ALLEGATO A – ALLEGATO TECNICO
Certificati Autenticazione Siti Web di tipo "Organization Validation"
"Global Sign"

Sommario

***

1. RIFERIMENTI ESTERNI:

Documentazione	Link di dettaglio
Manuale Operativo	https://www.globalsign.com/en/repository/GlobalSign_CPS_v10.3_final.pdf
Manuale Utente	https://www.globalsign.com/en/repository/GlobalSign_PDS_v2.0_final.pdf
Documentazione API	N.D.
SLA Agreement	media.globalsign.com/GlobalSign_Service_and_Support_Service_Level_Agreement
Link di supporto (FAQ, Video, Guide)	N.D.

2. Descrizione del servizio

I servizi di autenticazione dei siti web (d'ora in avanti, "**Servizio**") consentono al visitatore di un sito, al Cliente oppure all'Utente di cui all'Accordo, di accertarsi che dietro a quel sito web vi sia un'entità reale e legittima.

Il Servizio ha quale oggetto la rivendita da parte di InfoCert di un certificato qualificato o non qualificato per un dominio con convalida dell'organizzazione (d'ora in avanti, "**Certificato qualificato OV**" o "**Certificato OV**") oppure per un dominio con convalida estesa dell'organizzazione ("d'ora in avanti, "**Certificato EV**" e congiuntamente con i già menzionati certificati, collettivamente, i "**Certificati**") emessi da parte del fornitore GlobalSign (d'ora in avanti, "**GlobalSign**", "**CA**" o il "**Fornitore**").

Tali Certificati sono conformi ai requisiti del consorzio volontario di autorità di certificazione "Forum Autorità di certificazione/Browser (CA/B Forum)", e vengono emessi secondo le modalità da questo previste.

I Certificati sono altresì conformi ai requisiti di cui all'allegato IV del Regolamento UE n. 190/2014 (d'ora in avanti, "**Regolamento eIDAS**").

I Certificati contengono informazioni chiave tra cui il nome del dominio, la data di scadenza degli stessi, la chiave pubblica e la firma digitale della CA. I browser web dei visitatori controllano automaticamente la validità dei Certificati e visualizzano un avviso in caso di problemi sui medesimi.

Nel novero dei Certificati SSL, possono essere emessi dalla CA i QWAC, ossia certificati di autenticazione del sito web regolato dal Regolamento eIDAS. Ogni QWAC contiene informazioni sulle entità che emettono e ricevono i Certificati, nonché informazioni sui Certificati stessi.

I QWAC sono utilizzati oltre ai siti web poiché autenticano la connessione e l'identità dell'entità o della persona che controlla la connessione. Gli standard sull'implementazione dei QWAC sono stabiliti dall'Istituto europeo per le norme delle telecomunicazioni (ETSI). L'ETSI decide se i QWAC sono compatibili con i Certificati EV.

3. Specifiche tecnico-normative

3.1 Richiesta di registrazione e certificazione

Il Cliente deve richiedere la registrazione e l'emissione dei Certificati, utilizzando l'apposito modulo di attivazione (d'ora in avanti, il "**Modulo di Attivazione**") del Servizio per completare l'attività di richiesta di registrazione e certificazione.

Il Cliente prende atto che GlobalSign registra e mantiene per almeno 10 (dieci) anni le informazioni concernenti i Certificati e per 7 (sette) anni dopo che il certificato della CA, su cui si basano i log dei Certificati, cessa di essere valido.
La cessazione del Servizio e/o dell'attività della CA è disciplinata nel Manuale Operativo di cui al Par. 1.

3.2 Obblighi del Cliente

Oltre a quanto stabilito nell'Accordo, il Cliente è tenuto altresì a:

- assicurare la custodia delle chiavi dei Certificati e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
- osservare la massima diligenza nell'indicazione, utilizzo, conservazione e protezione degli strumenti di autenticazione ivi compresi la chiave privata. Il Cliente, inoltre, è tenuto a provvedere all'adeguamento dei propri sistemi hardware e software alle misure di sicurezza previste dalla legislazione vigente. Più in generale, il Cliente garantisce l'assoluta sicurezza ed affidabilità del sito su cui vengono utilizzati i Certificati.
- prima dell'installazione dei Certificati sul proprio server, verificare la correttezza degli stessi e di tutti i dati ivi contenuti.
- installare i Certificati esclusivamente su server accessibili solo attraverso il dominio cui i Certificati medesimi si riferiscono, e utilizzare le relative chiavi solo per il dominio presente nei Certificati stessi.
- comunicare immediatamente e per iscritto ad InfoCert ogni circostanza che possa far ragionevolmente e prudentemente sospettare una compromissione (a titolo esemplificativo: furto, smarrimento, danneggiamento...) della chiave privata o dei Certificati.
- astenersi dall'utilizzare in alcun modo i Certificati o la relativa chiave dopo la sua scadenza, o revoca o sospensione, ovvero per certificare o comunque per far conseguire gli effetti tipici della certificazione in favore di altri soggetti.

Il Cliente non può utilizzare i Certificati, anche indirettamente, per:

- depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici in contrasto o in violazione di diritti di proprietà intellettuale, di segreti commerciali, marchi brevetti o altri diritti di proprietà di terzi o che danneggino, violino o tentino di farlo la segretezza della corrispondenza ed il diritto alla riservatezza;
- pubblicare e/o condividere materiale che, a titolo esemplificativo: violi o trasgredisca diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti, contenuti contro la morale e l'ordine pubblico, abbia contenuti di tipo pedopornografico, pornografico, osceno o comunque contrario alla pubblica morale, sia idoneo a violare o tentare di violare la riservatezza o dati personali o sensibili altri, o sia finalizzato a danneggiare l'integrità delle risorse altrui o a provocare danno diretto o indiretto a chiunque (software pirata, cracks, key generators, serials, virus, worm, trojan horse o altri componenti dannosi), possa costituire abuso, minaccia, calunnia, molestia, spamming, o possa incitare alla violenza, all'odio razziale, al terrorismo, ecc..

3.3 Responsabilità del Cliente

Il Cliente è responsabile della veridicità dei dati comunicati nel Modulo di Attivazione.

Qualora il Cliente, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto, o comunque agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, egli sarà considerato responsabile di tutti i danni derivanti ad InfoCert e/o a terzi dall'inesattezza delle informazioni contenute nel certificato, con obbligo di garantire e manlevare InfoCert da eventuali richieste di risarcimento danni.

Il Cliente è tenuto a manlevare, tenere indenne e risarcire InfoCert da tutti i danni che questa dovesse subire in conseguenza, diretta o indiretta, dell'inadempimento -anche parziale- degli obblighi posti a carico del Cliente dall'Accordo e dal presente Allegato Tecnico, nonché di quanto InfoCert sia tenuta a corrispondere a terzi, o a versare a titolo di sanzione amministrativa o pecuniaria, in conseguenza del citato inadempimento.

Il Cliente è inoltre tenuto a manlevare e tenere indenne InfoCert da ogni responsabilità in merito ai contenuti e a tutte le informazioni pubblicate tramite i Certificati, in merito all'uso dei Certificati stessi e in caso di denunce, azioni, legali, azioni amministrative o giudiziarie, perdite o danni (incluse spese legali ed onorari) scaturite dall'uso illegale, o comunque contrario all'Accordo, del Servizio da parte del Cliente stesso o dei suoi Utenti.

3.4 Durata del Servizio e rinnovo dei Certificati

I Certificati SSL di Autenticazione siti web "GlobalSign" hanno la durata indicata, rispettivamente per ogni tipologia, all'interno del CPS e non sono rinnovabili.

4. SLA e KPI

Gli SLA e KPI sono indicati all'interno dello SLA Agreement di cui al Par. 1.