ALLEGATO TECNICO
Certificati QWAC – Application to Application

Sommario

***

1. RIFERIMENTI ESTERNI:

Documentazione	Link di dettaglio
Manuale Operativo	https://qtsp.infocert.it/pdf/ICERT_INDI_MOWS.pdf
PDS (PKI Disclosure Statement)	https://qtsp.infocert.it/pdf/ICERT_INDI_PDSWS.pdf
Manuale Utente	N.D.
Documentazione API	N.D.
Link di supporto (FAQ, Video, Guide)	N.D.

2. Descrizione del servizio – Introduzione

Tinexta Infocert, nel contesto del presente documento, opera in qualità di prestatore di servizi fiduciari qualificati (di seguito "QTSP") per i servizi di emissione di certificati qualificati di autenticazione di siti web "Application to Application" (di seguito, il "Servizio"), secondo quanto previsto dal Manuale Operativo ICERT-INDI-MOWS (di seguito anche "CPS" o "PS") e dal PKI Disclosure Statement (PDS).
Per tali servizi, Tinexta Infocert ha ottenuto una valutazione di conformità effettuata dal CAB CSQA Certificazioni S.r.l. ai sensi del Regolamento eIDAS (UE) n. 910/2014, come modificato dal Regolamento (UE) 2024/1183, nonché delle norme ETSI applicabili, tra cui ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, 412-3, 412-4 e 412-5 ed ETSI TS 119 495, secondo lo schema di valutazione eIDAS definito da ACCREDIA ai sensi delle norme ETSI EN 319 403 e UNI CEI ISO/IEC 17065:2012.
Per tali servizi Tinexta Infocert ha ottenuto accreditamento presso AgID ed è presente, come previsto dal regolamento eIDAS nella *Trusted Service List* consultabile al seguente link: https://eidas.ec.europa.eu/efda/trust- services/browse/eidas/tls.
I servizi di autenticazione dei siti web consentono alle parti che instaurano una comunicazione su rete pubblica di verificare l'identità del soggetto che gestisce il dominio e di stabilire un canale di comunicazione sicuro.

Nel contesto delle comunicazioni su protocollo TLS (Transport Layer Security), tale funzione è svolta dai certificati comunemente noti come certificati SSL/TLS, che permettono:

- l'autenticazione del server nei confronti del client;
- l'instaurazione di un canale cifrato;
- la garanzia di integrità dei dati scambiati.

I Certificati contengono informazioni chiave, tra cui il nome del dominio, il periodo di validità, la chiave pubblica e la firma digitale della Certification Authority che li ha emessi. Nei contesti web tradizionali, i browser verificano automaticamente la validità dei certificati e segnalano eventuali anomalie o criticità agli utenti.
I certificati TLS pubblicamente riconosciuti sono emessi da Certification Authority secondo regole condivise a livello internazionale, in particolare quelle definite dal CA/Browser Forum, e sono utilizzati da browser e applicazioni per stabilire relazioni di fiducia nelle comunicazioni su rete pubblica.
Nel contesto del presente documento, l'oggetto del servizio è costituito dai certificati qualificati di autenticazione dei siti web in ambito "Application-to-Application" (Qualified Website Authentication Certificates – QWAC), disciplinati dal Regolamento eIDAS (UE) n. 910/2014 e successive modifiche e integrazioni. Tali certificati sono destinati a contesti applicativi e non sono riconosciuti dai principali browser web e dai relativi trust store pubblici, essendo utilizzati unicamente per l'autenticazione e la sicurezza delle comunicazioni tra sistemi.
Tali certificati rappresentano una specifica tipologia di certificati TLS che, oltre a garantire le funzionalità tecniche di autenticazione e cifratura, attestano l'identità del soggetto titolare del certificato sulla base di un processo di verifica qualificato effettuato da un prestatore di servizi fiduciari qualificato (QTSP) e sono pertanto soggetti a requisiti normativi e di conformità più stringenti rispetto ai certificati TLS non qualificati.
Il presente Allegato Tecnico costituisce parte integrante e sostanziale del contratto di acquisto dei servizi (di seguito, l'"Accordo"), stipulato con il Cliente.
Ai soggetti che attivano, utilizzano o fanno affidamento sul Servizio si applicano le Condizioni Generali di Attivazione (di seguito, "CGA"), di cui il presente Allegato Tecnico costituisce parte integrante, fermo restando che, nei rapporti con il Cliente, trovano applicazione anche le disposizioni dell'Accordo.

2.1 Definizione Delle Parti

Cliente
Persona fisica o giuridica che ha formalizzato un contratto di acquisto (Accordo) dei servizi a fronte di un corrispettivo economico. Il Cliente può coincidere con il Richiedente.

Soggetto
È il sistema o sito web per cui il Richiedente richiede il certificato.

Richiedente:
Persona giuridica che richiede a Tinexta Infocert il rilascio di un certificato per un Soggetto. Il Richiedente è la persona fisica dotata dei necessari poteri di rappresentanza o autorizzazione ad agire in nome e per conto della persona giuridica che richiede il certificato;

Utente/Relying party:
È l'organizzazione, il sistema o applicazione che verifica il certificato digitale del Soggetto e che fa affidamento sulla validità del certificato stesso per stabilire una comunicazione sicura e autenticata con il sistema o sito web.

tinexta infocert

3. Specifiche tecnico-normative

3.1 Rilascio e utilizzo del servizio

Il servizio prevede il rilascio e l'utilizzo di certificati qualificati per l'autenticazione di siti web (Qualified Website Authentication Certificates – QWAC), nonché la gestione del relativo ciclo di vita.
Il certificato è rilasciato a seguito della richiesta del Richiedente, mediante sottoscrizione della Richiesta di Attivazione, presentata secondo le modalità previste da Tinexta Infocert, e della trasmissione della richiesta di certificazione della chiave pubblica (Certificate Signing Request – CSR), contenente gli identificativi (i domini) del sistema per cui è richiesta la certificazione.
A seguito delle verifiche previste e dell'esito positivo delle stesse, Tinexta Infocert provvede alla generazione del certificato e lo mette a disposizione del Richiedente.
Il servizio comprende altresì le attività di gestione del certificato per l'eventuale revoca, secondo quanto previsto nel presente documento. Tutte le informazioni relative all'emissione e al ciclo di vita del certificato rimangono in conservazione per almeno 20 anni dalla scadenza del certificato

3.1.1 Certificato e chiavi crittografiche

Un Certificato digitale è un documento elettronico, firmato da Tinexta Infocert, che certifica l'associazione tra il Soggetto, inteso come sistema o sito web, e la relativa coppia di chiavi crittografiche (pubblica e privata), utilizzate per l'autenticazione e la protezione delle comunicazioni.
Le chiavi sono generate e gestite sotto il controllo e responsabilità del Richiedente.
Il QTSP con l'emissione del certificato garantisce la corretta associazione della chiave pubblica con il Soggetto, conformemente alla normativa applicabile e al Manuale Operativo.

3.1.2 Processo e verifica dell'identità

Il rilascio del certificato è subordinato alla verifica dell'identità del Richiedente, persona fisica e giuridica, nonché dei relativi poteri in relazione al Soggetto.
Le attività di identificazione e verifica sono svolte da Tinexta Infocert tramite soggetti appositamente delegati, sulla base della documentazione fornita dal Richiedente e mediante controlli effettuati su fonti ufficiali, registri pubblici e banche dati ritenute affidabili, al fine di accertare l'identità dichiarata e la sussistenza dei poteri di rappresentanza.
Le modalità operative di identificazione e verifica sono definite nel Manuale Operativo ICERT-INDI-MO.
Sono inoltre effettuate le verifiche necessarie a comprovare il controllo del sistema applicativo e dei domini associati per cui il certificato è richiesto. Nel caso di certificati QWAC PSD2, sono altresì verificati gli ulteriori attributi specifici previsti dalla normativa applicabile.

3.1.3 Processo di utilizzo e verifica del certificato

Il certificato è utilizzato dal sistema o applicazione per cui è stato emesso nell'ambito delle comunicazioni su rete, al fine di consentire agli altri sistemi con cui interagisce di verificarne l'identità.
Nelle comunicazioni tra applicazioni, il sistema che espone il servizio presenta il proprio certificato al sistema chiamante. Quest'ultimo utilizza il certificato per verificarne la validità, la provenienza e lo stato, accertando che sia stato emesso da Tinexta Infocert e che non risulti scaduto o revocato.
Nel caso di comunicazioni protette mediante protocollo mTLS (Mutual Transport Layer Security), anche il sistema chiamante presenta il proprio certificato al sistema che espone il servizio, consentendo una autenticazione reciproca tra le parti. Entrambi i sistemi effettuano pertanto le verifiche di validità, provenienza e stato del certificato presentato dalla controparte, al fine di accertarne l'affidabilità e l'associazione al relativo Soggetto.
L'esito positivo di tali verifiche consente ai sistemi coinvolti di confermare reciprocamente l'identità della controparte e di instaurare una comunicazione protetta e autenticata tra i sistemi applicativi.

3.1.4 Durata e rinnovo

Il certificato è emesso con una durata limitata, indicata all'interno del certificato stesso.
Tinexta Infocert non prevede il rinnovo del certificato mantenendo la medesima chiave pubblica. Alla scadenza, il certificato può essere sostituito mediante una nuova emissione, a seguito della generazione di una nuova coppia di chiavi crittografiche e della trasmissione di una nuova richiesta di certificazione della chiave pubblica (CSR).
Il nuovo certificato mantiene le informazioni relative al Soggetto, salvo eventuali aggiornamenti, e può differire per periodo di validità, identificativi e eventuali altre informazioni.

3.1.5 Revoca

La revoca comporta la cessazione della validità del certificato prima della sua naturale scadenza.
I certificati revocati sono inseriti in apposite liste di revoca (CRL) pubblicate dalla Certification Authority, nonché resi disponibili tramite servizi online di verifica dello stato del certificato (OCSP).
La revoca può essere richiesta dal Richiedente o disposta da Tinexta Infocert e nei casi previsti dal Manuale Operativo, tra cui, a titolo esemplificativo, la compromissione della chiave privata, l'inesattezza delle informazioni contenute nel certificato o la perdita dei requisiti del Soggetto. Per i certificati emessi nell'ambito del presente servizio non è prevista la sospensione.

3.2 Prodotti e Servizi

Nell'ambito del presente servizio, Tinexta Infocert emette certificati qualificati per l'autenticazione di siti web (Qualified Website Authentication Certificates – QWAC), destinati all'utilizzo in contesti applicativi "Application-to-Application" (A2A), per l'identificazione di sistemi e servizi esposti su rete.
I certificati sono rilasciati a seguito di attività di validazione del dominio e dell'organizzazione che ne detiene il controllo e attestano l'associazione tra il Soggetto, inteso come sistema o sito web, e i relativi identificativi tecnici, quali i nomi di dominio.
In particolare, Tinexta Infocert emette le seguenti tipologie di certificati:

- **Certificati QWAC per applicazioni A2A**
  Certificati qualificati utilizzati per l'autenticazione di sistemi o siti web nell'ambito di comunicazioni su rete.
- **Certificati QWAC PSD2 / Open Banking**
  Certificati qualificati utilizzati nell'ambito dei servizi di pagamento e degli ecosistemi di open banking, che includono gli attributi specifici del prestatore di servizi di pagamento previsti dalla normativa applicabile.

I certificati sono emessi secondo i profili suddetti, identificati da specifici Object Identifier (OID), che ne determinano le caratteristiche, inclusa la durata di validità. In particolare, entrambi i certificati possono avere una durata fino a un anno, mentre, nei soli casi previsti per i servizi PSD2 o di open banking, fino a due anni.
Le caratteristiche tecniche dei certificati, inclusi i relativi OID, i profili di certificato e gli eventuali attributi qualificati, sono definite nel Manuale Operativo ICERT-INDI-MOWS, al quale si rinvia.

3.3 Obblighi e Responsabilità

3.3.1 Obblighi del Richiedente

Oltre a quanto previsto nelle condizioni generali di attivazione (e nell' Accordo, quando Cliente e Richiedente coincidono) il Richiedente è tenuto:

- ad assicurare la custodia e la riservatezza delle chiavi dei Certificati e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danni a terzi.

- ad osservare la massima diligenza nell'indicazione, utilizzo, conservazione e protezione degli strumenti di autenticazione ivi compresi la chiave privata. Il Richiedente, 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 Richiedente garantisce la sicurezza ed affidabilità del sistema su cui vengono utilizzati i Certificati.
- prima dell'installazione dei Certificati sul proprio server, a verificare la correttezza degli stessi e di tutti i dati ivi contenuti.
- comunicare immediatamente e per iscritto a Tinexta 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,

Il Richiedente si impegna a non utilizzare il Servizio e i Certificati in relazione a domini, sistemi o applicazioni che comportino violazioni di legge, diritti di terzi o che possano arrecare danno a terzi, ivi inclusi, a titolo esemplificativo, casi di utilizzo illecito delle risorse informatiche, diffusione di contenuti dannosi o attività contrarie alla normativa applicabile.

Il Richiedente si impegna altresì a non utilizzare il Servizio e i Certificati per finalità fraudolente o ingannevoli, inclusi, a titolo esemplificativo, attività di phishing, diffusione di malware, furti di identità ecc.

È vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel Manuale Operativo e nei contratti di fornitura, e comunque in violazione dei limiti d'uso o attributi aggiuntivi eventualmente richiesti (key usage, extended key usage, user notice, …) indicati nel certificato.

Il Richiedente si impegna a richiedere tempestivamente la revoca del Certificato qualora le informazioni contenute nello stesso non siano più accurate, complete o aggiornate.

3.3.2 Responsabilità del Richiedente

Oltre a quanto previsto nelle condizioni generali di attivazione (e nell' Accordo, quando Cliente e Richiedente coincidono), il Richiedente è responsabile della veridicità dei dati comunicati ai fini del rilascio del certificato

Qualora il Richiedente, 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, ovvero abbia agito dolosamente o colposamente 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 al Certificatore e/o a terzi dall'inesattezza delle informazioni contenute nel Certificato, con obbligo di manlevare e tenere indenne il Certificatore da eventuali richieste di risarcimento danni.

Il Richiedente è tenuto a manlevare, tenere indenne e risarcire Tinexta Infocert da tutti i danni che questa dovesse subire in conseguenza, diretta o indiretta, dell'inadempimento –anche parziale– degli obblighi posti a carico del Richiedente nelle condizioni generali di attivazione (e/o nell'Accordo, quando presente) e dal presente Allegato Tecnico, nonché di quanto Tinexta Infocert sia tenuta a corrispondere a terzi, o a versare a titolo di sanzione amministrativa o pecuniaria, in conseguenza del citato inadempimento.

Il Richiedente è inoltre tenuto a manlevare e tenere indenne Tinexta Infocert da ogni responsabilità 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 del Servizio da parte del Richiedente stesso.

I Certificati non possono essere in alcun modo ceduti o trasferiti, dal Richiedente, a terzi (neanche a seguito di cessione o affitto di azienda), senza il previo consenso scritto di Tinexta Infocert. Non possono inoltre essere trasferiti o esportati in altri paesi al di fuori dell'Italia, in violazione di leggi o regolamenti di altre giurisdizioni.

Una volta che il Certificato sia scaduto o sia stato revocato, o comunque in ogni caso in cui non ne sia più legittimamente autorizzato l'utilizzo, il Richiedente è obbligato a cessarne immediatamente l'utilizzo e a rimuovere in forma permanente il Certificato stesso dai server in uso.

3.3.3 Obblighi e responsabilità della Certification Authority

Tinexta Infocert, in qualità di Certification Authority, opera nel rispetto della normativa applicabile, degli standard tecnici di riferimento e del Manuale Operativo ICERT-INDI-MOWS.

In particolare, Tinexta Infocert provvede a:

- verificare le informazioni fornite dal Richiedente secondo le modalità previste, inclusa la validazione del dominio e dell'organizzazione che ne detiene il controllo;
- garantire la corretta associazione tra la chiave pubblica e il Soggetto, nonché la conformità del certificato ai requisiti normativi e tecnici applicabili;
- gestire il ciclo di vita del certificato, incluse le operazioni di emissione, revoca e pubblicazione dello stato mediante i servizi previsti (CRL e OCSP);
- conservare, secondo le modalità previste dal Manuale Operativo, i certificati emessi e le informazioni relative agli eventi del ciclo di vita, inclusi i log del servizio.

Tinexta Infocert non assume ulteriori obblighi rispetto a quelli previsti dalle condizioni generali di attivazione (e/o dall'Accordo, quando presente), dal presente Allegato Tecnico, dal Manuale Operativo e dalla normativa vigente in materia di servizi fiduciari.

In particolare, Tinexta Infocert non assume responsabilità in relazione:

- alla gestione, configurazione e sicurezza dei sistemi, delle infrastrutture e dei software utilizzati dal Richiedente o da terzi;
- all'uso del certificato non conforme alle finalità previste o ai limiti d'uso indicati nel certificato stesso, nel Manuale Operativo o nella normativa applicabile;
- alla compromissione della chiave privata imputabile al Richiedente o comunque a soggetti terzi;
- al malfunzionamento o all'indisponibilità di reti di comunicazione, sistemi informatici o infrastrutture non direttamente controllate dalla Certification Authority.

Tinexta Infocert non assume altresì alcun obbligo di sorveglianza in merito ai contenuti, ai servizi o alle applicazioni rese disponibili tramite il soggetto del certificato.

Fermo restando quanto previsto dalla normativa applicabile e salvo i soli casi di dolo o colpa ove previsti, la responsabilità della Certification Authority è limitata ai casi e nei limiti previsti dal Manuale Operativo e dal presente documento.

4. SLA e KPI

In termini di erogazione, i valori di disponibilità mensile dei servizi sono rappresentati dettagliatamente nel Manuale Operativo