el medio de autenticación fuerte inscrito inicialmente por la AR; • utilizar el certificado de firma respetando los límites de utilización previstos;



	• para garantizar el control exclusivo de su clave privada de firma y en caso de registro de un medio de autenticación, el titular debe: ○ configurar una autenticación robusta en su teléfono (código PIN o contraseña, con límite del número de intentos de desbloqueo); ○ no prestar nunca su teléfono, ni siquiera a una persona de confianza; ○ en caso de pérdida o robo, aplicar las medidas recomendadas por el proveedor del teléfono (borrado a distancia, por ejemplo) y revocar la identidad contactando con Youtrust; ○ en caso de transmisión definitiva del teléfono a un tercero (venta, cesión, etc.), aplicar las medidas recomendadas por el proveedor del teléfono para restablecerlo y contactar con Youtrust para la revocación de la identidad; ○ mantener actualizado su teléfono, instalando las actualizaciones de software propuestas por su fabricante y por el desarrollador del sistema operativo; ○ instalar en el teléfono únicamente aplicaciones publicadas en las tiendas oficiales del sistema operativo, evitar las aplicaciones potencialmente peligrosas (incluidas las herramientas de jailbreak) y mantener actualizadas las aplicaciones instaladas; ○ conservar de manera confidencial en su teléfono su clave privada de autenticación y cualquier otro dato relativo a su identidad; ○ no compartir su clave privada de autenticación ni cualquier otro dato relativo a su identidad en otro teléfono o dispositivo, aun cuando ese otro teléfono o dispositivo perteneciera al titular o a otra persona, incluida una persona de confianza. Toda firma realizada tras la autenticación en el teléfono se presume efectuada por el titular que registró ese teléfono; el principio de no repudio no permite al titular negar haber firmado. • obligarse a avisar a la AC cuando se produzca una de las siguientes causas de revocación: ○ los datos que figuran en su certificado ya no se ajustan a la identidad o a la utilización prevista en
--	--



	el certificado, y ello antes de la expiración normal del certificado; ○ se ha detectado un error (intencionado o no) en su expediente de registro; ○ se sospecha que la clave privada del titular está comprometida, está comprometida o se ha perdido (eventualmente junto con los datos de activación asociados); ○ su medio de autenticación para autorizar una transacción de firma ha sido comprometido o se sospecha que lo ha sido; ● obligarse a comprobar el estado del certificado de firma expedido a través de las LCR publicadas por la AC y del servicio OCSP implantado; ● utilizar el certificado de firma en las condiciones de uso previstas por la PC y recogidas en las presentes CGU.
Obligaciones de la AC	Youtrust es responsable: ● de la validación y de la publicación de la PC, de la DPC y de las CGU de la AC; ● de la conformidad de los certificados emitidos con respecto a la PC; ● del respeto de todos los principios de seguridad por las distintas componentes y de los controles correspondientes; ● en caso de incidente grave (pérdida, sospecha de compromiso, compromiso o robo de la clave privada de gestión de los certificados, por ejemplo), de comunicar el incidente a la ANSSI (supervision-elDAS@ssi.gouv.fr). Youtrust es responsable de toda consecuencia dañosa derivada del incumplimiento del presente documento por su parte. Salvo que demuestre que Youtrust no ha cometido ninguna falta intencionada ni negligencia, Youtrust es responsable de todo perjuicio causado a cualquier persona física o jurídica que se confíe razonablemente en los certificados expedidos en cada uno de los siguientes casos: ● los datos contenidos en el certificado no corresponden a los datos facilitados en el momento del registro; ● la expedición del certificado no dio lugar a la comprobación de la posesión de la clave privada correspondiente por el titular; ● la AC no hizo registrar la revocación de un certificado ni publicó esa información conforme a sus compromisos.



	Youtrust no es responsable del perjuicio causado por un uso del certificado que exceda los límites fijados para su utilización. En caso de cese de la actividad de la AC, los certificados emitidos y aún dentro de su periodo de validez serán revocados. Por último, Youtrust asume su responsabilidad en caso de falta o de negligencia en las precauciones que deben adoptarse en materia de confidencialidad de los datos personales que le confían los titulares.
Comprobación del estado de los certificados	El usuario de un certificado está obligado a comprobar el estado de los certificados, incluidos los de la cadena de confianza correspondiente. La AC pone a disposición de los usuarios una LCR actualizada, publicada en Internet en el sitio: • http://crl.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl2.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl3.yousign.fr/crl/yousignsasqualifsignca.crl Youtrust implanta asimismo un servicio OCSP accesible en la siguiente dirección: http://ocsp.yousign.fr. Esta información está disponible siete días a la semana, veinticuatro horas al día, con una disponibilidad del 99,7 % en un mes. La LCR contiene la extensión «ExpiredCertsOnCRL» y conserva los números de serie de todos los certificados revocados, incluso los que han caducado. El servicio OCSP implanta la extensión «archive cutoff», según lo previsto en la RFC 6960, con una fecha idéntica a la fecha de inicio de validez del certificado de la AC y mantiene disponible el estado de revocación del certificado tras su caducidad. Si la solicitud OCSP contiene una consulta relativa a un número de serie no emitido por la AC, el servidor OCSP indicará en la respuesta correspondiente el estado «unknown». Si la solicitud OCSP contiene una consulta relativa a un número de serie emitido por la AC, la respuesta OCSP será conforme con los estándares IETF RFC 6960.



	Los certificados emitidos por la AC son certificados cualificados en virtud del Reglamento eIDAS. Conviene comprobarlo sobre la base de la lista de confianza (Trusted List) publicada por la ANSSI en https://www.ssi.gouv.fr/eidas/TL-FR.xml. Esta lista debe incluir en particular el certificado de la AC y su estado de cualificación. En caso de revocación de la AC, por ejemplo a raíz de un compromiso de su clave privada, la información de revocación se publica en una LRA accesible en: • http://crl.yousign.fr/crl/yousignsasroot2ca.crl • http://crl2.yousign.fr/crl/yousignsasroot2ca.crl • http://crl3.yousign.fr/crl/yousignsasroot2ca.crl En el caso de un fin de vida de la AC, Youtrust generará: • una última LCR cuya fecha de caducidad se fijará en el valor 99991231235959Z; • una última respuesta OCSP se pregenerará para cada certificado emitido, con una fecha de fin de validez fijada en el valor 99991231235959Z. Si Youtrust cesa la actividad de la AC, se compromete a mantener disponibles las LCR y las respuestas OCSP pregeneradas.
Limitación de responsabilidad	Youtrust no podrá ser considerada responsable de una utilización no autorizada o no conforme de los datos de autenticación, de los certificados, de las LCR, así como de cualquier otro equipo o software puesto a disposición. Youtrust declina su responsabilidad por cualquier daño derivado de los errores o de las inexactitudes que afecten a los datos contenidos en los certificados, cuando esos errores o inexactitudes resulten directamente del carácter erróneo de los datos comunicados por el titular. En todo caso, y en la estricta medida permitida por la legislación aplicable, Youtrust no podrá estar obligada al pago de daños y perjuicios, de cualquier naturaleza que sean, directos, materiales, comerciales, financieros o morales, con motivo de la ejecución de las presentes condiciones.



Acuerdos aplicables y prácticas de certificación	Las políticas de certificación que describen los requisitos que la AC pretende respetar están publicadas en la dirección https://yousign.fr/fr/public/document. La política de servicio y las condiciones de uso del servicio de verificación de identidad a distancia del socio de Youtrust son aplicables.
Confidencialidad	La información considerada confidencial es, al menos, la siguiente: • los procedimientos internos de la AC; • las claves privadas de la AC, de las componentes y de los titulares de certificados; • los datos de activación asociados a las claves privadas de la AC y de los titulares; • todos los secretos de la ICP; • los registros de eventos de las componentes de la ICP; • los expedientes de registro de los titulares; • las causas de revocación, salvo acuerdo explícito del titular. Youtrust aplica procedimientos de seguridad para garantizar la confidencialidad de esta información. Youtrust se compromete a respetar la legislación y la normativa vigentes.
Política de seguros	Youtrust certifica que es titular de una póliza de seguro que garantiza su responsabilidad civil profesional. Se compromete a mantener en vigor esta póliza de seguro durante toda la duración de su actividad profesional.
Idioma	Las presentes CGU se han redactado en varios idiomas, entre ellos el francés. El idioma de interpretación será el francés en caso de contradicción o de controversia sobre el significado de un término o de una disposición.
Legislación aplicable y resolución de conflictos	Las presentes CGU se rigen e interpretan conforme al derecho francés. En caso de litigio entre las partes derivado de la interpretación, de la aplicación y/o de la ejecución del contrato y en defecto de acuerdo amistoso entre las partes anteriormente citadas, la competencia exclusiva se atribuye a los tribunales de París.
Gestión de los datos de carácter personal	Youtrust se compromete a respetar la legislación y la normativa vigentes en materia de gestión de los datos de carácter personal, en particular el Reglamento europeo n.º



	2016/679, de 27 de abril de 2016, denominado «Reglamento General de Protección de Datos» (RGPD). Se informa al titular de que la expedición de certificados electrónicos y la ejecución del proceso de firma electrónica implican la realización por parte de Youtrust de tratamientos de datos de carácter personal. Se invita al titular a consultar la Política de Privacidad para obtener más información sobre cómo se tratan sus datos de carácter personal y sobre cómo ejercer sus derechos.
Auditoría y certificación	El módulo criptográfico utilizado por Youtrust para la AC y la firma electrónica avanzada está cualificado por la ANSSI. El dispositivo de creación de firma electrónica cualificada es un dispositivo cualificado de creación de firma a distancia ("Remote QSCD"), cualificado en virtud del Reglamento eIDAS. El servicio de verificación de identidad a distancia está certificado por la ANSSI en el nivel de seguridad sustancial o alto. Los certificados son conformes a la norma ETSI 319 411-2 y están cualificados, en el sentido del Reglamento eIDAS, por la ANSSI. Los certificados son de nivel QCP-n-qscd. Los certificados contienen los siguientes campos cualificados: • esi4-qcStatement-4 = id-etsi-qcs-QcSSCD • esi4-qcStatement-1 = id-etsi-qcs-QcCompliance • esi4-qcStatement-6 = id-etsi-qct-esign