



Autorità di certificazione e marcatura temporale

## Condizioni generali d'uso (CGU) - YOUSIGN SAS - SIGN2 CA

Esportata il 31/03/2021

---

Autore : Yves Rocha - 24/03/2021

Ultimo aggiornamento : Yves Rocha - 30/03/2021

Diffusione : C1 - Pubblico

Questo documento è di esclusiva proprietà di Yousign.



## Sommario :

1 - Storico delle modifiche.....	3
2 - Introduzione.....	4
2.1 - Presentazione generale .....	4
2.2 - Identificazione del documento .....	4
2.3 - Acronimi .....	4
3 - Condizioni Generali d'Uso .....	5



## 1 - Storico delle modifiche

Versione	Scopo della revisione	Data	Autore
1.1.4	Aggiornamento degli acronimi Modifica dell'indirizzo e-mail di contatto dell'autorità di certificazione Aggiornamento delle clausole "Limitazione di responsabilità" e "Gestione dei dati personali" Aggiunta di una clausola "Lingua" Clausole di "Risoluzione delle controversie" e "Legge applicabile" raggruppate nella stessa clausola	21 dic 2020	<a href="#">Yves</a> <a href="#">Rocha</a>
1.1.3	Modifica dell'impaginazione	18 ago 2020	<a href="#">Florent</a> <a href="#">Eudeline</a>
1.1.2	Creazione del documento	3 apr 2020	<a href="#">Antoine</a> <a href="#">Louiset</a>



## 2 - Introduzione

### 2.1 - Presentazione generale

Il presente documento definisce le Condizioni Generali d'Uso (CGU) dei certificati emessi nell'ambito del processo di firma elettronica da parte dell'Autorità di Certificazione "YOUSIGN SAS - SIGN2 CA".

Le presenti CGU sono accettate dal titolare del certificato durante il processo di firma. Lo scopo di questo documento è di presentare in maniera sintetica i requisiti rispettati dall'Autorità di Certificazione e che sono più esplicitamente definiti nella Politica di Certificazione dell'AC "YOUSIGN SAS - SIGN2 CA".

Il titolare del certificato è una persona fisica.

Se il titolare del certificato firma a nome e per conto di una persona giuridica, dichiara di avere facoltà di rappresentare legalmente tale persona giuridica nell'ambito dell'operazione alla quale viene applicato il processo di firma elettronica.

### 2.2 - Identificazione del documento

Questo documento è identificato dal numero di versione.

Tale numero è soggetto a modifiche indipendentemente dall'OID della Politica di Certificazione.

Questa versione delle CGU si applica pertanto ai seguenti OID:

- OID: 1.2.250.1.302.1.5.1.0 per i certificati di livello LCP nella norma ETSI 319 411-1,
- OID: 1.2.250.1.302.1.6.1.0 per i certificati generati con almeno un fattore di identificazione del Titolare da un'AR interna a Yousign,
- OID: 1.2.250.1.302.1.8.1.0 per i certificati generati con almeno un fattore di identificazione del Titolare da un'AR esterna a Yousign,

Gli elementi specifici di un OID saranno preceduti dall'OID tra parentesi quadre: [OID]. È possibile specificare più OID, separati da punto e virgola.

### 2.3 - Acronimi

AC	Autorità di Certificazione
AR	Autorità di Registrazione
CGU	Condizioni Generali d'Uso
DPC	Dichiarazione delle Pratiche di Certificazione
DPO	Data Protection Officer (Responsabile della protezione dei dati)
IGC	Infrastruttura di Gestione delle Chiavi
LCP	Lightweight Certificate Policy



LCR	Lista dei Certificati Revocati
OID	Object Identifier
PC	Politica di Certificazione
SMS	Short Message Service
URL	Uniform Resource Locator

### 3 - Condizioni Generali d'Uso

Contatti dell'Autorità di Certificazione	Gestione dell'AC Yousign Yousign SAS 8 allée Henri Pigis 14000 CAEN, Francia <a href="mailto:authority@yousign.com">authority@yousign.com</a>
Tipo di certificati emessi	<p>Le CGU si applicano ai certificati specificati nella sezione <a href="#">Identificazione del documento</a>. I certificati emessi dall'AC sono certificati di firma per i clienti di Yousign nell'ambito del processo di firma elettronica proposto da Yousign. Si tratta di certificati temporanei generati dall'AC per conto del titolare durante il processo di firma. Detti certificati non possono essere utilizzati in altri contesti.</p> <p>I certificati vengono emessi tramite la seguente catena di certificazione:</p> <pre>graph TD; A[YOUSIGN SAS - ROOT2 CA] --&gt; B[YOUSIGN SAS - SIGN2 CA]</pre> <p>I certificati della catena di certificazione sono disponibili al seguente indirizzo <a href="https://yousign.fr/fr/public/document">https://yousign.fr/fr/public/document</a>.</p>
Oggetto dei certificati	I certificati emessi dall'AC sono certificati destinati a persone fisiche. Vengono archiviati in un modulo protetto sotto il controllo dell'AC e possono essere utilizzati solo durante la transazione di firma.



Modalità di ottenimento	<p>Il titolare del certificato è una persona fisica.</p> <p>[OID : 1.2.250.1.302.1.5.1.0]</p> <p>La registrazione di un titolare avviene direttamente presso YOUSIGN che valida l'identità del titolare attraverso il suo documento di identità, il suo indirizzo e-mail e/o il suo numero di telefono.</p> <p>[OID : 1.2.250.1.302.1.6.1.0 ; 1.2.250.1.302.1.8.1.0]</p> <p>Viene quindi effettuata la validazione iniziale dell'identità del titolare: l'AR valida almeno un criterio di identificazione del titolare. Di seguito diamo un elenco non esaustivo dei criteri che possono essere verificati: codice univoco inviato per e-mail, codice univoco inviato tramite SMS, validazione di un documento di identità, scatto di una foto del firmatario.</p> <p><b>Validazione dell'identità di un soggetto per l'ottenimento di un certificato</b></p> <p>[OID : 1.2.250.1.302.1.5.1.0]</p> <p>La registrazione del futuro titolare richiede la validazione del suo documento di identità, dell'esistenza di un indirizzo e-mail e/o di un numero di telefono.</p> <p>I documenti di identità accettati sono:</p> <ul style="list-style-type: none"><li>• carta d'identità,</li><li>• passaporto,</li><li>• permesso di soggiorno.</li></ul> <p>Per fare ciò, eseguiremo il seguente processo:</p> <ul style="list-style-type: none"><li>• utilizzo di un URL univoco ;</li><li>• verifica del documento di identità inviato dal titolare ;</li><li>• invio di un codice di autenticazione (codice che consente di autenticare un titolare per validare una firma).</li></ul> <p>Una volta che il futuro titolare sarà andato sull'URL univoco, avrà caricato il suo documento di identità che verrà verificato immediatamente e ci avrà fornito il codice di autenticazione, la sua identità verrà validata.</p> <p>[OID : 1.2.250.1.302.1.6.1.0 ; 1.2.250.1.302.1.8.1.0]</p> <p>La registrazione del futuro titolare richiede la verifica di un parametro di identificazione. L'identificazione può essere eseguita in diversi modi. Di seguito diamo un elenco non esaustivo dei criteri che possono essere verificati: codice univoco inviato per e-mail, codice univoco inviato tramite SMS, validazione di un documento di identità, scatto di una foto del firmatario.</p> <p>Per fare ciò, eseguiremo il seguente processo:</p> <ul style="list-style-type: none"><li>• utilizzo di un URL univoco ;</li><li>• identificazione del firmatario tramite il sistema prescelto ;</li></ul> <p>Una volta che il futuro titolare sarà andato sull'URL univoco, effettuerà l'identificazione richiesta, la sua identità verrà validata.</p>
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Metodo di accesso alla chiave privata e utilizzo del certificato di firma**

La chiave privata è completamente gestita, archiviata e protetta dall'infrastruttura Yousign.

Implementiamo comunque mezzi tecnici e organizzativi per garantire che la chiave privata sarà utilizzata solo dal titolare. In nessun caso Yousign potrà utilizzare detta chiave per uso proprio o per conto di qualcuno che non sia il titolare.

La chiave privata è associata in maniera logica al titolare e quest'ultimo è l'unico ad avere i dati di attivazione.

Per utilizzare la propria chiave privata, il titolare dovrà infatti autenticarsi successivamente tramite due canali:

- attraverso l'ottenimento di un URL univoco ;
- tramite un codice di autenticazione.

Si fa notare che l'ottenimento dell'URL univoco è trasparente per il titolare perché viene inviato tramite e-mail quando il titolare clicca sul pulsante che consente l'accesso ai documenti da firmare oppure in modo trasparente se il processo di firma è incorporato in un'applicazione terza gestita dal cliente di Yousign.

La nostra architettura tecnica consente l'utilizzo di una chiave privata solo se il codice di autenticazione è inserito dall'utente. Inoltre, una firma effettuata tramite l'AC "YOUSIGN SAS - SIGN2 CA" è valida solo se l'IGC Yousign può attestare il ciclo completo di una richiesta di firma tramite una serie di registri e di tracce che sono documentati. Detti registri e tracce restano archiviati per 17 anni.

Modalità di rinnovo

Non è previsto alcun processo di rinnovo.

Modalità di revoca

La richiesta di revoca di un certificato può essere effettuata per telefono o e-mail. La procedura è la seguente:

- Revoca per telefono: l'utente può contattare telefonicamente Yousign per chiedere la revoca del proprio certificato. A tal fine, Yousign si accerterà della sua identità. Al titolare verrà posta una serie di 2 domande casuali riguardanti la sua identità. Tale domande saranno basate sulle informazioni in possesso di Yousign. La validazione sarà effettiva, a seguito di una conferma ottenuta tramite un canale diverso dalla telefonata. Per esempio, possiamo inviargli un link di conferma al suo indirizzo e-mail.
- Revoca tramite posta elettronica: l'utente può contattare telefonicamente Yousign per chiedere la revoca del proprio certificato. A tal fine, Yousign si accerterà della sua identità. Al titolare verrà posta una serie di 2 domande casuali riguardanti la sua identità. Tale domande saranno basate sulle informazioni in possesso di Yousign. La validazione sarà effettiva, a seguito di una conferma ottenuta tramite un canale diverso dall'e-mail. Per esempio, possiamo:
  - inviargli un codice sul suo numero di telefono
  - chiamarlo al telefono per avere una conferma

La revoca di un certificato può avvenire solo durante il periodo di validità del certificato stesso, cioè durante i 15 minuti successivi alla generazione del certificato.

Tale periodo estremamente breve comporta il fatto che il processo di revoca sarà difficilmente utilizzabile nell'ambito della PC associata.



Limiti di utilizzo	<p>I certificati emessi sono utilizzabili solo per le transazioni di firma fornite dall'infrastruttura Yousign.</p> <p>I certificati dei titolari hanno una durata di validità di 15 minuti. Le corrispondenti chiavi private hanno una durata equivalente alla durata del processo di firma.</p> <p>Yousign conserva per 17 anni i registri e le tracce riguardanti l'emissione e l'uso delle chiavi private dei titolari.</p>
Obblighi dei titolari	<p>Il titolare ha il dovere di:</p> <ul style="list-style-type: none"><li>• comunicare informazioni accurate e aggiornate al momento della richiesta o del rinnovo del certificato ;</li><li>• proteggere i propri dati di autenticazione ;</li><li>• accettare le presenti condizioni generali d'uso ;</li><li>• verificare che i dati presenti nel certificato del documento firmato che gli è stato consegnato siano corretti ;</li><li>• richiedere il rinnovo del suo certificato con un ragionevole anticipo prima della scadenza ;</li><li>• fare senza indugio una richiesta di revoca del suo certificato a Yousign in caso di compromissione o sospetta compromissione dei suoi dati di autenticazione.</li></ul> <p>L'accettazione di un certificato emesso dall'AC è tacita una volta effettuata la firma tramite il sistema di firma Yousign.</p> <p>Prima di tale utilizzo, il titolare può rifiutare la generazione del certificato interrompendo il processo di firma. Se la doppia chiave era già stata generata, quest'ultima verrà distrutta in modo automatico da un processo tecnico.</p>
Obblighi di verifica dei certificati da parte degli utenti	<p>Gli utenti dei certificati devono:</p> <ul style="list-style-type: none"><li>• verificare e rispettare l'uso per il quale è stato emesso il certificato ;</li><li>• per ogni certificato della catena di certificazione, dal certificato del titolare fino all'AC "YOUSIGN SAS – ROOT2 CA", verificare la firma digitale dell'AC che ha emesso il certificato in questione e controllare la validità di tale certificato (date di validità, stato di revoca) ; gli utenti possono utilizzare un file firmato per eseguire questi controlli. Il contenuto del certificato può essere verificato e controllato.</li><li>• verificare e rispettare gli obblighi degli utenti dei certificati indicati nella PC.</li></ul>
Limitazione di responsabilità	<p>Yousign non può essere ritenuta responsabile per qualsiasi utilizzo non autorizzato o non conforme dei dati di autenticazione, dei certificati, degli LCR, nonché di qualsiasi altro dispositivo o software messo a disposizione.</p> <p>Yousign declina ogni responsabilità per eventuali danni derivanti da errori o inesattezze nelle informazioni contenute nei certificati, quando tali errori o inesattezze derivino direttamente dalla natura errata delle informazioni comunicate dal titolare.</p> <p>In ogni caso, Yousign non può essere ritenuta responsabile per il pagamento di danni di qualsiasi natura, diretti, materiali, commerciali, finanziari o morali, a seguito dell'esecuzione del presente documento.</p>





Riferimenti documentali	La Politica di Certificazione dell'AC "YOUSIGN SAS - SIGN2 CA" è accessibile al seguente indirizzo: <a href="https://yousign.fr/fr/public/document">https://yousign.fr/fr/public/document</a> . La DPC è accessibile su richiesta all'AC utilizzando i dati di contatto più sopra forniti.
Condizioni di risarcimento	Non applicabile
Lingua	Le presenti CGU sono state redatte in più lingue, tra cui il francese. La lingua d'interpretazione sarà la lingua francese in caso di contraddizione o contestazione del significato di un termine o di una disposizione.
Legge applicabile e risoluzione delle controversie	Le presenti CGU sono disciplinate e interpretate secondo la legge francese. In caso di controversia tra le parti derivante dall'interpretazione, dall'applicazione e/o dall'esecuzione del contratto e in mancanza di un accordo amichevole tra le suddette parti, il foro competente in via esclusiva sono i tribunali di Caen.
Gestione dei dati personali	Yousign si impegna a rispettare le leggi e i regolamenti vigenti in materia di gestione dei dati personali, in particolare il Regolamento Europeo n. 2016/679 del 27 aprile 2016 noto come "Regolamento Generale sulla Protezione dei Dati" (GDPR). Si informa il titolare che l'emissione di certificati elettronici e l'esecuzione del processo di firma elettronica presuppone l'attuazione da parte di Yousign di trattamenti dei dati personali a cui il titolare acconsente, in conformità con la politica di riservatezza di Yousign disponibile all'indirizzo <a href="https://yousign.com/it-it/privacy">https://yousign.com/it-it/privacy</a> . Il titolare è informato che la comunicazione dei suoi dati è obbligatoria e necessaria per poter prendere in considerazione la sua richiesta e per l'esecuzione del processo di firma elettronica. Il titolare ha il diritto di accesso, modifica, rettifica e cancellazione dei dati che lo riguardano, nonché un diritto di opposizione da formulare al DPO di Yousign, all'indirizzo <a href="mailto:dpo@yousign.com">dpo@yousign.com</a> .
Auditing e riferimenti applicabili	L'Autorità di Certificazione "YOUSIGN SAS - SIGN2 CA" è certificata conforme, per i certificati emessi secondo la politica 1.2.250.1.302.1.5.1.0, alla norma ETSI 319 411-1 per il livello LCP. Yousign ha in essere un Comitato di Direzione Tecnico Yousign. Quest'ultimo procede alla validazione della conformità della DPC rispetto alla PC. Viene effettuato un controllo di conformità al momento della messa in servizio del sistema e in seguito ad ogni modifica significativa. Inoltre, almeno ogni anno verrà effettuato un auditing. Gli audit sono svolti internamente da personale di Yousign o sotto forma di un servizio effettuato da società specializzate nella sicurezza dei sistemi d'informazione e che hanno riconosciute competenze nel campo della firma elettronica. Nell'ambito dell'ottenimento delle certificazioni dei servizi dell'IGC, l'auditing di certificazione è svolto da una società esterna debitamente accreditata.



<p>Convenzione di prova</p>	<p>Per ogni firma elettronica effettuata, Yousign e il Titolare concordano che:</p> <ul style="list-style-type: none"><li>• gli elementi di identificazione utilizzati per effettuare la firma elettronica dei documenti, ovvero il nome e il cognome del Titolare, il numero di telefono personale utilizzato, il suo indirizzo e-mail, il Certificato Elettronico di Firma, i documenti giustificativi,</li><li>• gli elementi di marcatura temporale,</li><li>• le procedure utilizzate per firmare elettronicamente i documenti (per esempio inserendo il codice di sicurezza inviato tramite SMS),</li><li>• il dossier delle prove contenente una serie di tracce informatiche,</li></ul> <p>siano ammissibili in tribunale e dimostrino i dati e gli elementi in essi contenuti, nonché le procedure di autenticazione che essi esprimono.</p> <p>Detta cartella sarà poi archiviata e munita di marcatura temporale da parte del terzo archiviatore.</p>
<p>Archiviazione presso un terzo archiviatore</p>	<p>Nel caso in cui il cliente di Yousign abbia sottoscritto l'opzione di archiviazione dei documenti firmati elettronicamente, quest'ultimi saranno archiviati presso un terzo archiviatore (CDC ARKHINEO), in condizioni tali da garantire la sicurezza e l'integrità nel tempo, ai sensi dei requisiti dell'articolo 1367 del Codice Civile francese.</p>