Condizioni Generali di Utilizzo della CA YOUSIGN SAS - QUALIFIED SIGNATURE CA

v1.2.5 | Diffusione: C1 - Pubblico

STORICO DELLE VERSIONI			
Versione	**Oggetto della modifica**	**Data**	**Autore**
1.2.5	Modifica della ragione sociale da Yousign a Youtrust (sezione Presentazione generale e intero documento); Ridefinizione del percorso di registrazione del titolare (sezione Tipi di certificati, procedure di convalida e restrizioni d'uso); Eliminazione dei servizi **[Incontro fisico in presenza]**: OID 1.2.250.1.302.1.11.1.0 e **[Incontro a distanza]**: OID: 1.2.250.1.302.1.15.1.0; Generalizzazione della terminologia "PVID" verso una formulazione multi-fornitore; Modifica dell'indirizzo della sede legale (sezione Punto di contatto).	2 lug. 2026	Tony DUFOUR
1.2.4	Modifica della durata di vita dei certificati dei titolari a 60 minuti (precedentemente 15 minuti).	23 gen. 2024	Tony DUFOUR
1.2.3	Modifica dell'impaginazione	3 ott. 2023	Sid Ahmed Remmide
1.2.2	Completamento degli acronimi e aggiunta delle traduzioni ove applicabile (sezione acronimi) Aggiornamento dell'indirizzo postale (sezione condizioni generali di utilizzo, paragrafo punto di contatto) Sostituzione del termine “cliente” con “titolare” (sezione condizioni generali di utilizzo, paragrafo tipi di certificati, procedure di convalida e restrizioni d'uso) Aggiunta di un riferimento alla Politica di Certificazione che descrive il processo di revoca ed eliminazione delle informazioni ridondanti rispetto a essa (sezione condizioni generali di utilizzo, paragrafo tipi	9 mag. 2023	Adrien Van Den Branden Tony Belot

	di certificati, procedure di convalida e restrizioni d'uso) Aggiunta di obblighi per il titolare relativi alla conservazione e alla condivisione della chiave privata di autenticazione (sezione condizioni generali di utilizzo, paragrafo obblighi dei titolari) Aggiunta dei collegamenti alle CRL di `YOUSIGN SAS - QUALIFIED SIGNATURE CA` (sezione condizioni generali di utilizzo, paragrafo verifica dello stato dei certificati) Precisazione in merito al limite dell'esonero dal risarcimento dei danni (sezione condizioni generali di utilizzo, paragrafo limitazione di responsabilità) Ridenominazione del paragrafo (sezione condizioni generali di utilizzo, paragrafo riservatezza) Eliminazione del riferimento locale alla legislazione e alla normativa vigenti (sezione condizioni generali di utilizzo, paragrafo riservatezza) Sostituzione dei tribunali competenti di Caen con quelli di Parigi (sezione condizioni generali di utilizzo, paragrafo legge applicabile e risoluzione delle controversie) Revisione del contenuto del paragrafo e aggiunta di un rinvio alla Politica di Riservatezza online (sezione condizioni generali di utilizzo, paragrafo gestione dei dati personali) Correzioni minori di errori di ortografia e di formulazione		
1.2.1	Eliminazione del campo qualificato `esi4-qcStatement-5` dalla sezione condizioni generali di utilizzo, paragrafo audit e certificazione	27 gen. 2023	Sid Ahmed Remmide
1.2.0	Aggiunta di una previsione relativa all'accettazione delle presenti CGU da	4 gen. 2023	Tony Belot

	parte dei firmatari, quale condizione per l'ottenimento di un certificato (sezione presentazione generale) Riferimento alle diverse politiche di certificazione in base all'OID (sezione identificazione del documento) Aggiunta del termine QSCD (sezione acronimi) Aggiornamento dell'indirizzo postale della società Yousign (sezione condizioni generali di utilizzo, paragrafo punto di contatto) Aggiunta dei certificati qualificati per la firma elettronica qualificata, di tipo QCP-n-qscd, con OID 1.2.250.1.302.1.16.1.0 (sezione condizioni generali di utilizzo, paragrafi tipi di certificati, procedure di convalida e restrizioni d'uso e accordi applicabili e pratiche di certificazione) Aggiunta dell'obbligo per il titolare di registrare un mezzo di autenticazione nel caso dell'OID 1.2.250.1.302.1.11.1.0 (sezione condizioni generali di utilizzo, paragrafo tipi di certificati, procedure di convalida e restrizioni d'uso) Aggiunta dell'attributo UID nei DN nel caso dell'OID 1.2.250.1.302.1.16.1.0 (sezione condizioni generali di utilizzo, paragrafo tipi di certificati, procedure di convalida e restrizioni d'uso) Modifica del componente responsabile del confronto tra cognome e nome forniti dalla RA (sezione condizioni generali di utilizzo, paragrafo tipi di certificati, procedure di convalida e restrizioni d'uso) Precisazione della durata di conservazione dei fascicoli di registrazione dei titolari (sezione condizioni generali di utilizzo, paragrafo limitazioni d'uso)		

	Aggiunta degli obblighi dei titolari per gli OID 1.2.250.1.302.1.15.1.0 e 1.2.250.1.302.1.16.1.0 (sezione condizioni generali di utilizzo, paragrafo obblighi dei titolari) Aggiunta dei documenti applicabili in relazione al PVID (sezione condizioni generali di utilizzo, paragrafo accordi applicabili e pratiche di certificazione) Aggiunta delle qualificazioni e delle certificazioni applicabili al Remote QSCD e al PVID (sezione condizioni generali di utilizzo, paragrafo audit e certificazione) Aggiunta dei livelli di certificato e dei campi qualificati supplementari (sezione condizioni generali di utilizzo, paragrafo audit e certificazione) Correzione di errori tipografici nei campi qualificati supplementari (sezione Condizioni Generali di Utilizzo, paragrafo Audit e certificazione)		
1.1.1	Aggiunta degli indirizzi di pubblicazione delle informazioni di revoca della CA, ad esempio in caso di compromissione della stessa (sezione verifica dello stato dei certificati)	28 lug. 2022	Tony Belot
1.1.0	Modifica dell'impaginazione Aggiunta dell'incontro a distanza Aggiornamento della clausola "Gestione dei dati personali" per quanto riguarda i diritti del titolare Verifica del certificato completata in relazione alla Trusted List eIDAS Aggiornamento e completamento degli obblighi del titolare Correzione degli URL di pubblicazione delle CRL	27 mag. 2022	Tony Belot

	Precisazione dei recapiti per l'invio delle richieste di revoca		
1.0.4	Aggiornamento degli acronimi Modifica dell'indirizzo email di contatto dell'autorità di certificazione Aggiornamento della clausola "Limitazione di responsabilità" Aggiunta delle clausole "Gestione dei dati personali" e "Lingua"	21 dic. 2020	yves.rocha@yousign.com
1.0.3	Aggiornamento di Verifica dello stato dei certificati. Precisazione sulla risposta OCSP.	22 set. 2020	Kévin Dubourg
1.0.2	Modifica dell'impaginazione	18 ago. 2020	Florent Eudeline
1.0.1	Aggiornamento delle responsabilità del titolare e aggiunta di un test di firma durante la registrazione del titolare	2 nov. 2018	Antoine Louiset
1.0.0	Creazione del documento	25 set. 2018	Antoine Louiset

Indice

1. Introduzione

1.1. Presentazione generale

La società Youtrust è un Prestatore di Servizi di Certificazione Elettronica (PSCE) che fornisce ai propri clienti e utilizza per uso proprio servizi che comportano certificati elettronici e in particolare una firma elettronica.

In tale contesto, il presente documento costituisce le Condizioni Generali di Utilizzo dei certificati rilasciati dall'Autorità di Certificazione «YOUSIGN SAS - QUALIFIED SIGNATURE CA». Il presente documento illustra le modalità di gestione dei certificati nonché gli impegni e gli obblighi delle diverse parti.

Il titolare del certificato accetta espressamente le presenti Condizioni Generali di Utilizzo nella fase di richiesta del certificato. In caso contrario, nessun certificato può essergli rilasciato dall'Autorità di Certificazione «YOUSIGN SAS - QUALIFIED SIGNATURE CA».

La società Youtrust si è denominata Yousign fino al 01/07/2026, data in cui la sua denominazione sociale è stata modificata presso il Registro delle imprese (RCS) senza variazione del numero SIREN. Di conseguenza, le Autorità di Certificazione recano il nome Yousign e conservano un identificativo corretto della persona giuridica Youtrust.

1.2. Identificazione del documento

Le presenti «Condizioni Generali di Utilizzo» si riferiscono alla CA «YOUSIGN SAS - QUALIFIED SIGNATURE CA», che rilascia certificati secondo la propria Politica di Certificazione.

I profili dei certificati sono identificati dai rispettivi OID:

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

Altri elementi, più espliciti (nome, numero di versione, data di aggiornamento), consentono altresì di identificarlo.

1.3. Acronimi

Acronimo	Significato	Traduzione
CA	Autorità di Certificazione	-
RA	Autorità di Registrazione	-
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	Agenzia nazionale francese per la sicurezza dei sistemi informativi
CGU	Condizioni Generali di Utilizzo	-
DN	Distinguished Name	Nome distintivo
DPC	Dichiarazione delle Pratiche di Certificazione	-
DPO	Data Protection Officer (Responsabile della Protezione dei Dati)	-
eIDAS	electronic IDentification, Authentication and trust Services	Identificazione elettronica e servizi fiduciari
PKI	Public Key Infrastructure	Infrastruttura a chiave pubblica
ARL	Authority Revocation List	Elenco dei certificati di CA revocati
CRL	Certificate Revocation List	Elenco dei certificati revocati
OCSP	Online Certificate Status Protocol	Protocollo di verifica online dello stato dei certificati
OID	Object Identifier	Identificatore di oggetto
PC	Politica di Certificazione	-
PVID	Prestataire de Vérification d'Identité à Distance	Fornitore di verifica dell'identità a distanza
QCP-n	Policy for EU qualified certificate issued to a natural person (politica per i certificati qualificati rilasciati a una persona fisica)	-
QSCD	Qualified Signature Creation Device	Dispositivo qualificato per la creazione di firme elettroniche

2. Condizioni Generali di Utilizzo

Le presenti CGU sono basate sul modello previsto dall'allegato A della norma EN 319 411-1 (versione 1.3.1).

Punto di contatto	Youtrust Gestione della CA Yousign 36 rue de Saint Petersbourg 75008 Paris authority@yousign.com
Tipi di certificati, procedure di convalida e restrizioni d'uso	I certificati coperti dalle presenti CGU sono emessi dalla seguente catena di Autorità di Certificazione: ● CA Radice: «YOUSIGN SAS - ROOT2 CA» ○ CA Emittente: «YOUSIGN SAS - QUALIFIED SIGNATURE CA» La CA rilascia certificati qualificati effimeri, utilizzati secondo il processo, per la firma elettronica qualificata a distanza o la firma elettronica avanzata ai sensi del regolamento eIDAS. I certificati qualificati per la firma elettronica qualificata a distanza sono rilasciati previa verifica iniziale dell'identità a distanza. La chiave privata del titolare è generata e utilizzata all'interno di un dispositivo qualificato per la creazione di firme a distanza (Remote QSCD). Il titolare può registrare un mezzo di autenticazione forte, conforme ai requisiti dei mezzi di identificazione elettronica di livello significativo, che consente di ottenere nuovi certificati di firma elettronica qualificata a distanza. Tali certificati recano l'OID 1.2.250.1.302.1.16.1.0 e, quando determinate regole si applicano specificamente a questo tipo di certificato, esse sono identificate nel presente documento dalla dizione **[Firma qualificata]**. I certificati possono essere utilizzati esclusivamente nell'ambito del servizio di firma proposto da Youtrust, per firmare un documento o un messaggio in tutti gli ambiti per i quali è richiesta una firma a titolo di validità o di prova e in particolare: ● firma elettronica da parte di un titolare, seguita dalla verifica di tale firma da parte di una pubblica amministrazione o di un'impresa per via elettronica; ● firma elettronica da parte di un titolare, seguita dalla verifica di tale firma da parte di una persona fisica.

Oltre all'autenticità e all'integrità dei dati così firmati, tale firma elettronica manifesta il consenso del firmatario in merito al contenuto di tali dati. La firma elettronica qualificata è inoltre presunta affidabile ed è equivalente, ai sensi del regolamento eIDAS, a una firma autografa.

Il titolare è una persona fisica.

I DN sono costruiti come segue:

Attributo	Descrizione	Presenza
CN	commonName: cognome e nome del titolare	Sì
SN	surname: cognome del titolare	Sì
GN	givenName: nome del titolare	Sì
OI	organizationIdentifier: identificativo dell'entità con la quale il titolare è collegato, secondo la sintassi eIDAS: NTRFR-<numero SIREN>	Solo in caso di collegamento con una persona giuridica
OU	organizationUnit: identificativo dell'entità con la quale il titolare è collegato, secondo la sintassi RGS: 0002 <numero SIREN>	
O	organizationName: nome dell'entità con la quale il titolare è collegato	
C	countryName: paese dell'autorità di registrazione di Youtrust, sempre pari a FR (Francia)	Sì
SerialNumber	serialNumber: data e ora di avvio della generazione del certificato.	Sì

UID	userIdentifier: identificativo di transazione del firmatario nell'infrastruttura Youtrust.	Solo [Firma qualificata]

I certificati di test emessi dalla CA «YOUSIGN SAS - QUALIFIED SIGNATURE CA» sono immediatamente identificabili grazie all'aggiunta del prefisso «TEST – » nel valore dell'attributo CN, ad esempio:
CN = TEST – Jean DUPONT,...

Al di fuori di questa specificità, i certificati di test emessi dalla CA «YOUSIGN SAS - QUALIFIED SIGNATURE CA» seguono gli stessi processi dei certificati di produzione nominale.

L'utilizzo di un certificato qualificato richiede un processo di verifica dell'identità del titolare.

1. **Caso della convalida con un documento d'identità fisico**

La convalida iniziale dell'identità del titolare è effettuata sul sito web della RA nel corso di un incontro a distanza. Il processo di verifica a distanza comprende le fasi seguenti:

- il titolare si collega al sito della RA tramite un collegamento univoco ricevuto al proprio indirizzo email e deve assicurarsi di disporre di uno smartphone dotato di fotocamera;
- la RA mostra al titolare le informazioni identificative utilizzate per la sua richiesta di certificato:
  - cognome e nome;
  - indirizzo di posta elettronica;
- il titolare conferma di aver preso conoscenza delle condizioni generali di utilizzo in vigore e accetta di sottoscriverle senza riserve;
- il titolare conferma l'esattezza delle informazioni presentate e acconsente a firmare il modulo di richiesta di certificato redatto su tale base;

	• se il titolare non si trova su un dispositivo mobile, gli viene chiesto di proseguire l'identificazione su un dispositivo mobile (dotato di fotocamera), tramite la scansione di un QR code o tramite la ricezione di un SMS;
	• la verifica dell'identità a distanza è effettuata da un prestatore PVID certificato (con convalida da parte di un operatore umano) e comprende le fasi seguenti:
	  ○ il titolare accetta le CGU e la politica di riservatezza del servizio PVID e acconsente al trattamento dei propri dati biometrici affinché il PVID possa accertare la sua identità;
	  ○ il titolare si assicura di disporre di uno smartphone conforme ai requisiti indicati dal PVID;
	  ○ il titolare presenta alla fotocamera un documento ufficiale d'identità in corso di validità tra i seguenti:
	  ○ la carta d'identità;
	  ○ il passaporto;
	  ○ il permesso di soggiorno;
	  e segue le istruzioni successive fornite dal PVID;
	  ○ il PVID verifica la validità e l'autenticità del documento presentato e ne estrae le informazioni identificative del titolare;
	  ○ il PVID chiede al titolare di presentare il proprio volto alla fotocamera e di rispettare le istruzioni fornite dinamicamente;
	  ○ il titolare segue le istruzioni successive fornite dal PVID;
	  ○ il PVID accerta che il volto del titolare corrisponda alla fotografia presente sul documento d'identità;

	○ il PVID trasmette l'esito della verifica dell'identità alla RA. Il verdetto finale del PVID è inviato in modo asincrono, dopo la verifica degli elementi da parte di un operatore umano. **2. Caso della convalida di un'identità mediante un mezzo di identificazione elettronica** La convalida iniziale dell'identità del titolare è effettuata sul sito o sull'applicazione mobile del fornitore del mezzo di identificazione elettronica. Il processo di verifica a distanza comprende le fasi seguenti: ● il titolare deve disporre preventivamente di un mezzo di identificazione elettronica supportato dalla RA e attivo; ● il titolare si collega al sito della RA tramite un collegamento univoco ricevuto al proprio indirizzo email; ● la RA mostra al titolare le informazioni identificative utilizzate per la sua richiesta di certificato: ○ cognome e nome; ○ indirizzo di posta elettronica; ● il titolare conferma di aver preso conoscenza delle condizioni generali di utilizzo in vigore e accetta di sottoscriverle senza riserve; ● il titolare conferma l'esattezza delle informazioni presentate e acconsente a firmare il modulo di richiesta di certificato redatto su tale base; ● il titolare viene reindirizzato verso una pagina web o un'applicazione appartenente al fornitore del mezzo di identificazione elettronica; ● il titolare deve autenticarsi presso il fornitore del mezzo di identificazione elettronica;

	• il fornitore del mezzo di identificazione elettronica trasmette l'esito della verifica dell'identità alla RA. La RA archivia quindi il modulo di richiesta di certificato firmato, le CGU firmate nonché le prove della verifica dell'identità del titolare. A seguito di tale verifica iniziale dell'identità, il titolare può registrare un mezzo di autenticazione che gli consentirà di ottenere successivamente nuovi certificati qualificati di firma qualificata senza ripetere la verifica iniziale dell'identità. In sua assenza, il firmatario dovrà effettuare una nuova verifica iniziale dell'identità in occasione della successiva firma elettronica qualificata. Le informazioni identificative contenute nel certificato effimero generato per ciascuna firma sono quelle convalidate mediante l'incontro a distanza. Tali informazioni restano valide per una durata massima di 3 anni prima che il titolare sia obbligato a far convalidare nuovamente le informazioni identificative; tale durata deve essere ridotta in coerenza con la data di scadenza del documento d'identità o del mezzo di identificazione elettronica presentato al momento del rilascio del mezzo di autenticazione. È responsabilità del titolare richiedere un aggiornamento delle informazioni identificative qualora queste non fossero più aggiornate prima del termine dei 3 anni. Il titolare deve presentare una richiesta di revoca del proprio mezzo di autenticazione nei casi seguenti: • la sua chiave privata è sospettata di compromissione, è compromessa oppure è andata perduta (eventualmente con i dati di attivazione associati); • il suo mezzo di autenticazione per autorizzare una transazione di firma è stato compromesso o è sospettato di compromissione. Una richiesta di revoca garantisce al titolare che nessuna nuova firma sarà consentita con il suo attuale mezzo di autenticazione.
Limitazioni d'uso	I certificati rilasciati sono utilizzabili esclusivamente per le transazioni di firma gestite dall'infrastruttura Youtrust. I certificati dei titolari hanno una durata di validità di 120 minuti. Le corrispondenti chiavi private hanno una durata di vita equivalente alla durata del processo di firma.

	Youtrust conserva per 10 anni i fascicoli di registrazione dei titolari (20 anni per i certificati rilasciati nell'ambito di un processo di firma elettronica avviato da un cliente di Youtrust stabilito in Italia). Youtrust conserva per 17 anni i registri e le tracce relativi al rilascio e all'utilizzo delle chiavi private dei titolari.
Obblighi dei titolari	Il titolare prende atto dei seguenti requisiti: ● impegnarsi a fornire elementi identificativi aggiornati e validi durante il processo di registrazione; ● rispettare gli obblighi relativi al servizio di verifica dell'identità a distanza, imposti dal prestatore di verifica dell'identità a distanza; ● accettare tacitamente il certificato emesso dalla CA convalidando la creazione della firma, dopo la convalida del modulo di richiesta e l'accettazione delle CGU; ● accettare la conservazione da parte della CA delle informazioni del fascicolo di registrazione e di gestione delle proprie chiavi di firma; ● impegnarsi a utilizzare il mezzo di autenticazione forte inizialmente registrato dalla RA; ● utilizzare il certificato di firma nel rispetto delle limitazioni d'uso previste; ● per garantire il controllo esclusivo della propria chiave privata di firma e in caso di registrazione di un mezzo di autenticazione, il titolare deve: ○ configurare un'autenticazione robusta sul proprio telefono (codice PIN o password, con limite del numero di tentativi di sblocco); ○ non prestare mai il proprio telefono, nemmeno a una persona di fiducia; ○ in caso di perdita o furto, applicare le misure raccomandate dal fornitore del telefono (ad esempio la cancellazione a distanza) e revocare l'identità contattando Youtrust; ○ in caso di cessione definitiva del telefono a un terzo (vendita, cessione, ecc.), applicare le misure raccomandate dal fornitore del telefono per ripristinarlo e contattare Youtrust per la revoca dell'identità; ○ mantenere aggiornato il proprio telefono, installando gli aggiornamenti software proposti dal produttore e dallo sviluppatore del sistema operativo; ○ installare sul telefono solo applicazioni pubblicate sugli store ufficiali del sistema operativo, evitare le

	applicazioni potenzialmente pericolose (compresi gli strumenti di jailbreak) e mantenere aggiornate le applicazioni installate; ○ conservare in modo riservato sul proprio telefono la chiave privata di autenticazione e ogni altra informazione relativa alla propria identità; ○ non condividere la propria chiave privata di autenticazione o qualsiasi altra informazione relativa alla propria identità su un altro telefono o dispositivo, anche qualora tale altro telefono o dispositivo appartenga al titolare o a un'altra persona, compresa una persona di fiducia. Ogni firma effettuata dopo l'autenticazione sul telefono si presume apposta dal titolare che ha registrato tale telefono; il principio di non ripudio non consente al titolare di negare di aver firmato. ● impegnarsi ad avvertire la CA quando si verifica una delle seguenti cause di revoca: ○ le informazioni contenute nel suo certificato non sono più conformi all'identità o all'utilizzo previsto nel certificato, e ciò prima della normale scadenza del certificato; ○ è stato rilevato un errore (intenzionale o no) nel suo fascicolo di registrazione; ○ la chiave privata del titolare è sospettata di compromissione, è compromessa oppure è andata perduta (eventualmente con i dati di attivazione associati); ○ il suo mezzo di autenticazione per autorizzare una transazione di firma è stato compromesso o è sospettato di compromissione; ● impegnarsi a verificare lo stato del certificato di firma rilasciato mediante le CRL pubblicate dalla CA e il servizio OCSP attuato; ● utilizzare il certificato di firma nelle condizioni d'uso previste dalla PC e riprese nelle presenti CGU.
Obblighi della CA	Youtrust è responsabile: ● della convalida e della pubblicazione della PC, della DPC e delle CGU della CA; ● della conformità dei certificati emessi rispetto alla PC; ● del rispetto di tutti i principi di sicurezza da parte delle diverse componenti e dei relativi controlli;

	• in caso di incidente grave (ad esempio perdita, sospetta compromissione, compromissione o furto della chiave privata di gestione dei certificati), di segnalare l'incidente all'ANSSI (supervision-eIDAS@ssi.gouv.fr). Youtrust è responsabile di qualsiasi conseguenza dannosa derivante dal mancato rispetto del presente documento da parte della stessa. Salvo che dimostri di non aver commesso alcuna colpa intenzionale o negligenza, Youtrust è responsabile di qualsiasi pregiudizio causato a qualsiasi persona fisica o giuridica che si affidi ragionevolmente ai certificati rilasciati, in ciascuno dei casi seguenti: • le informazioni contenute nel certificato non corrispondono alle informazioni fornite in fase di registrazione; • il rilascio del certificato non è stato subordinato alla verifica del possesso della corrispondente chiave privata da parte del titolare; • la CA non ha fatto registrare la revoca di un certificato e non ha pubblicato tale informazione conformemente ai propri impegni. Youtrust non è responsabile del pregiudizio causato da un utilizzo del certificato che eccede i limiti fissati per il suo impiego. In caso di cessazione dell'attività della CA, i certificati emessi e ancora nel loro periodo di validità saranno revocati. Infine, Youtrust assume la propria responsabilità in caso di colpa o negligenza nelle precauzioni da adottare in termini di riservatezza dei dati personali affidatile dai titolari.
Verifica dello stato dei certificati	L'utilizzatore di un certificato è tenuto a verificare lo stato dei certificati, compresi quelli della corrispondente catena di fiducia. La CA mette a disposizione degli utilizzatori una CRL aggiornata, pubblicata su Internet all'indirizzo: • http://crl.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl2.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl3.yousign.fr/crl/yousignsasqualifsignca.crl Youtrust attua inoltre un servizio OCSP accessibile al seguente indirizzo: http://ocsp.yousign.fr.

	Tali informazioni sono disponibili sette giorni su sette, ventiquattro ore su ventiquattro, con una disponibilità del 99,7% su un mese. La CRL contiene l'estensione «ExpiredCertsOnCRL» e conserva i numeri di serie di tutti i certificati revocati, anche di quelli scaduti. Il servizio OCSP attua l'estensione «archive cutoff», come previsto dalla RFC 6960, con una data identica alla data di inizio di validità del certificato della CA e mantiene disponibile lo stato di revoca del certificato dopo la sua scadenza. Se la richiesta OCSP contiene un'interrogazione per un numero di serie non emesso dalla CA, il server OCSP inserirà nella risposta corrispondente lo stato «unknown». Se la richiesta OCSP contiene un'interrogazione per un numero di serie emesso dalla CA, la risposta OCSP sarà conforme agli standard IETF RFC 6960. I certificati emessi dalla CA sono certificati qualificati ai sensi del regolamento eIDAS. È opportuno verificarlo sulla base dell'elenco di fiducia (Trusted List) pubblicato dall'ANSSI all'indirizzo https://www.ssi.gouv.fr/eidas/TL-FR.xml. Tale elenco deve in particolare includere il certificato della CA e il suo stato di qualificazione. In caso di revoca della CA, ad esempio in seguito a una compromissione della sua chiave privata, l'informazione di revoca è pubblicata in una ARL accessibile all'indirizzo: • http://crl.yousign.fr/crl/yousignsasroot2ca.crl • http://crl2.yousign.fr/crl/yousignsasroot2ca.crl • http://crl3.yousign.fr/crl/yousignsasroot2ca.crl In caso di fine del ciclo di vita della CA, Youtrust genererà: • un'ultima CRL la cui data di scadenza sarà impostata al valore 99991231235959Z; • un'ultima risposta OCSP sarà pre-generata per ciascun certificato emesso, contenente una data di fine validità impostata al valore 99991231235959Z. Se Youtrust cessa l'attività della CA, si impegna a mantenere disponibili le CRL e le risposte OCSP pre-generate.
Limitazione di responsabilità	Youtrust non potrà essere ritenuta responsabile di un utilizzo non autorizzato o non conforme dei dati di autenticazione, dei

	certificati, delle CRL, nonché di qualsiasi altra apparecchiatura o software messo a disposizione. Youtrust declina la propria responsabilità per qualsiasi danno derivante da errori o inesattezze che inficino le informazioni contenute nei certificati, quando tali errori o inesattezze derivino direttamente dal carattere erroneo delle informazioni comunicate dal titolare. In ogni caso, e nella misura strettamente consentita dalla legge applicabile, Youtrust non potrà essere tenuta al pagamento di risarcimenti di qualsiasi natura, diretti, materiali, commerciali, finanziari o morali, in ragione dell'esecuzione delle presenti condizioni.
Accordi applicabili e pratiche di certificazione	Le politiche di certificazione che descrivono i requisiti che la CA intende rispettare sono pubblicate all'indirizzo https://yousign.fr/fr/public/document, Si applicano la politica di servizio e le condizioni di utilizzo del servizio di verifica dell'identità a distanza del partner di Youtrust.
Riservatezza	Le informazioni considerate riservate sono almeno le seguenti: • le procedure interne della CA; • le chiavi private della CA, delle componenti e dei titolari di certificati; • i dati di attivazione associati alle chiavi private della CA e dei titolari; • tutti i segreti della PKI; • i registri degli eventi delle componenti della PKI; • i fascicoli di registrazione dei titolari; • le cause di revoca, salvo accordo esplicito del titolare. Youtrust applica procedure di sicurezza per garantire la riservatezza di tali informazioni. Youtrust si impegna a rispettare la legislazione e la normativa vigenti.
Politica assicurativa	Youtrust certifica di essere titolare di una polizza assicurativa a garanzia della propria responsabilità civile professionale. Si impegna a mantenere in vigore tale polizza assicurativa per tutta la durata della propria attività professionale.
Lingua	Le presenti CGU sono state redatte in più lingue, tra cui il francese. La lingua di interpretazione sarà la lingua francese in

	caso di contraddizione o di contestazione sul significato di un termine o di una disposizione.
Legge applicabile e risoluzione delle controversie	Le presenti CGU sono disciplinate e interpretate secondo il diritto francese. In caso di controversia tra le parti derivante dall'interpretazione, dall'applicazione e/o dall'esecuzione del contratto e in mancanza di accordo amichevole tra le parti sopra indicate, la competenza esclusiva è attribuita ai tribunali di Parigi.
Gestione dei dati personali	Youtrust si impegna a rispettare la legislazione e la normativa vigenti in materia di gestione dei dati personali, in particolare il regolamento europeo n. 2016/679 del 27 aprile 2016 denominato «Regolamento Generale sulla Protezione dei Dati» (RGPD). Il titolare è informato del fatto che il rilascio di certificati elettronici e l'esecuzione del processo di firma elettronica comportano l'attuazione da parte di Youtrust di trattamenti di dati personali. Il titolare è invitato a consultare la Politica di Riservatezza per maggiori informazioni sulle modalità di trattamento dei propri dati personali e sulle modalità di esercizio dei propri diritti.
Audit e certificazione	Il modulo crittografico utilizzato da Youtrust per la CA e per la firma elettronica avanzata è qualificato dall'ANSSI. Il dispositivo per la creazione di firme elettroniche qualificate è un dispositivo qualificato per la creazione di firme a distanza ("Remote QSCD"), qualificato ai sensi del regolamento eIDAS. Il servizio di verifica dell'identità a distanza è certificato dall'ANSSI al livello di garanzia significativo o elevato. I certificati sono conformi alla norma ETSI 319 411-2 e sono qualificati, ai sensi del regolamento eIDAS, dall'ANSSI. I certificati sono di livello QCP-n-qscd. I certificati contengono i seguenti campi qualificati: • esi4-qcStatement-4 = id-etsi-qcs-QcSSCD • esi4-qcStatement-1 = id-etsi-qcs-QcCompliance • esi4-qcStatement-6 = id-etsi-qct-esign