Contratto di Sottoscrizione di Certificato SSL

1. Definizioni

Archivio: si intende la raccolta di documenti accessibile mediante collegamento all'archivio attraverso il sito Web della Società (www.trustitalia.it) e dei suoi Fornitori alla quale il Sottoscrittore ha richiesto il proprio Certificato, ad esempio www.symantec.com, www.thawte.com, www.geotrust.com e www.rapidssl.com.
Autorità di certificazione o CA: si intende un'entità autorizzata al rilascio, alla gestione, alla revoca e al rinnovo di Certificati all'interno di una PKI. Ai fini del presente Contratto, ove applicabile, Trust Italia S.p.A. e DigiCert Inc. Autorità di certificazione.
Autorità di registrazione o RA: si intende un'entità autorizzata da un'Autorità di certificazione per assistere i Richiedenti certificato e per approvare o rifiutare le Richieste di certificato, revocare i Certificati stessi o rinnovarli.
Contratto di licenza del simbolo: si intende il contratto sottoscritto tra il Sottoscrittore e la Società che disciplina gli obblighi e gli utilizzi del titolare in relazione al Simbolo Symantec™ e/oNorton™ (oppure, a seconda, al Simbolo GeoTrust®, Thawte® o RapidSSL™), disponibile nell'archivio del produttore.
Certificato: si intende un messaggio che, come minimo, nomina o identifica un'Autorità di certificazione (CA), identifica il Sottoscrittore, contiene la chiave pubblica del Sottoscrittore, identifica il Periodo operativo del Certificato, contiene il numero di serie del Certificato ed è firmato digitalmente dall'Autorità di certificazione (CA).
Certificato SSL: si intende un Certificato utilizzato per supportare sessioni SSL tra un browser Web (o altro client) ed un server Web che utilizza la crittografia.
Dichiarazione delle procedure di certificazione o CPS: si intende una dichiarazione delle procedure adottate da un'Autorità di certificazione o di registrazione per approvare o rifiutare le Richieste di certificato e per rilasciare, gestire e revocare i Certificati. La CPS è pubblicata nell'archivio web della CA.
Infrastruttura a chiave pubblica o PKI: si intende l'infrastruttura a chiave pubblica basata sul Certificato e disciplinata dalla politica di certificazione della CA che abilita la diffusione a livello mondiale e l'utilizzo dei Certificati da parte della Società, Fornitori, delle sue consociate, dei loro rispettivi clienti, Sottoscrittori e Parti cedenti. La PKI di Symantec è denominata "Symantec Trust Network" o "STN"; la PKI di GeoTrust e RapidSSL è denominata "PKI GeoTrust"; e la PKI di Thawte è denominata "PKI Thawte".
Opzione di certificato con licenza: si intende l'opzione di servizio che concede a un Sottoscrittore il diritto di utilizzare un Certificato su un dispositivo fisico (di seguito "Dispositivo fisico iniziale") e di ottenere licenze aggiuntive per il Certificato per (i) server fisici aggiuntivi o dispositivi fisici protetti dal Dispositivo fisico iniziale, a titolo esemplificativo ma non esaustivo, server protetti con un bilanciatore di carico su cui è installato il Certificato; o (ii) server fisici aggiuntivi in cui sono installati certificati replicati. Questa opzione potrebbe non essere disponibile per qualsiasi Sottoscrittore. Dipendendo dalla tipologia del prodotto, le Opzioni di certificato con licenza potrebbero essere a pagamento, incluse o illimitate
Parte cedente (Relying Party): si intende un individuo o un'organizzazione che opera facendo affidamento su un Certificato e/o una firma digitale.
Periodo operativo: si intende il periodo che inizia alla data e all'ora di rilascio di un Certificato (o data e ora certa successive, se specificato nel Certificato) e termina alla data e all'ora di scadenza o revoca anticipata del Certificato.
Piano di protezione: si intende il programma di garanzia estesa offerto dalla Società, così come descritto nell'archivio web . Il Piano di protezione di Symantec è denominato "Piano di protezione NetSure" (https://www.websecurity.symantec.com/content/dam/websitesecurity/digitalassets/desktop/pdfs/repository/netsure-protection-plan.pdf); il Piano di protezione di GeoTrust e RapidSSL è denominato "Piano di protezione GeoSure" (https://www.symantec.com/content/en/us/about/media/repository/netsure-protection-plan.pdf); il Piano di protezione di Thawte è denominato "Piano di protezione Thawte"(https://www.thawte.com/assets/documents/repository/agreements/extended-warranty-program.pdf).
Relying Party Agreement o RPA (Accordo della parte cedente): si intende un contratto in virtù del quale l'Autorità di certificazione stabilisce i termini e condizioni a fronte dei

quali un individuo o un'organizzazione opera in qualità di Parte cedente, nello specifico si intende l'Accordo della parte cedente pubblicato nell'archivio.

Richiedente certificato: si intende un individuo o un'organizzazione che come Sottoscrittore richiede il rilascio di un Certificato da parte di un'Autorità di certificazione. Il Richiedente certificato è in grado di utilizzare, ed è autorizzato a farlo, la chiave privata corrispondente alla chiave pubblica elencata nel Certificato

Richiesta di certificato: si intende una richiesta da parte di un Richiedente certificato (o suo agente autorizzato) ad un'Autorità di certificazione (CA) con l'obiettivo di ottenere il rilascio di un Certificato.

Rivenditore o Partner: si intende un'entità autorizzata dalla Società a rivendere i Certificati o i Servizi disciplinati dal presente Contratto.

Simbolo (Seal): si intende un'immagine elettronica che rappresenta un marchio Symantec™ e/o Norton™ (oppure, ove applicabile, il marchio GeoTrust®, Thawte® o RapidSSL™) che, quando mostrato dal Sottoscrittore sul proprio sito Web, indica che questi ha acquistato uno o più Servizi della Società e che, facendovi clic sopra, mostra determinate informazioni relative ai Servizi e al loro stato di attivazione.

Servizi: si intende collettivamente il servizio di certificato digitale e qualsiasi prodotto, beneficio o utilità correlati che la Società renda disponibile al Sottoscrittore mediante l'acquisto del certificato SSL.

Symantec, Symantec Trust Network o STN: si intende l'Infrastruttura a chiave pubblica disciplinata da Symantec Trust Network CPS che abilita la diffusione a livello mondiale e l'utilizzo dei Certificati da parte di DigiCert Inc. e di Trust Italia S.p.A. come CA Intermedia , delle sue consociate, dei loro rispettivi clienti, Sottoscrittori e Parti cedenti.

Titolare: si intende in caso di Certificato individuale, l'individuo fisico a cui è stato rilasciato un Certificato e ne è dunque titolare. In caso invece di un Certificato per un'organizzazione, si intende l'organizzazione, proprietaria dell'apparecchiatura o del dispositivo, a cui è stato rilasciato un Certificato e ne è dunque titolare.

2. Oggetto del contratto

2.1. Il presente CONTRATTO regola le modalità con cui la Società fornisce al Sottoscrittore i Certificati SSL definendo al tempo stesso i termini e le condizioni che si applicano al sottoscrittore nell'utilizzo dei suddetti Certificati SSL.

2.2. Al presente contratto si applicano le condizioni generali di contratto esposte all'indirizzo https://www.trustitalia.it//archivio/legal_agreements/Condizioni_Generali_di_Contratto_Trust_Italia_v1.pdf

3. Perfezionamento del contratto

3.1. Il presente Contratto si perfeziona, quale accettazione della proposta contrattuale ai sensi dell'Art. 1326 cod. civ., tramite l'accettazione dello stesso, da parte del Sottoscrittore, con il sistema del "point and click" sulle pagine di registrazione del Sito "www.trustitalia.it" .

3.2. Utilizzando il Certificato, il sottoscrittore dichiara e garantisce di avere pieno titolo a stipulare il presente contratto, di adempiere in toto agli obblighi che ne derivano, di rappresentare una parte nell'ambito del contratto e di essere vincolato dai termini in esso contenuti.

3.3. L'effettuazione della richiesta e l'accettazione o l'utilizzazione di qualsiasi Certificato rilasciato in virtù del presente contratto comporta la piena accettazione dei termini e delle condizioni del Contratto da parte del Richiedente certificato

3.4. Nel caso in cui il Sottoscrittore e Richiedente certificato sia un rivenditore e agisca in qualità di rappresentante autorizzato di un Titolare al fine di richiedere un certificato, lo stesso accetta le dichiarazioni e le garanzie come stabilito nel presente contratto, ed in particolare garantisce che il Titolare abbia autorizzato detto rivenditore a richiedere, accettare, installare, mantenere, rinnovare e, se necessario, revocare il certificato per suo conto

4. Fornitore del Servizio

4.1. Al fine di espletare le richieste del Sottoscrittore, la Società potrà emettere/produrre direttamente il certificato oppure rivendere al Sottoscrittore i Servizi/Prodotti di altri (Fornitore, Produttore o CA). DigiCert Inc. è un Fornitore esplicitamente espresso.

4.2. Nel caso in cui il Prodotto/Servizio si fornito da altri, il Sottoscrittore dichiara e di aver preso visione delle condizioni specifiche di contratto disponibili presso il sito web del fornitore, e conferma di accettarne le condizioni manlevando la Società da qualsivoglia rivalsa per atti o danni con non rientrino nella responsabilità della Società. Il Sottoscrittore fornirà la documentazione necessarie all'erogazione del Servizio/Prodotto in maniera diretta alla CA emittente o indirettamente tramite la Società, che autorizza, ora per allora, alla trasmissione di tutte le informazioni alla CA Emittente da parte della Società.

5. Elaborazione della Richiesta di certificato

5.1. Alla ricezione del pagamento dovuto, la Società inoltrerà la sua richiesta alla CA emittente per effettuare le procedure di autenticazione per il Certificato SSL richiesto dal Sottoscrittore e, successivamente, elaborerà una Richiesta di certificato.

5.2. Ad approvazione della richiesta di Certificato SSL e prima del rilascio dello stesso, il Sottoscrittore deve inoltrare una Richiesta di firma certificato ("CSR") in un formato specificato dalla Società o dal fornitore. L'approvazione della Richiesta di certificato scadrà automaticamente nel caso in cui la Società non riceva un CSR entro dodici (12) mesi dal giorno in cui la Richiesta di certificato viene approvata, anche se il Certificato è pronto per essere rilasciato.

5.3. Il Sottoscrittore deve verificare le informazioni contenute nel Certificato e avvisare tempestivamente la Società in caso di errori. Alla ricezione di tale avviso, la Società può revocare il Certificato e rilasciarne un altro dopo aver effettuato le opportune correzioni.

6. Uso e limitazioni

6.1. Un Certificato è destinato esclusivamente all'installazione su server che siano accessibili nel/i subjectAltName(s) in esso elencati.

6.2. L'utilizzo di un Certificato non è ammesso: (i) a favore o per conto di qualsiasi altra organizzazione; (ii) per eseguire operazioni in chiave privata o pubblica in relazione a qualsiasi dominio e/o nome di organizzazione diverso da quello riportato nella Richiesta di certificato; (iii) su più di un server o dispositivo fisico contemporaneamente, a meno che il Sottoscrittore non abbia acquistato l'Opzione di certificato con licenza o un Certificato che includa esplicitamente licenze server aggiuntive o illimitate; (iv) per utilizzo come apparecchiatura di controllo in situazioni pericolose o impieghi che necessitino di funzionamento a prova di errore, quali attività in impianti nucleari, sistemi di navigazione o comunicazione aerea, sistemi di controllo del traffico aereo, sistemi di controllo armi, ovvero nei casi in cui un eventuale guasto può avere come conseguenza diretta morte, lesioni personali o gravi danni ambientali.

6.3. Nel caso in cui il Sottoscrittore stia utilizzando una Opzione di certificato con licenza, riconosce e conviene che tale opzione può comportare un aumento del rischio per la sicurezza della rete e che la Società si ritiene esonerata da qualsiasi responsabilità per violazioni della sicurezza conseguenti alla distribuzione di una singola chiave su più dispositivi. LA SOCIETÀ CONSIDERA ATTO DI PIRATERIA L'UTILIZZO SENZA LICENZA DI UN CERTIFICATO SU UN DISPOSITIVO CHE RISIEDA SU UN SERVER O IN UNA SERVER FARM; I TRASGRESSORI SARANNO PERSEGUITI NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE.

6.4. Qualora il Sottoscrittore scelga di esibire il Simbolo, dovrà installare ed esibire tale Simbolo esclusivamente in conformità con i termini del Contratto di licenza del simbolo pubblicati nel rispettivo archivio.

6.5. Il Sottoscrittore dovrà utilizzare l'OCSP in maniera coerente con i servizi acquistati. La Società si riserva il diritto di addebitare tariffe aggiuntive in caso di utilizzo eccessivo dell'OCSP.

7. Segnalazioni e revoca

7.1. Nel caso in cui si rilevi, o vi sia ragione di credere, che la sicurezza della chiave privata fornita in virtù del presente contratto sia, o sia stata, messa a rischio, o che l'informazione all'interno del Certificato sia, o sia diventata, non corretta o imprecisa, o se il nome dell'organizzazione del Sottoscrittore e/o la registrazione del nome di dominio hanno subito variazioni, il Sottoscrittore dovrà interrompere immediatamente l'utilizzo del Certificato e della chiave privata ad esso associata e dovrà richiedere tempestivamente alla Società la revoca del Certificato (o dei Certificati) in oggetto. Nel caso in cui la Società rilevi o abbia

ragione di credere che la sicurezza della chiave privata sia stata messa a rischio o che si sia fatto uso improprio di un Certificato, il Sottoscrittore dovrà attuare le misure prescritte dalla Società entro il periodo di tempo da questa specificato. La Società si riserva il diritto di revocare il Certificato in qualsiasi momento, e senza alcun preavviso, qualora: (i) venga a conoscenza del fatto che le informazioni contenute nel Certificato non sono più valide; (ii) il Sottoscrittore violi o manchi di adempiere agli obblighi previsti dai termini del presente Contratto o del Contratto di licenza del simbolo; oppure (iii) la Società decida a sua esclusiva discrezione che la prosecuzione dell'utilizzo del Certificato possa mettere a rischio la sicurezza o l'integrità della PKI o della Società stessa. La Società può inoltre revocare un Certificato in caso di mancato pagamento.

8. Obblighi in caso di revoca o scadenza

8.1. Alla scadenza o all'avviso di revoca di un Certificato, il Sottoscrittore dovrà rimuovere tempestivamente il Certificato da tutti i dispositivi sui quali è stato installato ed interromperne l'utilizzo. Nel caso in cui il Sottoscrittore, insieme al Certificato revocato, abbia installato anche un Simbolo, dovrà rimuovere tale Simbolo da qualsiasi sito Web.

9. Servizi correlati

9.1. Il Sottoscrittore può ricevere Servizi correlati aggiuntivi quali, a titolo esemplificativo: (i) scansione giornaliera di un sito Web per la ricerca di codice nocivo; (ii) valutazione delle vulnerabilità di un ambiente di rete; (iii) servizi relativi al Simbolo; e/o (iv) accesso alle funzionalità di gestione account tramite consolle basata sul Web. La fornitura di tali Servizi può essere soggetta a prerequisiti e termini e condizioni aggiuntivi imposti ad esclusiva discrezione della Società e/o dei suoi Fornitori.

10. Dichiarazioni e garanzie della Società

10.1. La Società per proprio conto, e i Fornitori per quanto di loro competenza, dichiara e garantisce che (i) le informazioni del Certificato non presentano errori dovuti alla carenza di attenzione da parte della Società e/o del Fornitore nella creazione del Certificato; (ii) che il rilascio di Certificati da parte della Società e/o dei Fornitori è conforme in tutti gli aspetti materiali alla relativa Dichiarazione delle procedure di certificazione (CPS); e (iii) che i servizi di revoca e l'utilizzo di un archivio sono conformi in tutti gli aspetti materiali alla propria CPS.

11. Dichiarazioni e garanzie del Sottoscrittore

11.1. Il Sottoscrittore dichiara e garantisce alla Società e alle Parti cedenti che:

a. tutto il materiale informativo relativo al rilascio di un Certificato, fornito dal Sottoscrittore alla Società per ciascuna Richiesta di certificato, è accurato e completo;
b. il Sottoscrittore informerà la Società nel caso in cui le dichiarazioni fatte alla Società in una Richiesta di certificato abbiano subito variazioni o non siano più valide;
c. le informazioni del Certificato fornite dal Sottoscrittore (inclusi eventuali indirizzi e-mail) non violano i diritti di proprietà intellettuale di terze parti;
d. le informazioni del Certificato fornite dal Sottoscrittore (inclusi eventuali indirizzi e-mail) non sono state né saranno utilizzate per fini illeciti;
e. il Sottoscrittore, o chiunque da questi esplicitamente autorizzato, è stato e continuerà ad essere l'unica persona (collettivamente, le uniche persone) in possesso della chiave privata, sin dal momento della creazione, o di qualsiasi frase segreta, PIN, dispositivo software o hardware per la protezione della chiave privata, e che nessuna persona non autorizzata ha avuto o avrà accesso a tali materiali o informazioni;
f. il Sottoscrittore utilizzerà il Certificato esclusivamente per le finalità legittime e autorizzate previste dal presente Contratto;
g. il Sottoscrittore utilizzerà ogni Certificato in qualità di utente finale e non di Autorità di certificazione per il rilascio di Certificati, elenchi di revoca di certificazione o altro;
h. ogni firma digitale creata utilizzando la chiave privata costituisce la firma digitale del Sottoscrittore, e che il Certificato è stato accettato ed è operativo (non scaduto o revocato) al momento della creazione della firma digitale;
i. il Sottoscrittore stipula il presente Contratto come condizione per ricevere un Certificato; e

j. il Sottoscrittore non monitorerà, interferirà con, né eseguirà l'ingegnerizzazione inversa (fatti salvi i casi in cui espressamente consentito dalle leggi vigenti) dell'implementazione tecnica della PKI, se non previa autorizzazione scritta da parte della Società, e in alcun modo metterà a rischio intenzionalmente la sicurezza della PKI. Inoltre, il Sottoscrittore dichiara e garantisce che: dispone di informazioni sufficienti ad assumere una decisione informata relativamente alla misura in cui sceglie utilizzare un certificato digitale rilasciato nell'ambito della PKI; è responsabile esclusivamente della decisione di utilizzare o meno a tali informazioni; sosterrà le conseguenze legali di qualsiasi sua mancata osservanza degli obblighi in qualità di Parte cedente, così come previsto dall'Accordo della parte cedente in vigore.

k. inoltre, se i Servizi ricevuti includono la valutazione dei malware e/o delle vulnerabilità, il Sottoscrittore dichiara e garantisce alla Società di disporre dei poteri societari e dell'autorità per consentire alla Società di procedere alla valutazione; nel caso in cui il sito Web oggetto di valutazione sia gestito e/o ospitato da un provider di servizi di terze parti, il Sottoscrittore garantisce di aver ottenuto dal provider di servizi il consenso e l'autorizzazione necessari alla Società per eseguire la valutazione.

12. Dichiarazioni e garanzie del Rivenditore

12.1. Il Rivenditore dichiara e garantisce alla Società e alle Parti cedenti che (i) ha ottenuto dal proprio cliente l'autorizzazione a stipulare il presente Contratto per suo conto e/o a vincolare il proprio cliente al presente Contratto; e (ii) che rispetterà il Contratto e farà in modo che anche il proprio cliente lo rispetti.

13. Politica di rimborso

13.1. Nel caso in cui il Sottoscrittore non sia per qualsivoglia motivo interamente soddisfatto del Certificato o dei Servizi, avrà diritto a richiedere, entro trenta (30) giorni dall'approvazione della Richiesta di certificato, che la Società revochi il Certificato (qualora sia stato già rilasciato) ed emetta un rimborso. Dopo il periodo iniziale di 30 giorni, il Sottoscrittore avrà diritto al rimborso soltanto nel caso in cui la Società abbia violato i termini della garanzia o qualsiasi altro obbligo materiale previsto dal presente Contratto. In caso di Certificati RapidSSL, si applicherà la suddetta politica di rimborso, con la sola eccezione del periodo iniziale di richiesta di rimborso che qui si conviene in sette (7) giorni dall'approvazione della Richiesta di certificato.

14. Privacy

14.1. Le modalità e le condizioni di trattamento dei dati personali sono indicate sulla relativa pagina del Sito a cui espressamente si rimanda:
https://www.trustitalia.it//archivio/legal_agreements/informativa_sulla_privacy.pdf

15. Risarcimento

15.1. Il Sottoscrittore accetta di difendere e sollevare da ogni responsabilità la Società, i suoi dirigenti, azionisti, funzionari, agenti, dipendenti, subentranti, Fornitori ed aventi causa da tutte le eventuali richieste di risarcimento, azioni legali, procedimenti, danni e costi (compresi gli onorari giustificati e le spese processuali) da parte di terzi, derivanti da:

a. violazione di una qualsiasi garanzia, dichiarazione e obbligo del Sottoscrittore secondo quanto disposto dal presente Contratto,
b. qualsiasi informazione falsa o mendace contenuta nella Richiesta di certificato,
c. qualsiasi violazione del diritto di proprietà intellettuale di qualsiasi persona o entità nelle informazioni o nei contenuti forniti dal Sottoscrittore,
d. mancata divulgazione di fatti materiali nella Richiesta di certificato, qualora la dichiarazione non corretta o l'omissione siano dovute a negligenza o a volontà di ingannare, oppure
e. mancata protezione della chiave privata, utilizzo di un sistema inaffidabile o mancata adozione delle precauzioni necessarie ad evitare che la chiave privata sia messa a rischio, persa, divulgata, modificata o soggetta ad uso non autorizzato, secondo quanto disposto dal presente Contratto.

15.2. La Società avrà l'obbligo di avvisare tempestivamente il Sottoscrittore di qualsiasi eventuale richiesta di risarcimento (e delle eventuali transazioni), e il Sottoscrittore dovrà assumersi la piena responsabilità della difesa, posto comunque

a. che il Sottoscrittore tenga informata di ciò la Società e si consulti con essa in relazione allo stato di avanzamento del contenzioso o della transazione;
b. che il Sottoscrittore, senza il consenso scritto da parte della Società, che non potrà essere negato senza valido motivo, non avrà alcun diritto a liquidare le cifre richieste, laddove la transazione sia il risultato o sia parte di un'azione, una causa o un procedimento penale o contenga un'indicazione, un'ammissione o un riconoscimento di qualsiasi responsabilità o illecito (contrattuale, civile o altro) da parte della Società, o richieda a quest'ultima qualsiasi prestazione specifica o compensazione non pecuniaria; e
c. la Società avrà il diritto di partecipare alla difesa di una richiesta di risarcimento avvalendosi di un legale di sua scelta e a proprie spese.

15.3. I termini del presente paragrafo rimarranno in vigore anche dopo l'estinzione del presente Contratto. In qualità di Parte cedente, il Sottoscrittore accetta di risarcire, difendere e sollevare da ogni responsabilità la Società, i suoi Fornitori, i suoi dirigenti, azionisti, funzionari, agenti, dipendenti, subentranti ed aventi causa da tutti le eventuali richieste di risarcimento, azioni legali, procedimenti, danni e costi (compresi gli onorari giustificati e le spese processuali) da parte di terzi derivanti da:
a. mancato adempimento degli obblighi di Parte cedente, come definiti nell'Accordo della parte cedente in essere;
b. affidamento del Sottoscrittore su un Certificato non ragionevole in circostanze specifiche; oppure
c. mancato controllo della condizione del Certificato per se fosse scaduto o revocato.

16. Piano di protezione

16.1. Il Sottoscrittore può essere coperto dalla versione più aggiornata del Piano di protezione da parte del Fornitore, i cui dettagli sono pubblicati nell'archivio del Fornitore stesso. Nel rispetto dei termini del Piano di protezione, il Fornitore compenserà il Sottoscrittore per determinati danni derivanti da violazione da parte del Fornitore di una o più garanzie limitate previste dal Piano, fino a concorrenza dei limiti in esso contenuti. I Certificati eventualmente forniti a titolo gratuito o in relazione ad offerte di prova della Società non rientrano nella copertura del Piano di protezione.

17. Esonero di responsabilità

17.1. Nel caso in cui il servizio includa la scansione di siti web o di reti,
d. la società non garantisce che tale/i scansione/i rilevi/no tutti i malware e/o le vulnerabilità, nè che i report forniti insieme alla/e scansione/i sia/no completo/i o privo/privi di errori; e
e. il sottoscrittore riconosce e accetta i rischi connessi con la scansione del proprio sito web.

18. Limitazioni di responsabilità

18.1. Se il certificato acquistato è coperto dal piano di protezione, l'importo massimo che il fornitore deve corrispondere al sottoscrittore equivale a quello determinato dal piano di protezione. Inoltre, le limitazioni su danni e pagamenti di cui nel presente paragrafo non si applicano ai rimborsi. Le limitazioni di responsabilità stabilite nel presente contratto dovranno essere le stesse indipendentemente dal numero di firme digitali, transazioni o richieste di risarcimento relative al presente contratto. Il presente paragrafo non pone alcun limite ai rimborsi o ai corrispettivi previsti dal piano di protezione.

19. Diritti del terzo beneficiario

19.1. Per quanto attiene i certificati GeoTrust/RapidSSL, il Sottoscrittore accetta che Microsoft, Inc. sia un terzo beneficiario espresso degli obblighi specificati nel presente Contratto.

20. Aggiornamenti

20.1. La Società e i suoi Fornitori potranno aggiornare il Servizio in qualsiasi momento al fine di garantirne l'efficacia costante.

21. Accessibilità

21.1. Sarà possibile accedere e utilizzare il Servizio in qualsiasi parte del mondo, nel rispetto delle limitazioni

vigenti in materia di esportazioni e dei limiti tecnici, in conformità con gli standard del Fornitore in vigore.

Luogo e data

Trust Italia S.P.A. Il Cliente/Partner

Ai sensi e per gli effetti degli artt. 1341 e 1342 del cod. civ. il Cliente/Partner dichiara di approvare specificamente le pattuizioni contenute negli articoli di seguito indicati:

Art. 5 (Elaborazione della Richiesta di certificato); Art. 6 (Uso e limitazioni); Art. 7 (Segnalazioni e revoca); Art. 8 (Obblighi in caso di revoca o scadenza); Art. 11 (Dichiarazioni e garanzie del Sottoscrittore); Art. 13 (Politica di rimborso); Art. 15 (Risarcimento) Art. 16 (Piano di protezione); Art. 17 (Esonero di responsabilità); Art. 18 (Limitazioni di responsabilità); Art. 19 (Diritti del terzo beneficiario); Art. 21 (Accessibilità).

Luogo e data

Trust Italia S.p.A. Il Cliente/Partner