

| | | | | |
|---|------------------|---|------------------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |

Classificazione: Pubblico

QTSP

SERVIZI QUALIFICATI DI CERTIFICAZIONE

CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY



Classificazione: Pubblico

| | | | |
|------------------|---|------------------|------------------|
| Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | Data | 08/02/2021 |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

INDICE

| | | |
|----------|---|-----------|
| 1 | INTRODUZIONE | 8 |
| 1.1 | PANORAMICA | 8 |
| 1.2 | NOME DEL DOCUMENTO E IDENTIFICAZIONE | 8 |
| 1.2.1 | Identificazione del documento | 8 |
| 1.3 | PKI PARTICIPANTS | 11 |
| 1.3.1 | Certification Authorities | 12 |
| 1.3.2 | Registration Authorities | 12 |
| 1.3.3 | Sottoscrittori e Relying Parties | 12 |
| 1.3.4 | Altri partecipanti | 13 |
| 1.4 | UTILIZZO DEL CERTIFICATO | 13 |
| 1.4.1 | Utilizzi consentiti del certificato | 14 |
| 1.4.2 | Utilizzi non consentiti del certificato | 15 |
| 1.5 | AMMINISTRAZIONE DELLA POLICY | 15 |
| 1.5.1 | Amministrazione del documento | 15 |
| 1.5.2 | Responsabilità dell'Idoneità | 16 |
| 1.5.3 | Procedure di approvazione | 16 |
| 1.6 | DEFINIZIONI ED ACRONIMI | 16 |
| 1.6.1 | Definizioni | 16 |
| 1.6.2 | Acronimi | 18 |
| 2 | PUBBLICAZIONE | 20 |
| 2.1 | REPOSITORY | 20 |
| 2.2 | PUBBLICAZIONE DI INFORMAZIONI DI CERTIFICAZIONE | 20 |
| 2.3 | FREQUENZA DI PUBBLICAZIONE | 20 |
| 2.3.1 | Frequenza di pubblicazione dei Termini e Condizioni | 20 |
| 2.3.2 | Frequenza di pubblicazione dei certificati | 20 |
| 2.3.3 | Frequenza pubblicazione stati di revoca | 20 |
| 2.4 | CONTROLLO DEGLI ACCESSI SUI REPOSITORY | 20 |
| 3 | IDENTIFICAZIONE ED AUTENTICAZIONE | 21 |
| 3.1 | DENOMINAZIONE | 21 |
| 3.1.1 | Tipi di nomi | 21 |
| 3.1.2 | Requisiti di identificazione | 22 |
| 3.1.3 | Sottoscrittori anonimi e uso di pseudonimi | 22 |
| 3.1.4 | Regole per l'interpretazione dei nomi | 22 |
| 3.1.5 | Unicità dei nomi | 22 |
| 3.2 | VALIDAZIONE DELL'IDENTITÀ | 22 |
| 3.2.1 | Metodi per comprovare il possesso della chiave privata | 22 |
| 3.2.2 | Processi di consegna Token OTP fisici | 23 |
| 3.2.3 | Validazione dell'identità di una entità organizzativa | 23 |
| 3.2.4 | Validazione dell'identità di una entità individuale | 23 |
| 3.2.5 | Informazioni di sottoscrizione non verificabili | 25 |
| 3.3 | IDENTIFICAZIONE ED AUTENTICAZIONE PER RIEMISSIONE | 25 |
| 3.3.1 | Identificazione e Autenticazione per rimissione di un certificato in corso di validità | 26 |
| 3.3.2 | Identificazione e Autenticazione per rimissione dopo revoca/scadenza | 26 |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | | |
|----------|--|-----------|
| 3.4 | IDENTIFICAZIONE ED AUTENTICAZIONE IN CASO DI RICHIESTE DI MODIFICA DEL CERTIFICATO | 26 |
| 3.5 | IDENTIFICAZIONE ED AUTENTICAZIONE PER RICHIESTE DI REVOCA | 26 |
| 4 | REQUISITI CICLO DI VITA DEL CERTIFICATO | 26 |
| 4.1 | RICHIESTA DI UN CERTIFICATO | 26 |
| 4.1.1 | Sottomissione della richiesta di certificato | 30 |
| 4.1.2 | Processo di Registrazione/Enroll e Responsabilità | 30 |
| 4.1.3 | Attivazione del certificato | 31 |
| 4.2 | PROCESSI DI GESTIONE DELLA RICHIESTA DI CERTIFICATO | 31 |
| 4.2.1 | Esecuzione di funzioni di Identificazione e di Autenticazione | 31 |
| 4.2.2 | Approvazione o rigetto | 31 |
| 4.2.3 | Tempo di esecuzione della richiesta | 31 |
| 4.3 | RILASCIO DEL CERTIFICATO | 32 |
| 4.3.1 | Azioni di CA durante il rilascio del certificato | 32 |
| 4.3.2 | Notifiche al titolare circa il rilascio del certificato | 33 |
| 4.4 | ACCETTAZIONE DEL CERTIFICATO | 33 |
| 4.4.1 | Condotta sulla accettazione del certificato | 33 |
| 4.4.2 | Pubblicazione del certificato da parte della CA | 33 |
| 4.5 | COPPIA DI CHIAVI E UTILIZZO DEL CERTIFICATO | 33 |
| 4.5.1 | Chiave privata del sottoscrittore e utilizzo del certificato | 33 |
| 4.5.2 | Parti interessate – Chiave pubblica e utilizzo del certificato | 34 |
| 4.6 | RIEMMISSIONE | 34 |
| 4.6.1 | Requisiti per la riemissione del certificato | 34 |
| 4.6.2 | Sottomissione richiesta di riemissione | 35 |
| 4.6.3 | Processo della richiesta di riemissione | 35 |
| 4.6.4 | Registrazione sulla piattaforma del QTSP e Autorizzazione del certificato | 35 |
| 4.6.5 | Attivazione del Certificato | 35 |
| 4.6.6 | Notifiche relative al rilascio del certificato | 36 |
| 4.6.7 | Condotta sulla accettazione della riemissione del certificato | 36 |
| 4.6.8 | Pubblicazione del certificato riemesso da parte della CA | 36 |
| 4.7 | MODIFICHE AL CERTIFICATO | 36 |
| 4.8 | REVOCA E SOSPENSIONE DEL CERTIFICATO | 36 |
| 4.8.1 | Circostanze di revoca | 36 |
| 4.8.2 | Sottomissione della richiesta di revoca | 37 |
| 4.8.3 | Processo per la richiesta della revoca | 37 |
| 4.8.4 | Grace Period richiesta di revoca | 38 |
| 4.8.5 | Tempo entro il quale la CA deve processare la richiesta di revoca | 38 |
| 4.8.6 | Requisiti sul controllo della revoca da parte delle parti interessate | 38 |
| 4.8.7 | Frequenza emissione della CRL | 38 |
| 4.8.8 | Massima latenza sulla CRL | 38 |
| 4.8.9 | Disponibilità del servizio OCSP | 38 |
| 4.8.10 | Requisiti servizio OCSP | 38 |
| 4.8.11 | Requisiti particolari sulla compromissione della chiave | 39 |
| 4.9 | SERVIZI PER LA VERIFICA DELLO STATO DEL CERTIFICATO | 39 |
| 4.9.1 | Caratteristiche operazionali | 39 |
| 4.9.2 | Disponibilità del servizio | 39 |
| 4.10 | FINE DELLA SOTTOSCRIZIONE | 40 |
| 4.11 | KEY ESCROW E RECOVERY | 40 |
| 4.11.1 | Policy e Pratiche Key Escrow e Recovery | 40 |
| 4.11.2 | Incapsulamento chiave Cifratura simmetrica Politiche di Recovery | 40 |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | | |
|----------|--|-----------|
| 5 | FACILITY, MANAGEMENT, E CONTROLLI OPERATIVI | 41 |
| 5.1 | CONTROLLI FISICI | 41 |
| 5.1.1 | Locazione del sito e Caratteristiche | 41 |
| 5.1.2 | Accessi fisici | 41 |
| 5.1.3 | Alimentazione ed Aria condizionata | 42 |
| 5.1.4 | Esposizione all'acqua | 43 |
| 5.1.5 | Prevenzione e protezione antincendio | 43 |
| 5.1.6 | Media Storage | 44 |
| 5.1.7 | Disposizioni sulla dismissione di apparati | 44 |
| 5.1.8 | Off-Site Backup | 44 |
| 5.2 | CONTROLLI PROCEDURALI | 44 |
| 5.2.1 | Ruoli | 44 |
| 5.2.2 | Numero di persone richieste per task | 45 |
| 5.2.3 | Identificazione ed Autenticazione per Ruoli | 45 |
| 5.2.4 | Ruoli che richiedono segregazione | 45 |
| 5.3 | CONTROLLO DEL PERSONALE | 46 |
| 5.3.1 | Qualifiche, esperienze e chiarezza dei requisiti | 46 |
| 5.3.2 | Procedure di verifica di Background | 46 |
| 5.3.3 | Requisiti di formazione | 46 |
| 5.3.4 | Frequenza di aggiornamento | 47 |
| 5.3.5 | Sanzioni su azioni non autorizzate | 47 |
| 5.3.6 | Requisiti su consulenti | 47 |
| 5.3.7 | Documentazione fornita al personale | 47 |
| 5.4 | PROCEDURE DI AUDIT | 48 |
| 5.4.1 | Tipologie di eventi memorizzati | 48 |
| 5.4.2 | Frequenza dei processi di Audit | 48 |
| 5.4.3 | Periodo di retention dei log di Audit | 49 |
| 5.4.4 | Protezione dei log di audit | 49 |
| 5.4.5 | Procedure di backup log di Audit | 49 |
| 5.4.6 | Sistemi di raccolta eventi di Audit | 49 |
| 5.4.7 | Notifica in caso di identificazione di eventi sospetti - | 49 |
| 5.4.8 | Vulnerability Assessment | 49 |
| 5.5 | ARCHIVIAZIONE DEI RECORD | 50 |
| 5.6 | CA KEY CHANGEOVER | 50 |
| 5.7 | COMPROMISSIONE E DISASTER RECOVERY | 50 |
| 5.7.1 | Incident e procedure di gestione della compromissione | 51 |
| 5.7.2 | Computing Resources, Software, e/o dati corrotti | 51 |
| 5.7.3 | Procedure di compromissione chiave privata | 51 |
| 5.7.4 | Capacità di Business Continuity in caso di disastro | 51 |
| 5.8 | CESSAZIONE DELLA ATTIVITÀ | 51 |
| 6 | CONTROLLI TECNICI DI SICUREZZA | 52 |
| 6.1 | GENERAZIONE ED INSTALLAZIONE COPPIA DI CHIAVI | 52 |
| 6.1.1 | Generazione coppia di chiavi | 52 |
| 6.1.2 | Rilascio della chiave privata ai sottoscrittori | 52 |
| 6.1.3 | Rilascio della chiave pubblica al QTSP | 52 |
| 6.1.4 | Rilascio della chiave pubblica di CA alle parti interessate | 53 |
| 6.1.5 | Lunghezza chiavi | 53 |
| 6.1.6 | Parametri di generazione chiavi e controllo della qualità | 53 |
| 6.1.7 | Scopi del Key Usage (vedi campo Key Usage X.509 v3) | 53 |
| 6.2 | PROTEZIONE DELLA CHIAVE PRIVATA E CONTROLLI SULLA COMPONENTE CRITTOGRAFICA | 53 |

| | | | |
|------------------|---|------------------|------------------|
| Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | Data | 08/02/2021 |

Classificazione: Pubblico

| | | |
|------------|--|-----------|
| 6.2.1 | Standard e controlli dei Moduli crittografici | 53 |
| 6.2.2 | Controllo segregazione chiave privata (MofN)..... | 54 |
| 6.2.3 | Key Escrow della chiave privata..... | 54 |
| 6.2.4 | Backup chiave privata..... | 54 |
| 6.2.5 | Archiviazione della chiave | 54 |
| 6.2.6 | Trasferimento della chiave privata da/per il modulo crittografico | 54 |
| 6.2.7 | Memorizzazione della chiave privata sul modulo crittografico..... | 55 |
| 6.2.8 | Metodi di attivazione della chiave privata | 55 |
| 6.2.9 | Metodo di disattivazione della chiave privata | 55 |
| 6.2.10 | Metodo di distruzione della chiave privata | 56 |
| 6.2.11 | Valutazione del modulo crittografico..... | 56 |
| 6.2.12 | Validità del certificato e delle chiavi | 56 |
| 6.3 | DATI DI ATTIVAZIONE | 56 |
| 6.3.1 | Generazione ed installazione dati di attivazione..... | 56 |
| 6.3.2 | Protezione dei dati di attivazione..... | 57 |
| 6.3.3 | Altri aspetti sui dati di attivazione..... | 57 |
| 6.4 | CONTROLLI DI SICUREZZA SU COMPUTER | 57 |
| 6.4.1 | Requisiti Tecnici di sicurezza specifici su sistemi IT | 57 |
| 6.4.2 | Valutazione della Sicurezza dei sistemi IT | 58 |
| 6.5 | CICLO DI VITA DEI CONTROLLI TECNICI..... | 58 |
| 6.5.1 | Controllo dei sistemi di sviluppo..... | 58 |
| 6.5.2 | Controlli di gestione della sicurezza..... | 58 |
| 6.5.3 | Ciclo di vita dei controlli di sicurezza | 59 |
| 6.6 | CONTROLLI DI SICUREZZA DELLA RETE | 59 |
| 6.7 | TIME-STAMPING | 60 |
| 7 | CERTIFICATI, CRL, E PROFILI OCSP..... | 61 |
| 7.1 | PROFILO DI CERTIFICATO | 61 |
| 7.1.1 | Specifica X509..... | 61 |
| 7.1.2 | Estensioni di certificato | 62 |
| 7.1.2.1 | Gestione in continuità dei certificati di Lottomatica S.p.A | 75 |
| 7.1.2.2 | Gestione in continuità dei certificati di Lottomatica Holding a seguito di cambio di P.IVA | 75 |
| 7.1.3 | Object Identifier Algoritmi | 75 |
| 7.1.4 | Composizione del nome..... | 75 |
| 7.1.5 | Vincoli sul nome..... | 76 |
| 7.1.6 | Object Identifier policy di certificato..... | 76 |
| 7.1.7 | Utilizzo dell'estensione Policy Constraint | 76 |
| 7.1.8 | Sintassi e semantica dei qualificatori della Policy | 76 |
| 7.1.9 | Gestione della semantica per estensioni di certificate policy critiche | 76 |
| 7.2 | PROFILO CRL..... | 76 |
| 7.2.1 | Versione..... | 76 |
| 7.2.2 | Specifica delle estensioni della CRL..... | 76 |
| 7.3 | PROFILO OCSP | 77 |
| 7.3.1 | Versione..... | 77 |
| 7.3.2 | Estensioni OCSP | 77 |
| 8 | COMPLIANCE AUDIT E ALTRI ASSESSMENTS..... | 78 |
| 8.1 | FREQUENZE O REQUISITI DI ASSESSMENT | 78 |
| 8.2 | IDENTITÀ/QUALIFICA DEGLI ASSESSOR..... | 78 |
| 8.3 | INDIPENDENZA DELL'ASSESSOR..... | 78 |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | | |
|-----------|--|-----------|
| 8.4 | ARGOMENTI COPERTI DALL' ASSESSMENT | 78 |
| 8.5 | AZIONI INTRAPRESE IN CASO DI NON CONFORMITÀ..... | 79 |
| 8.6 | COMUNICAZIONE DEI RISULTATI..... | 79 |
| 9 | ASPETTI ECONOMICO LEGALI..... | 80 |
| 9.1 | TARiffe..... | 80 |
| 9.2 | RESPONSABILITÀ FINANZIARIE..... | 80 |
| 9.2.1 | Copertura assicurativa..... | 80 |
| 9.3 | CONFIDENZIALITÀ DELLE INFORMAZIONI DI BUSINESS | 80 |
| 9.4 | TUTELA DEI DATI PERSONALI | 80 |
| 9.4.1 | Modalità di protezione dei dati personali..... | 81 |
| 9.5 | DIRITTI DI PROPRIETÀ INTELLETTUALE | 85 |
| 9.6 | DICHIARAZIONI E GARANZIE..... | 85 |
| 9.6.1 | Dichiarazioni e garanzie della CA | 85 |
| 9.6.2 | Dichiarazioni e garanzie della RA | 85 |
| 9.6.3 | Dichiarazioni e Garanzie del sottoscrittore..... | 87 |
| 9.7 | DICHIARAZIONI DI GARANZIA..... | 89 |
| 9.8 | LIMITE DI RESPONSABILITÀ | 89 |
| 9.9 | INDENNITÀ..... | 90 |
| 9.10 | DURATA E CESSAZIONE DEL SERVIZIO..... | 90 |
| 9.10.1 | Durata | 90 |
| 9.10.2 | Risoluzione..... | 90 |
| 9.10.3 | Effetti della cessazione..... | 90 |
| 9.11 | NOTIFICHE E COMUNICAZIONI CON GLI UTENTI..... | 90 |
| 9.12 | MODIFICHE AL CPS..... | 90 |
| 9.12.1 | Procedure per la diffusione del CPS | 91 |
| 9.12.2 | Meccanismi di notifica e tempi | 91 |
| 9.12.3 | Circostanze sotto le quali è necessario il cambio di OID | 91 |
| 9.13 | RISOLUZIONE DELLE CONTROVERSIE | 91 |
| 9.14 | LEGGI GOVERNATIVE..... | 91 |
| 9.15 | COMPLIANCE CON LEGGI IN VIGORE | 91 |
| 10 | RIFERIMENTI | 92 |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

1 INTRODUZIONE

Questo documento contiene le specifiche relative alla policy per l'emissione di certificati qualificati (Certificate Policy –in seguito CP) e ai processi operativi (Certification Practice Statement – in seguito CPS) per l'emissione di certificati qualificati definite per il **prestatore di servizi fiduciari qualificato Lottomatica Holding S.r.l.**, e riguardanti il servizio di sottoscrizione.

Tale documento è compatibile ai requisiti espressi nel Regolamento Europeo 910/2014 – eIDAS [27], e l'attività descritta è compatibile con quanto previsto per i servizi erogati da Prestatori di Servizi Fiduciari Qualificati (in seguito QTSP).

Il QTSP (Lottomatica Holding S.r.l.) si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.

Ogni nuova versione del manuale annulla e sostituisce le precedenti versioni, che rimangono tuttavia applicabili ai certificati emessi durante la loro vigenza e fino alla prima scadenza degli stessi.

1.1 PANORAMICA

Il presente documento contiene la definizione di regole che specificano l'usabilità di un certificato per una comunità e / o una classe di applicazioni con requisiti comuni di sicurezza.

Le informazioni presenti nel presente documento sono strutturate per essere compatibili con quanto incluso nella specifica pubblica nell'RFC 3647.

Il presente documento è costituito da 10 capitoli che contengono i requisiti di sicurezza, i processi e le pratiche definite dal QTSP da seguire durante l'erogazione del servizio.

I certificati rilasciati in accordo con il presente documento, presentano degli identificatori (OID) di policy a cui i certificati devono essere conformi.

Il presente documento definisce requisiti e processi di base relativi a certificati con particolare riferimento al certificato del QTSP. Il modo nel quale questi requisiti sono rispettati, e le descrizioni dettagliate dei metodi menzionati nel presente documento, fanno altresì parte del presente Certification Practice Statement (CPS) rilasciato dal QTSP.

1.2 NOME DEL DOCUMENTO E IDENTIFICAZIONE

1.2.1 Identificazione del documento

Questo documento è denominato "*QTSP Servizi Qualificati di Certificazione – Certification Practice Statement e Certificate Policy*" ed è caratterizzato dal codice documento: LTIS-05-00001/18. La versione e il livello di rilascio sono identificabili sul frontespizio in calce ad ogni pagina.

I certificati rilasciati ai titolari vengono emessi con le limitazioni d'uso specificate nel cap. 1.4.

Il documento viene rivisto almeno annualmente così come i relativi criteri di applicabilità.

Tutti i Certificati rilasciati dal QTSP riferiscono a Policy specifiche per le quali sono rilasciati.

Il seguente OID è un identificativo univoco rilasciato a Lottomatica Holding S.r.l.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| OID | Descrizione |
|------|--|
| (1) | International Organization for Standardization (ISO) |
| (3) | Organization identification schemes registered according to ISO/IEC 6523-2 |
| (76) | UNINFO |
| (49) | Lottomatica Holding S.r.l. |

Tabella 1 - Policy Lottomatica Holding S.r.l.

Nella tabella che segue, l'OID di specifica del presente documento:

| OID | Descrizione |
|-------------|--|
| (1.3.76.49) | Lottomatica Holding S.r.l. |
| (1) | Lottomatica Holding S.r.l. Certification Authority |
| (2) | Documenti |
| (1) | Documenti pubblici |
| (11) | Lottomatica Holding S.r.l. Servizi di Certificazione – Certification Practice Statement and Certificate Policy |

Tabella 2 – Policy documento

Ai fini dell'attività di QTSP, Lottomatica Holding S.r.l. definisce i seguenti OID afferenti ad altrettante tipologia di certificato:

| OID | Descrizione | Abbreviazione |
|-------------|--|---------------|
| (1.3.76.49) | Lottomatica Holding S.r.l. | - |
| (1) | Lottomatica Holding S.r.l. Certification Authority | - |
| (1) | Certificates | - |
| (1) | Public | - |
| (20) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM - B2B -Area Giochi/Servizi | IGTCP01 |
| (22) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM ad uso interno - Area Giochi/Servizi | IGTCP03 |
| (23) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM per Firma Automatica – Area Giochi/Servizi | IGTCP04 |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| OID | Descrizione | Abbreviazione |
|------|---|---------------|
| (24) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM ad uso Master-RAO/RAO – Area Giochi/Servizi | IGTCP05 |
| (25) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM – B2B – Area Servizi | IGTCP06 |
| (26) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM ad uso Master-RAO/RAO – Area Servizi | IGTCP07 |
| (27) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM ad uso interno – Area Servizi | IGTCP08 |
| (28) | Certificato di firma Qualificato rilasciato a persona fisica su dispositivo HSM per Firma Automatica – Area Servizi | IGTCP09 |
| (1) | Main version | - |
| (0) | Sub version | - |

Tabella 3 - Policy di Certificato

La policy di certificato di cui tabella 3, si riferisce a certificati rilasciati a persone fisiche.

Le policy di certificato presenti in tabella 3 prevedono il rilascio di chiavi su HSM; in questo senso, il QTSP:

- Garantisce che la chiave privata associata al Certificato è memorizzata esclusivamente su dispositivo di sicurezza conforme alle specifiche di certificazione riportate in 6.2.1;

Il Prestatore di servizi fiduciari fornisce i processi di identificazione in accordo con i requisiti del Regolamento (UE) 2016/679 (GDPR) [25] descritti nel relativo CPS.

Riguardo il presente documento:

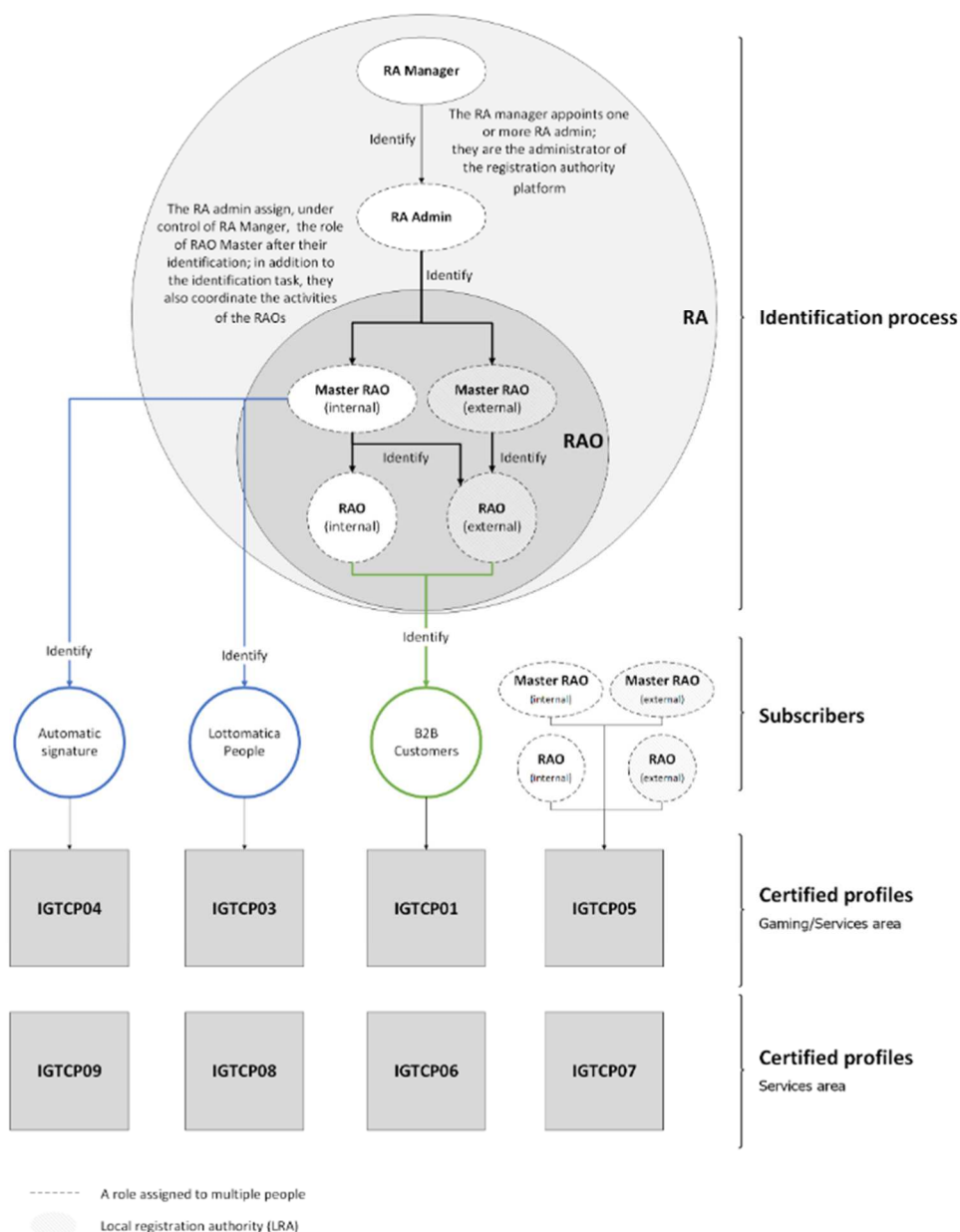
- Ogni policy di certificato è conforme alla policy [QCP-n-qscd] definita nello standard [4].

| | | | |
|------------------|---|------------------|------------------|
| Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | Data | 08/02/2021 |

Classificazione: Pubblico

1.3 PKI PARTICIPANTS

Di seguito riporta uno schema riassuntivo che vuole descrivere in modo sintetico l'organizzazione della Registration authority (RA) ai fini del processo di identificazione, i sottoscrittori e i profili di certificati rilasciati.



| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

1.3.1 Certification Authorities

Nome Organizzazione Lottomatica Holding S.r.l.
Indirizzo Viale del Campo Boario 56/d, 00154 Roma
Telefono +39 06 518991
Indirizzo email **firmaqualificata@pec.lottomatica.it** → dal **01 Marzo 2021**
l'indirizzo di riferimento sarà **caigt@pec.it**

Lottomatica Holding S.r.l. è un Prestatore di Servizi Fiduciari Qualificati (QTSP), qualificato secondo il Regolamento Europeo 910/2014 [27] in vigore dal 1 Luglio 2016, ed aderente a quanto descritto nel cap. 8.

1.3.2 Registration Authorities

La Registration Authority è una componente del QTSP, che svolge attività di identificazione e registrazione dei sottoscrittori. Il QTSP è in tutti i casi pienamente responsabile per il corretto funzionamento della Registration Authority.

Il QTSP si può avvalere di personale esterno per l'identificazione dei richiedenti certificato, come definito nel capitolo 1.3.3

Il funzionamento della Registration Authority rispetta i requisiti descritti nel presente CP CPS.

I compiti legati ai servizi di RA sono:

- L'identificazione del Sottoscrittore o del Richiedente;
- La registrazione dei dati del Soggetto;
- L'inoltro dei dati del Soggetto ai sistemi della CA;
- La raccolta della richiesta del certificato qualificato;
- Raccoglie le richieste di revoca/sospensione riemissione o rinnovo dei certificati;
- L'attivazione della procedura di certificazione della chiave pubblica.

1.3.3 Sottoscrittori e Relying Parties

I sottoscrittori sono gli utenti finali che usufruiscono del servizio. Il soggetto è la persona fisica, i cui dati sono indicati sul certificato.

Nel caso di un certificato per scopi di firma elettronica qualificata, il soggetto è il firmatario.

Ai fini delle limitazioni di cui al capitolo 1.4, si definiscono i seguenti sottoscrittori raggruppati in quattro categorie:

1. **B2B**: soggetti appartenenti al canale business (di seguito utente B2B); si tratta di persone fisiche, legali rappresentanti di punti vendita, che si vuole dotare di firma elettronica qualificata per la sottoscrizione di documenti contrattuali connessi con attività riconducibili o veicolate da Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A.;
2. **Operatori RAO** (RA Admin, Internal Master-RAO, External Master-RAO, Internal RAO e External RAO): si tratta di persone fisiche delegate da Lottomatica Holding S.r.l. ad operare l'identificazione e la richiesta di registrazione/registrazione dei sottoscrittori; in particolare:
 - a. **RA Admin**: hanno il compito di identificare i Master-RAO, di registrare sulla piattaforma del QTSP i sottoscrittori (Master-RAO, RAO, Utente Interno, Utente Firma Automatica) e di coordinare sotto la supervisione dell'RA Manager le attività degli altri RAO oltre a gestire

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

la piattaforma del QTSP; non è obbligatorio il rilascio di un certificato per questo sottoscrittore. Con la supervisione dell'RA Manager può procedere con la registrazione di un altro RA Admin.

b. **Master-RAO:**

Internal Master-RAO: hanno il compito di identificare e richiedere la registrazione dei RAO interni ed esterni, dei soggetti per la firma automatica e del personale Lottomatica (dipendenti e collaboratori); possono utilizzare il certificato di firma qualificata per controfirmare le richieste di registrazione dei soggetti che identificano.

External Master-RAO: hanno il compito di identificare e richiedere la registrazione dei RAO esterni; possono utilizzare il certificato di firma qualificata per controfirmare le richieste di registrazione dei soggetti che identificano.

c. **Internal RAO e External RAO:** sono soggetti che hanno sottoscritto apposito contratto/nomina ed hanno il compito di identificare e registrare i soggetti B2B; utilizzano il certificato di firma qualificata per controfirmare le richieste di registrazione dei soggetti che identificano;

3. **Persone Lottomatica:** sono dipendenti o collaboratori di Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A., (di seguito Utente Interno);

4. **Firma Automatica:** dipendenti o collaboratori di Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A. titolari di certificato per firma automatica (di seguito Utente Firma Automatica).

Il rapporto tra QTSP e sottoscrittori è regolato da appositi documenti che disciplinano i termini e le condizioni, firmati dai titolari al rilascio del servizio come specificato nel capitolo 9.6.3.

Gli attori esterni Master-RAO e RAO fanno parte di società/organizzazioni con le quali viene sottoscritto apposito contratto, dove sono specificati insieme al presente documento, ruoli, responsabilità e modalità di supervisione e controllo (ad esempio audit periodici) da parte del QTSP.

I RAO interni sono agenti Lottomatica.

L'identificazione e nomina degli Operatori RAO avviene a seguito di direttive e/o procedure interne al QTSP.

Le parti interessate sono i soggetti che fanno affidamento sulle informazioni contenute nel certificato digitale per le operazioni di verifica dei documenti firmati digitalmente dai sottoscrittori.

1.3.4 Altri partecipanti

Non definiti.

1.4 UTILIZZO DEL CERTIFICATO

L'area di usabilità del certificato è determinata da quanto contenuto nelle estensioni del certificato stesso. Le limitazioni d'uso sono anche specificate all'interno del presente documento.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

1.4.1 Utilizzi consentiti del certificato

I certificati sono emessi con le limitazioni d'uso riportate in doppia lingua come di seguito specificato.

Certificato del sottoscrittore B2B (IGTCP01)

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo.

Certificato del sottoscrittore Utente Interno (IGTCP03)

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo.

Certificato del sottoscrittore Utente Firma Automatica (IGTCP04)

Il certificato cui IGTCP04 è emesso con le limitazioni d'uso riportate in doppia lingua come di seguito specificato:

- The certificate may only be used for unattended/automatic digital signature;
- Il presente certificato è valido solo per firme apposte con procedura automatica.

Certificato del sottoscrittore Master-RAO, RAO (IGTCP05)

- The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued;
- Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato.

Certificato del sottoscrittore B2B (IGTCP06)

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo

Certificato del sottoscrittore Master-RAO, RAO (IGTCP07)

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued;
- Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato.

Certificato del sottoscrittore Utente Interno (IGTCP08)

- Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control;
- Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo.

Certificato del sottoscrittore Utente Firma Automatica (IGTCP09)

Il certificato cui IGTCP09 è emesso con le limitazioni d'uso riportate in doppia lingua come di seguito specificato:

- The certificate may only be used for unattended/automatic digital signature;
- Il presente certificato è valido solo per firme apposte con procedura automatica.

1.4.2 Utilizzi non consentiti del certificato

Certificato QTSP

Il certificato di root Lottomatica Holding S.r.l. e la relativa chiave privata, non può essere utilizzato prima della pubblicazione effettiva nella Trust List dei certificatori qualificati pubblicata da AgID.

Certificati sottoscrittori

Non è consentito utilizzare il certificato rilasciato e le relative chiavi private, per scopi diversi da quanto specificato in 1.4.1.

1.5 AMMINISTRAZIONE DELLA POLICY

1.5.1 Amministrazione del documento

I dati del personale che amministra il presente documento sono riportati di seguito:

| | |
|---------------------|----------------------------|
| Contatto | Carmine Tufano |
| Nome Organizzazione | Lottomatica Holding S.r.l. |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|-----------------|--|
| Indirizzo | Viale del Campo Boario 56/d, 00154 Roma |
| Telefono | + 39 06 518991 |
| Fax | - |
| Indirizzo email | firmaqualificata@pec.lottomatica.it → dal 01 Marzo 2021 l'indirizzo di riferimento sarà caigt@pec.it |

1.5.2 Responsabilità dell'Idoneità

Il QTSP è responsabile per la fornitura dei servizi in accordo con i regolamenti e gli standard citati nel presente CPS.

I servizi di certificazione e le relative procedure riportate nel presente CPS, sono sottoposti alla vigilanza dell'AgID (Agenzia per l'Italia Digitale).

La trust list dei certificati di certificazione dei Prestatori di servizi fiduciari Qualificati è resa disponibile presso il sito AgID.

1.5.3 Procedure di approvazione

Qualora previsto o a fronte di modifica ai regolamenti, il QTSP applica criteri di revisione e di approvazione del presente CPS in accordo con le procedure interne di revisione ed approvazione del documento, ed in conformità con quanto specificato in 9.12.

In particolare, il presente documento è sottoposto a un processo di revisione, almeno annuale, da parte dei Responsabili della Struttura Organizzativa del Servizio di Firma Digitale e le modifiche apportate sono sottoposte all'approvazione finale del CTO.

1.6 DEFINIZIONI ED ACRONIMI

1.6.1 Definizioni

Dal Regolamento Europeo 910-2014 eIDAS [27], Art 3:

1. «identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;
2. «mezzi di identificazione elettronica», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;
3. «dati di identificazione personale», un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;
4. «regime di identificazione elettronica», un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche;
5. «autenticazione», un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

6. «parte facente affidamento sulla certificazione», una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario;
7. «organismo del settore pubblico», un'autorità statale, regionale o locale, un organismo di diritto pubblico o un'associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un'autorità, un organismo o un'associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato;
8. «organismo di diritto pubblico», un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio;
9. «firmatario», una persona fisica che crea una firma elettronica;
10. «firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;
11. «firma elettronica avanzata», una firma elettronica che soddisfa i requisiti di cui all'articolo 26;
12. «firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;
13. «dati per la creazione di una firma elettronica», i dati unici utilizzati dal firmatario per creare una firma elettronica;
14. «certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;
15. «certificato qualificato di firma elettronica», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;
16. «servizio fiduciario», un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:
 - a. creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure
 - b. creazione, verifica e convalida di certificati di autenticazione di siti web; o
 - c. conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;
17. «servizio fiduciario qualificato», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente Regolamento;
18. «organismo di valutazione della conformità», un organismo ai sensi dell'articolo 2, punto 13, del Regolamento (CE) n. 765/2008, che è accreditato a norma di detto Regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati;
19. «prestatore di servizi fiduciari», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;
20. «prestatore di servizi fiduciari qualificato», un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;
21. «prodotto», un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;
22. «dispositivo per la creazione di una firma elettronica», un software o hardware configurato utilizzato per creare una firma elettronica;
23. «dispositivo per la creazione di una firma elettronica qualificata», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

24. «creatore di un sigillo», una persona giuridica che crea un sigillo elettronico;
25. «sigillo elettronico», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;
26. «sigillo elettronico avanzato», un sigillo elettronico che soddisfa i requisiti sanciti all'articolo 36;
27. «sigillo elettronico qualificato», un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;
28. «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;
29. «certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;
30. «certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;
31. «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;
32. «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;
33. «validazione temporale elettronica», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;
34. «validazione temporale elettronica qualificata», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;
35. «documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;
36. «servizio elettronico di recapito certificato», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;
37. «servizio elettronico di recapito qualificato certificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;
38. «certificato di autenticazione di sito web», un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;
39. «certificato qualificato di autenticazione di sito web», un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV;
40. «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;
41. «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

1.6.2 Acronimi

| | |
|------|--|
| AgID | Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari |
| CA | Certification Authority |
| CAB | Conformity Assessment Body – Organismo di valutazione conformità |
| CAD | Codice dell'Amministrazione Digitale |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|------------|--|
| CRL | Certificate Revocation List |
| HA | High Availability (Alta affidabilità) |
| HSM | Hardware Security Module |
| HTTP | HyperText Transfer Protocol |
| ICT | Information and Communication Technology |
| LIS | Lottomatica Italia Servizi S.p.A. |
| OCSP | Online Certificate Protocol Status |
| OID | Object Identifier |
| OTP | One Time PasswordPdV Punti vendita |
| PIN | Personal Identification Number – Numero di identificazione personale |
| PKI | PKI Public Key Infrastructure |
| PUK | Personal Unlock Key – Chiave personale di sblocco |
| QSCD | Qualified Signature Creation Device |
| QTSP | Qualified Trust Service Provider – Prestatore di Servizi Fiduciari Qualificato |
| MRAO | Master Registration Authority |
| RAO | Registration Authority Officer |
| RA | Registration Authority (Autorità di Registrazione) |
| RAA | Registration Authority Administrator |
| RA Manager | Responsabile della Registration Authority |
| RL | Rappresentante Legale del Punto Vendita (PdV) |
| SN | Serial Number. |
| SSL | Secure Socket Layer |
| TSA | Time Stamp Authority |
| TSU | Time Stamp Unit |
| VPN | Virtual Private Network |
| WS | Web Service |

| | | | | |
|--|------------------|---|------------------|------------------|
|  LOTTOMATICA | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |

Classificazione: Pubblico

2 PUBBLICAZIONE

2.1 REPOSITORY

Il QTSP pubblica il presente documento ed altri documenti contenenti termini e condizioni su cui è basato il proprio servizio.

I certificati, la documentazione e le CRL sono pubblicati e disponibili 24 ore al giorno per 7 giorni alla settimana.

2.2 PUBBLICAZIONE DI INFORMAZIONI DI CERTIFICAZIONE

Il certificato della CA è disponibile sul **Portale del QTSP** all'indirizzo:

<https://ca.firmadigitale.lottomaticaitalia.it/RAweb/Strumenti/Software.do>

La CA pubblica almeno la seguente documentazione sul proprio sito web:

- Certification Practice Statement (CPS);
- PKI Disclosure Statement;
- Certificati di CA;
- Modulistica;
- Elenco delle liste di revoca (CRL).

2.3 FREQUENZA DI PUBBLICAZIONE

2.3.1 Frequenza di pubblicazione dei Termini e Condizioni

Questo documento e la documentazione annessa vengono pubblicati con le modalità descritte nel paragrafo in occasione di ogni aggiornamento.

2.3.2 Frequenza di pubblicazione dei certificati

Il QTSP pubblica il certificato di root CA prima dell'avvio operativo. Il QTSP non pubblica il certificato del sottoscrittore.

2.3.3 Frequenza pubblicazione stati di revoca

Lo stato relativo ai certificati rilasciati ai sottoscrittori da parte del QTSP, deve essere immediatamente disponibile secondo quanto previsto per il servizio OCSP.

Le informazioni relative allo stato dei certificati revocati, sono pubblicate su sito all'interno della lista di revoca (CRL). L'aggiornamento della lista di revoca è in accordo con quanto specificato nel cap. 4.8.7.

2.4 CONTROLLO DEGLI ACCESSI SUI REPOSITORY

Le informazioni pubblicate sono modificate o cancellate solo ed esclusivamente dal QTSP. Il QTSP assicura altresì i controlli finalizzati alla prevenzione di modifiche non autorizzate sul suddetto repository, attraverso vari meccanismi di protezione.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

3 IDENTIFICAZIONE ED AUTENTICAZIONE

3.1 DENOMINAZIONE

Il presente capitolo stabilisce i requisiti dei dati indicati nel certificato rilasciato ai sottoscrittori, in accordo con il presente documento.

3.1.1 Tipi di nomi

Il presente documento richiede la specifica del campo Subject compatibilmente con quanto segue:

- Common Name (CN) – OID: 2.5.4.3 Il nome del Subject;
Il campo Common Name specifica la denominazione di una persona fisica.
- Surname – OID: 2.5.4.4 – Cognome della persona fisica
In questo campo deve essere specificato il cognome del Subject.
- Given Name – OID: 2.5.4.42 – Il nome della persona fisica.
In questo campo deve essere specificato il nome del Subject.
- Pseudonym – OID: 2.5.4.65 Pseudonimo del soggetto.
Lo pseudonimo del Subject può essere specificato in questo campo.
La possibilità di utilizzo di uno pseudonimo, è gestito a termini di legge.
- Serial Number – OID: 2.5.4.5 Identificativo univoco del Subject.
In questo campo è specificato un riferimento univoco associato al codice fiscale del Subject. In aderenza con quanto specificato in EN 319 412 01 v1.1.1, il SubjectDN del titolare include il campo serialNumber specificato come di seguito:
 - **"TIN": campo identificativo univoco associato alla persona; il codice fiscale del titolare;**
 - **"IT": codifica ISO 3166 del country code per L'Italia;**
 - **"-": carattere 0x2D (ASCII)**
 - **Identificativo: il valore del codice fiscale del titolare;**
- Organization – OID: 2.5.4.10 Il nome della Organizzazione
- Organization Identifier – OID: 2.5.4.97 – Identificativo della Organizzazione.
Normalmente questo campo contiene un identificativo numerico associato alla Organizzazione, come ad esempio la P.IVA.
- Organizational Unit (OU) – OID: 2.5.4.11 – Il nome della unità organizzativa.
In questo campo può essere specificato il nome di una unità organizzativa appartenente alla Organizzazione.
Il campo "OU" può esser specificato solo se sono presenti i campi "O", "L" e "C".
- Country (C) – OID: 2.5.4.6 – Identificativo del paese.
Il campo include il codice di due lettere del paese a cui appartiene l'organizzazione. Per l'Italia il presente campo ha valore "IT"
- Locality Name(L) – OID: 2.5.4.7 –Nome della località
Per una organizzazione, il campo esprime il dettaglio di dove si trova la località.
Nel caso di certificato non associato ad una Organizzazione, il campo non è utilizzato.
- DN Qualifier – OID: 2.5.4.46 – l'attributo DN Qualifier specifica informazioni di disambiguazione da aggiungere al DN del Certificato.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

3.1.2 Requisiti di identificazione

Il riconoscimento del sottoscrittore deve avvenire attraverso l'accertamento della validità dei documenti di identità forniti dal titolare, e la verifica sulla operazione di registrazione dei dati anagrafici ivi riportati. Il processo di validazione della identità viene operato nelle modalità specificate in 3.2.

3.1.3 Sottoscrittori anonimi e uso di pseudonimi

Lottomatica Holding S.r.l. rilascia i certificati qualificati a titolari sulla base dei dati anagrafici contenuti nei documenti forniti dai titolari stessi.

3.1.4 Regole per l'interpretazione dei nomi

Vedi cap 3.1.2.

3.1.5 Unicità dei nomi

Il soggetto viene identificato univocamente all'interno dei sistemi del QTSP. Al fine di indirizzare il requisito, l'anagrafica del titolare viene accompagnata da un serialNumber come specificato nel cap. 3.1.1. L'unicità del nome è conforme con quanto specificato nel documento EN 319412p02 v2.1.1 cap. 4.2.4.

Controversie legate al nome

Il QTSP, in fase di registrazione dei sottoscrittori, verifica i dati forniti dal sottoscrittore che dovranno essere riportate nel certificato. Il sottoscrittore conferma il dato attraverso esplicito consenso (vedi cap. 9.6.2). Il QTSP si riserva di revocare il certificato nel caso di uso illegale dei nomi o dei dati.

3.2 VALIDAZIONE DELL'IDENTITÀ

All'interno del seguente paragrafo sono descritte le modalità di verifica dell'identità per le differenti tipologie di richiedente certificato.

Il QTSP archivia tutte le informazioni fornite nella fase di identificazione dei sottoscrittori e in particolare il numero identificativo e la scadenza del documento di identificazione.

3.2.1 Metodi per comprovare il possesso della chiave privata

Prima del rilascio di un certificato, il QTSP deve garantire e verificare che il richiedente abbia sotto il suo controllo esclusivo la chiave privata corrispondente alla chiave pubblica del certificato.

Al momento della registrazione, al sottoscrittore viene associata un'utenza telefonica cellulare, assegnato un dispositivo Token se previsto, e consegnati i codici segreti per attivazione/utilizzo del servizio attraverso e-mail privata del titolare o numero di telefono cellulare, specificati dal titolare stesso in fase di richiesta/registrazione. Il possesso della chiave privata è comprovato attraverso un duplice meccanismo di

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

autenticazione fornito tramite 1) password/PIN fornita al titolare attraverso la modalità descritta in precedenza o scelta dal Titolare; 2) grazie alle prestazioni tecnologiche della rete GSM, ed un sistema di OTP (One Time Password): il QTSP effettua la verifica dell'identità del sottoscrittore accertandosi che egli stia usando esattamente l'utenza telefonica cellulare (o token fisico) che ha dichiarato al momento della sua registrazione. A tal fine, il sottoscrittore riceve via cellulare un codice numerico OTP utilizzato per le verifiche come secondo fattore di autenticazione.

3.2.2 Processi di consegna Token OTP fisici

Procedure di consegna dei dispositivi Token fisici

Il QTSP attua procedure interne al fine di assegnare al sottoscrittore al momento della registrazione, o successivamente, il Token fisico per la generazione di codici OTP per l'utilizzo dei servizi di firma.

Il QTSP consegna, tramite gli incaricati nelle proprie sedi, i Token fisici, registrando l'avvenuta consegna, e associando all'utente il numero seriale univoco del Token OTP. Il Token fisico per la generazione dei codici OTP per l'utilizzo dei servizi di firma può essere alternativamente inviato tramite raccomandata A/R in busta chiusa all'indirizzo di contatto fisico indicato in fase di identificazione. In quest'ultimo caso i dispositivi vengono rilasciati non attivi, e prima del loro utilizzo dovrà necessariamente essere effettuata la procedura di abilitazione, che prevede:

- Accesso con le proprie credenziali all'URL: <https://ca.firmadigitale.lottomaticaitalia.it/RAweb>;
- Accedere alla sezione "Interrogazioni-Token" ed eseguire la procedura di abilitazione del dispositivo OTP seguendo le istruzioni fornite.

Il QTSP registra sul sistema di Registration Authority tutte le informazioni necessarie per la corretta abilitazione del dispositivo.

3.2.3 Validazione dell'identità di una entità organizzativa

Il QTSP rilascia certificati di firma elettronica qualificata esclusivamente a persone fisiche.

3.2.4 Validazione dell'identità di una entità individuale

Il processo di verifica dell'identità associata con il rilascio di un certificato di firma elettronica qualificata, in accordo con l'articolo 24 del Regolamento 910/2014 (eIDAS [27]), è assicurato attraverso la presenza concreta della persona fisica o tramite conoscenza pregressa in base a quanto specificato nei paragrafi 3 e 4 del presente documento.

Modalità di identificazione per sottoscrittori RA Admin, Master-RAO, RAO, Persone Lottomatica e Firma Automatica

Il processo prevede il riconoscimento de visu. Di seguito si riporta una tabella che identifica per i diversi tipi di sottoscrittori i soggetti che possono effettuare l'identificazione e convalida dell'identità:

| Sottoscrittore | Identificato da |
|------------------------------|------------------------|
| RA Admin | RA Manager |
| Internal/External Master-RAO | RA Admin |
| Internal RAO | Internal Master-RAO |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|---------------------|------------------------------|
| External RAO | Internal/External Master-RAO |
| Firma Automatica | Internal Master-RAO |
| Persone Lottomatica | Internal Master-RAO |

Il processo prevede le seguenti attività:

- Identificazione attraverso i documenti di identità in corso di validità;
- Raccolta anagrafica e verifica la rispondenza;
- Compilazione apposito modulo di identificazione/nomina;

Se il soggetto viene identificato con successo, si procede verificando le competenze formative se previste per il ruolo.

Qualora il sottoscrittore di tipo "Persone Lottomatica" sia un dipendente di Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A., ed il soggetto che lo identifica sia un Master-RAO che lavora all'interno della funzione HR di Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A., in tale contesto, l'utente risulta essere stato già oggetto di procedure finalizzate all'identificazione in adempimento alla stipula del contratto di lavoro/collaborazione con Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A.. I dati relativi all'Identità del Titolare sono dunque acquisiti, verificati mantenuti aggiornati nell'ambito delle attività normalmente svolte dalla Funzione Risorse Umane e dagli uffici amministrativi di competenza.

Tutte le risorse (Dipendenti Aziendali) sono dunque identificate nei processi di assunzione e censiti nell'ambito del Gestionale di Risorse Umane (SAP-HCM: Master Anagrafico dei Dipendenti).

Ogni nuova assunzione viene peraltro comunicata da HR attraverso un flusso e-mail alle funzioni IT che svolgono attività specifiche di supporto, quale: la Funzione Sicurezza, la Funzione di Office Automation e Trusted Services.

I Dipendenti oltre ad essere censiti nel DB-HR sono inseriti nella Active Directory aziendale che gestisce per ciascuna identità una "Matricola" univoca, identificativo che consente accesso ai Sistemi e Dispositivi aziendali quali PC e Posta Elettronica; nella Active Directory è dunque inserito l'indirizzo e-mail aziendale o il proprio numero di cellulare.

In ogni caso prima dell'invio della richiesta di certificato, secondo le modalità descritte nel par. 4.1, il Master-RAO che lavora all'interno della funzione HR richiede al Dipendente copia di un documento di identità in corso di validità (F/R), tessera sanitaria (F/R) e numero di cellulare.

Modalità di identificazione B2B

| Sottoscrittore | Identificato da |
|-----------------------|------------------------|
| B2B | Internal/External RAO |

Si procede all'identificazione de visu come segue:

- Il RAO richiede all'utente B2B il Codice Fiscale, un documento d'identità in corso di validità, un numero di cellulare ed un indirizzo e-mail;
- Effettua il riconoscimento "de visu" dell'utente B2B verificando la validità del documento e l'effettiva corrispondenza dei dati con il codice fiscale;
- Acquisisce, inserendoli tramite terminale, i dati del documento di identità indicati (tipo documento, numero documento, ente che ha rilasciato il documento, data di emissione documento, data di scadenza documento), l'immagine del documento, e-mail e cellulare.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

L'utente B2B, in quanto legale rappresentante di un PdV, è oggetto di ulteriori controlli mirati ad accettarne la rispondenza ai requisiti necessari ad instaurare un rapporto contrattuale, tra cui:

- Accertamenti sulla bontà dei dati anagrafici forniti;
- Verifica della presenza dell'utente B2B all'interno di liste antiriciclaggio (AML) ed antiterrorismo.
- Visura camerale;
- Verifiche creditizie.

Ai fini di un rilascio di certificato da Portale Rivenditori con le modalità descritte nel par. 4.1, se il B2B ha rapporti contrattuali già in essere con Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A., l'utente B2B risulta essere stato già oggetto di procedure finalizzate all'identificazione in adempimento ai regolamenti / leggi di settore (es. AML) e alla verifica del possesso dei requisiti richiesti dagli standard aziendali (es. Credito); Il processo di attivazione di un Punto Vendita, prevede l'effettuazione, in via preventiva, di controlli volti a verificare il possesso dei requisiti di rispettabilità, onorabilità e solvibilità da parte dello stesso, oltre che una due diligence sulle persone fisiche collegate.

In particolare, il Punto Vendita viene automaticamente sottoposto a controlli camerali, nonché verifiche reputazionali su fonti aperte (Worldcheck). L'esito di tali verifiche consente di attribuire al punto vendita uno scoring di rischio di Compliance-AML, sulla base di apposite regole e criteri definiti in linea con il D.Lgs. 231/07 (criterio geografico, tipo di attività svolta, presenza nelle liste, ...). Con riferimento al monitoraggio continuo della permanenza dei requisiti reputazionali, si sottolinea anzitutto che, allorché Lottomatica Holding S.r.l. venga a conoscenza di eventi pregiudizievoli (sequestri, altre misure cautelari, notizie negative dalla stampa, ...), si attiva un processo di revisione della relazione con l'esercente interessato che porta all'effettuazione di un'istruttoria, in base alla quale il management decide le opportune azioni da intraprendere.

Lottomatica Holding S.r.l. adotta una soluzione informatica finalizzata ad automatizzare tale processo di monitoraggio. In particolare, attraverso tale soluzione, la base dati dei Punti Vendita viene sottoposta a scoring reputazionale e "compliance", mediante l'utilizzo di tabelle decisionali ispirate ai principi di approccio di rischio del D.Lgs. 231/07. Inoltre, il presidio di monitoraggio implementato prevede che la rete di Lottomatica Holding S.r.l. venga quotidianamente sottoposta sia a verifiche camerali (finalizzate ad acquisire eventuali aggiornamenti anagrafici e societari) sia ad analisi "di compliance" (finalizzate a intercettare possibili variazioni del profilo di rischio ed eventuali notizie negative sotto il profilo reputazionale).

3.2.5 Informazioni di sottoscrizione non verificabili

Si consulti il cap. 3.1.3.

3.3 IDENTIFICAZIONE ED AUTENTICAZIONE PER RIEMISSIONE

La riemissione del certificato è il processo nel quale il QTSP rilascia un nuovo certificato, al posto del precedente, per necessità di contrattualizzazione o per garantire la continuità delle proprie attività e servizi laddove:

- Siano sopraggiunti limiti di validità;
- Per avvenuta revoca del precedente certificato;
- Per variazione delle informazioni (ad esempio, uno dei dati del subject del certificato, numero di cellulare, e-mail) connesse con il certificato o con l'uso della firma.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Per il sottoscrittore B2B la riemissione del certificato avviene solo in caso di variazione di uno dei dati del subject del certificato, numero di cellulare o e-mail mentre per tutti le altre casistiche non si procede ad una riemissione ma viene effettuata una revoca da parte del QTSP.

In caso di riemissione, il QTSP verifica sempre l'esistenza e la validità dei certificati del titolare.

3.3.1 Identificazione e Autenticazione per riemissione di un certificato in corso di validità

Questa modalità si effettua se al momento della richiesta di riemissione il certificato è in corso di validità e se le operazioni di riemissione possono essere completate prima della sua scadenza.

Se le informazioni del sottoscrittore sono in corso di validità ed inviate alla CA/RA non oltre 39 mesi prima possono essere utilizzati per la validazione, altrimenti è necessario che il sottoscrittore le invii/fornisca nuovamente.

Per il sottoscrittore B2B, se la richiesta di riemissione avviene a causa di una variazione di almeno uno dei seguenti dati:

- Nome;
- Cognome;
- CF;
- E-mail;
- Cellulare.

Si procede con la riemissione effettuando l'identificazione nelle medesime modalità del primo rilascio.

3.3.2 Identificazione e Autenticazione per riemissione dopo revoca/scadenza

La riemissione del certificato conseguente alla revoca/scadenza prevede quanto specificato nel 3.2.

3.4 IDENTIFICAZIONE ED AUTENTICAZIONE IN CASO DI RICHIESTE DI MODIFICA DEL CERTIFICATO

Si veda il punto 3.3.

3.5 IDENTIFICAZIONE ED AUTENTICAZIONE PER RICHIESTE DI REVOCA

Il QTSP processa le richieste di revoca del certificato di firma. Le richieste possono essere inoltrate tramite funzionalità accessibile da link preposto sul **Piattaforma del QTSP**, previa autenticazione del sottoscrittore.

I meccanismi di autenticazione prevedono l'uso delle credenziali di accesso.

Le richieste possono essere inoltrate anche tramite i recapiti del QTSP dal sottoscrittore o dagli operatori RAO. Il QTSP accerta sempre l'identità del richiedente e la veridicità della richiesta.

4 REQUISITI CICLO DI VITA DEL CERTIFICATO

4.1 RICHIESTA DI UN CERTIFICATO

Il certificato di firma elettronica qualificata rilasciato da Lottomatica Holding S.r.l., viene utilizzato compatibilmente con le limitazioni d'uso specificate nel cap. 1.4.

Ogni nuovo processo di emissione di un certificato di sottoscrizione, è sottoposto alla verifica della identità del soggetto compatibilmente con quanto specificato nel cap. 3, ed in particolare nelle modalità descritte nel capitolo 3.2.

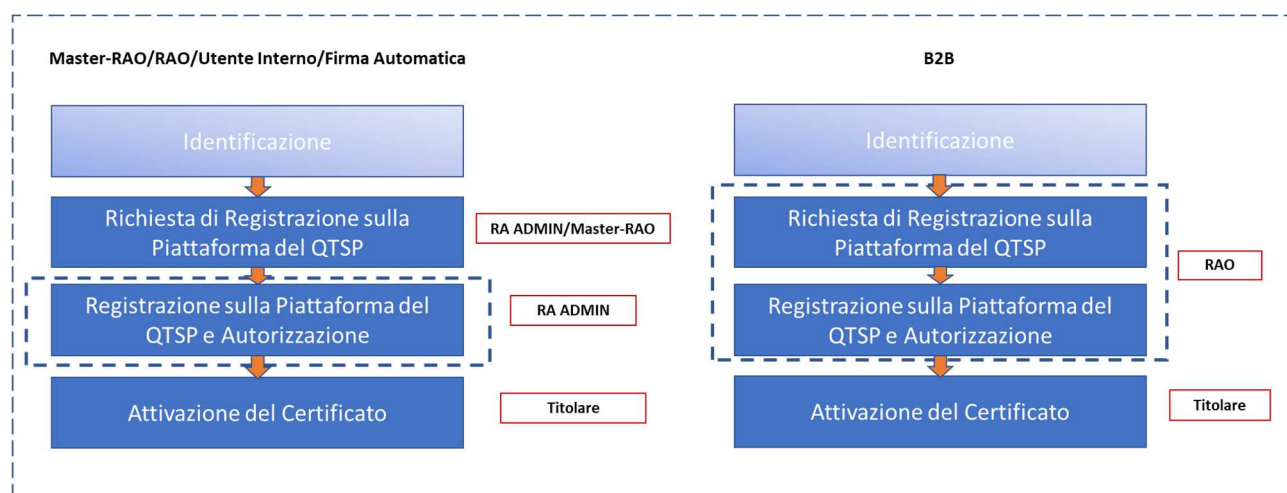
| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

L'identificazione e la registrazione dei dati del titolare sono convalidate attraverso modalità differenti a seconda della tipologia di appartenenza al canale di sottoscrizione (Master-RAO, RAO, B2B, Uso Interno, Firma Automatica).

La procedura di generazione delle chiavi e del relativo certificato è sottoposta ad accettazione da parte del sottoscrittore delle condizioni e dei termini di utilizzo del servizio. Il documento di accettazione è proposto in un formato comprensibile e dà la possibilità al titolare di poterlo scaricare in formato elettronico, al fine di poterlo stampare. L'accettazione da parte del sottoscrittore dei dati proposti costituisce accettazione della validità dei dati anagrafici visualizzati nel documento.

Unitamente al documento di contratto, il richiedente fornisce i documenti, le certificazioni, le procure o le dichiarazioni necessarie per la convalida dell'identità della persona fisica che sarà titolare del certificato qualificato.

Di seguito viene illustrato il flusso e gli attori coinvolti per i diversi sottoscrittori, descritti nel dettaglio nei successivi paragrafi:



Per l'utente B2B l'attivazione del certificato può avvenire anche tramite il Portale Rivenditori secondo le modalità descritte nei paragrafi successivi.

Richiesta certificato RA Admin, Master-RAO, RAO, Persone Lottomatica e Firma Automatica

Tramite opportuni strumenti di tracciamento interni, viene inserita la richiesta di certificato.

Il workflow approvativo prevede i seguenti step autorizzativi:

- Registration Authority Manager;
- Responsabile del Servizio di Certificazione e Validazione Temporale;

Qualora, secondo quanto previsto dal piano di business continuity o da specifici documenti di delega/comunicazioni, siano indisponibili i precedenti responsabile l'iter approvativo sarà condotta dai sostituti.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Per la richiesta di registrazione sulla Piattaforma del QTSP è previsto l'invio di un'e-mail a calottomatica@igt.com e al Registration Authority Manager contenente almeno:

- documento di riconoscimento fronte/retro (carta d'identità, patente di guida o passaporto).
- Codice Fiscale fronte/retro;
- esito del test di formazione (laddove previsto);

Tutti i documenti sono conservati in una cartella di rete accessibile solo alle persone autorizzate della funzione Trusted Services, e al Registration Authority Manager.

In seguito alla chiusura del workflow approvativo ed alla ricezione della documentazione prevista, i dati sono registrati dall'RA Admin all'interno della piattaforma del QTSP comprensivi di e-mail, cellulare, tipo documento, numero documento, data di scadenza documento, data di rilascio, emittente del documento.

L'RA Admin autorizza la richiesta del certificato, tramite Piattaforma del QTSP.

L'attività si conclude con l'invio di una e-mail generata in modo automatico al sottoscrittore contenente le credenziali di primo accesso e le istruzioni su come procedere.

Ricevuta la e-mail, il sottoscrittore procede all'attivazione del certificato:

- in seguito, accede alla sezione "Attivazione del Certificato" e procede all'attivazione della firma confermando gli estremi dei dati anagrafici prospettati a video, ivi incluso il numero di cellulare (necessario per OTP via SMS); in seguito in base alla tipologia di OTP:

➤ **OTP via SMS:**

L'utente quindi procede:

- All'inserimento di un nuovo codice PIN e la relativa conferma;
- Alla lettura delle condizioni generali del servizio;
- All'avvio della procedura di attivazione.

Il sistema, quindi, procede con:

- La generazione delle chiavi di sottoscrizione utilizzando il PIN specificato dal titolare, in conformità con quanto specificato nel cap.6.1.1;
- L'invio della richiesta di certificato alla CA;
- L'installazione del certificato generato dalla CA;
- L'inizializzazione del sistema OTP di cui al punto 6.3;
- L'invio della credenziale OTP via SMS, per lo sblocco della operazione di Firma. L'SMS è inviato al numero di telefono fornito in fase di validazione dell'identità (par.3.2).

➤ **Token fisico:**

- L'utente inserisce un nuovo codice PIN personale di firma confermando i dati;
- L'utente legge le condizioni generali del servizio;
- Il sistema genera le chiavi di sottoscrizione utilizzando il PIN specificato dal titolare, in conformità con quanto specificato nel cap.6.1.1;
- Il sistema invia la richiesta di certificato alla CA;
- Il sistema installa il certificato generato dalla CA;
- All'utente è assegnato un Token fisico per la generazione di codici OTP per lo sblocco delle operazioni di firma;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- L'utente accede alla sezione OTP abilitando il proprio Token fisico a sistema;
 - L'utente accede alla sezione Enroll inserendo il codice OTP generato dal Token fisico abilitando la generazione di codici OTP per lo sblocco delle operazioni di firma.
- L'utente, con il proprio PIN e Token OTP, sottoscrive le condizioni generali del servizio precedentemente lette.
 - Il QTSP conserva la dichiarazione firmata digitalmente dal Titolare con la quale questi certifica i dati e l'accettazione delle condizioni generali del servizio.
 - L'attività si conclude con l'invio di una e-mail generata in modo automatico dal QTSP al sottoscrittore con la conferma della creazione del certificato.

Richiesta di certificato B2B

Successivamente alla convalida dell'identità con una delle procedure descritte nel cap. 3.2 del presente documento, è l'utente RAO a confermare l'avvio della procedura durante la contrattualizzazione del PdV. Tramite l'apposito applicativo di contrattualizzazione richiede la registrazione/registra l'anagrafica del sottoscrittore B2B sul Piattaforma del QTSP, autorizza contestualmente il certificato, e:

- Si assicura che il sottoscrittore abbia letto ed accetti le condizioni generali del servizio;
- conferma sottoscrivendo digitalmente (con firma remota) il documento di rilascio del certificato al titolare del punto vendita.

Il sistema, quindi, procede con:

- La generazione delle chiavi di sottoscrizione in conformità con quanto specificato nel cap. 6.1.1, utilizzando un PIN randomico generato al momento;
- L'invio della richiesta di certificato alla CA;
- L'installazione del certificato generato dalla CA;
- L'inizializzazione del sistema OTP di cui al punto 6.3;
- L'invio della credenziale PIN e dell'OTP attraverso 2 SMS separati, per lo sblocco della operazione di Firma.

L'utente, con il proprio PIN e l'OTP ricevuto via SMS, sottoscrive le condizioni generali del servizio precedentemente espone.

Gli SMS sono inviati al numero di telefono fornito in fase di validazione dell'identità (par.3.2).

Il QTSP mantiene a sua disposizione in conservazione sostitutiva la dichiarazione firmata digitalmente dal Titolare con la quale questi certifica i dati che ha fornito al RAO per la registrazione al momento dell'identificazione e l'accettazione delle condizioni generali del servizio, accompagnata dalla dichiarazione sottoscritta digitalmente dal RAO che attesta l'esecuzione dell'operazione di identificazione secondo le istruzioni fornite dal QTSP.

In caso di sottoscrittori B2B che hanno rapporti contrattuali già in essere con Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A. Il processo consente a legali rappresentati di Punti Vendita aventi rapporti contrattuali già in essere con Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A., di ottenere un Certificato di Firma Digitale Remota attraverso l'utilizzo del Portale Rivenditori. In questo caso:

- L'utente accede al Portale Rivenditori con le credenziali già in suo possesso;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- L'utente B2B verifica i propri dati (tra cui il numero di cellulare) presenti sui sistemi anagrafici e richiede l'attivazione di un nuovo certificato. Tali dati, sia anagrafici che di contatto, non risultano modificabili. Nel caso rilevi la necessità di modificarne alcuni fruisce di servizi e processi di modifica e verifica dei dati anagrafici realizzati in adempimento alle normative / leggi / standard di settore (es. direttive AML, schemi atti di convenzione, etc.).
- Se tramite, controllo attraverso la Certification Authority, l'utente non ha già un certificato attivo, allora il Legale Rappresentante, richiede esplicitamente la creazione di un nuovo certificato, tale richiesta genera 2 documenti:
 - Il primo riporta i dati anagrafici e di contatto del Titolare e viene firmato digitalmente attraverso un certificato di firma automatica;
 - Il secondo sono le Condizioni Generali di Servizio (CGS).
- Il Rappresentante Legale del PDV riceve su 2 sms distinti il codice PIN ed il codice OTP;
- Il Rappresentante Legale del PdV ha la possibilità, dunque, di prendere visione/leggere le CGS (Condizioni Generali di Servizio) e firmarle inserendo PIN ed OTP ricevute sul proprio cellulare e completare così il processo.

La modalità di rilascio ambito del presente paragrafo consente all'utente B2B di ottenere un certificato di firma digitale Remota nell'ambito delle limitazioni di uso del certificato.

4.1.1 Sottomissione della richiesta di certificato

La richiesta del certificato può essere convalidata esclusivamente a seguito delle procedure di accertamento della identità del titolare.

La conferma della validità dei dati viene processata in funzione del canale di appartenenza del titolare a cui è rilasciato il certificato Qualificato. In ogni caso, la sottomissione della richiesta per la registrazione sulla piattaforma del QTSP ai fini dell'emissione del certificato viene eseguita da:

| Sottoscrittore | Richiesta Registrazione sulla Piattaforma del QTSP |
|------------------------------|---|
| RA Admin | RA Manager |
| Internal/External Master-RAO | RA Admin |
| Internal RAO | Internal Master-RAO |
| External RAO | Internal/External Master-RAO |
| Firma Automatica | Internal Master-RAO |
| Persone Lottomatica | Internal Master-RAO |
| B2B | Internal/External RAO |

Il sottoscrittore B2B può procedere alla richiesta anche tramite Portale Rivenditori secondo le modalità descritte precedentemente

4.1.2 Processo di Registrazione/Enroll e Responsabilità

Il processo di Registrazione/Enroll ha il principale compito di emettere il certificato di sottoscrizione.

Il QTSP, ricevuta la conferma sull'avvio della procedura di emissione, deve registrare le informazioni relative alla anagrafica del titolare, prima di procedere alla generazione del certificato.

Prima dell'avvio della procedura di attivazione, il sottoscrittore è chiamato a controllare i propri dati anagrafici ed a prendere visione delle condizioni e dei termini del servizio.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

La registrazione sulla Piattaforma del QTSP e la successiva autorizzazione della richiesta viene eseguita da:

| Sottoscrittore | Registrazione e Autorizzazione Richiesta Certificato |
|------------------------------|---|
| RA Admin | RA Admin |
| Internal/External Master-RAO | RA Admin |
| RAO | RA Admin |
| Firma Automatica | RA Admin |
| Persone Lottomatica | RA Admin |
| B2B | Internal/External RAO |

La registrazione e la successiva autorizzazione del certificato per i sottoscrittori Master-RAO, RAO, Firma Automatica, Persone Lottomatica viene effettuata dall'RA Admin direttamente dalla Piattaforma del QTSP. La registrazione per l'utente B2B avviene tramite l'applicativo di contrattualizzazione, l'autorizzazione può avvenire tramite l'applicativo di contrattualizzazione o il Portale Rivenditori.

Gli eventi conseguenti alla conferma dell'anagrafica e a quella relativa ai termini d'uso del servizio sono registrati dal QTSP ed archiviati per un periodo di tempo di anni venti. Qualora l'identità del sottoscrittore non sia validata dal sottoscrittore, il processo di attivazione del certificato non deve essere eseguito.

4.1.3 Attivazione del certificato

L'attivazione del certificato può essere fatta esclusivamente dal Titolare e prevede sempre, l'accettazione delle condizioni generali di servizio, firmate digitalmente, tramite lo sblocco della chiave privata associata attraverso la scelta, nel caso non sia un B2B per il quale viene generato in maniera automatica e randomica, di un proprio codice PIN e all'inserimento di un codice OTP, secondo le modalità descritte nel par. 4.1.

4.2 PROCESSI DI GESTIONE DELLA RICHIESTA DI CERTIFICATO

4.2.1 Esecuzione di funzioni di Identificazione e di Autenticazione

Il QTSP identifica il sottoscrittore in accordo con quanto pubblicato nel cap. 3.2.

4.2.2 Approvazione o rigetto

L'approvazione della richiesta può avere luogo qualora:

- Il titolare disponga dei requisiti connessi con l'accertamento della sua identità;
- Il titolare accetti i termini e condizioni sulla erogazione del servizio.

Il rigetto della richiesta può avere luogo qualora

- Non sia verificata nessuna delle condizioni per l'approvazione;
- Il titolare disponga di un altro certificato (con lo stesso profilo di certificato) valido a suo nome, che non sia prossimo alla scadenza.

4.2.3 Tempo di esecuzione della richiesta

Il certificato è rilasciato al termine di riscontri positivi a seguito delle procedure di accertamento sull'identità del titolare.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Tempi di esecuzione della richiesta per utente Master-RAO/RAO

Non sono definiti tempi legati alla gestione della richiesta, se non quelli legati alla validazione dei dati da parte del personale preposto, ed alla transazione telematica necessaria per l'esecuzione della procedura di Enroll.

Tempi di esecuzione della richiesta per utente B2B

Non sono definiti tempi legati alla gestione della richiesta, se non quelli legati alla validazione dei dati da parte del RAO, ed alla transazione telematica necessaria per l'esecuzione della procedura di Enroll.

Tempi di esecuzione della richiesta per il certificato per utente Automatica

Non sono definiti tempi legati alla gestione della richiesta, se non quelli legati alla validazione dei dati da parte di personale preposto, ed alla transazione telematica necessaria per l'esecuzione della procedura di Enroll.

Tempi di esecuzione della richiesta per utente interno

Non sono definiti tempi legati alla gestione della richiesta, se non quelli legati alla validazione dei dati da parte di personale preposto, ed alla transazione telematica necessaria per l'esecuzione della procedura di Enroll.

4.3 RILASCIO DEL CERTIFICATO

Per tutte le tipologie di sottoscrizioni:

- Il QTSP rilascia il certificato all'utente successivamente:
 - Alla convalida della identità del soggetto, con uno dei sistemi descritti in 3.2;
 - Alla accettazione dei termini e condizioni d'uso prima della emissione;
- Alla esecuzione con successo dei processi informatici necessari:
 - Alla convalida della identità del sottoscrittore, con uno dei sistemi descritti in 3.2;
 - Alla accettazione dei termini e condizioni d'uso da parte del sottoscrittore;
 - Alla convalida dei propri dati anagrafici;
 - Alla scelta, nel caso non sia un B2B per il quale viene generato in maniera automatica e randomica, di un proprio codice PIN associato alla operazione di Firma;
 - All'insieme delle operazioni tecniche connesse con la generazione delle chiavi di sottoscrizione e la relativa certificazione da parte della CA Lottomatica Holding S.r.l.;
 - Alla inizializzazione del sistema OTP di cui al punto 6.3.

4.3.1 Azioni di CA durante il rilascio del certificato

Il certificato viene emesso con le misure di sicurezza conformi alle norme in vigore.
La CA ha l'obbligo di emettere il certificato sulla base dei dati anagrafici contenuti nella richiesta pervenuta.

| | | | | |
|---|------------------|---|------------------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |

Classificazione: Pubblico

4.3.2 Notifiche al titolare circa il rilascio del certificato

Il QTSP informa il titolare circa l'emissione del certificato attraverso una notifica verso l'indirizzo e-mail fornito dal titolare in fase di gestione della richiesta.

4.4 ACCETTAZIONE DEL CERTIFICATO

4.4.1 Condotta sulla accettazione del certificato

Il rilascio del certificato, delle chiavi connesse e dei parametri di attivazione, sono rilasciate sotto il controllo esclusivo del titolare nel rispetto dei termini e condizioni da lui accettati.

4.4.2 Pubblicazione del certificato da parte della CA

Il QTSP non rende pubblici i certificati generati. Le condizioni correlate sono contenute nelle condizioni generali del servizio accettate dal titolare.

4.5 COPPIA DI CHIAVI E UTILIZZO DEL CERTIFICATO

4.5.1 Chiave privata del sottoscrittore e utilizzo del certificato

Il sottoscrittore utilizza la propria chiave privata corrispondente al certificato a lui rilasciato, solo per le condizioni specificate nel cap. 1.4. Ogni altro uso del certificato, è proibito.

L'operazione di sottoscrizione, è utilizzata dai titolari secondo il seguente schema:

- Per utenti B2B la sottoscrizione è prevista solamente per la firma di file di tipo PDF e PDF/A, esclusivamente nel contesto di un processo connesso alla contrattualizzazione dell'utente o processi veicolati/riconducibili secondo le limitazioni di uso specificate, realizzato attraverso soluzioni informatiche (es. portali web, sistemi ad uso interno) dedicate a tale scopo;
- L'utente Master-RAO/RAO firma documenti secondo le limitazioni d'uso definite nel par.1.4.1 attraverso soluzioni informatiche (es. portali web, sistemi ad uso interno) dedicate a tale scopo; il RAO firma il modulo di registrazione utenti B2B;
- Per l'utente interno, è consentita la firma di documenti mediante soluzioni informatiche dedicate a tale scopo ed utilizzabili in compliance con le limitazioni d'uso definite nel paragrafo 1.4.1. Nello specifico, tali soluzioni informatiche, accettano qualsiasi formato di documento o file, consentendo l'applicazione della firma nei formati:
 - PAdES/PAdES-T per documenti PDF;
 - CAdES/CAdES-T per tutti gli altri documenti.
- Per l'utente Firma Automatica, la firma di documenti è realizzata solo da sistemi di Lottomatica Holding S.r.l. e/o LIS - Lottomatica Italia Servizi S.p.A. o società sottoposte al comune controllo di Lottomatica Holding S.r.l. o LIS - Lottomatica Italia Servizi S.p.A. o Lottomatica Italia Servizi S.p.A. opportunamente configurati all'utilizzo del certificato di Firma Automatica. Tali sistemi accettano qualsiasi formato di documento o file, consentendo l'applicazione della firma nei formati:
 - PAdES/PAdES-T per documenti PDF;
 - CAdES/CAdES-T per tutti gli altri documenti.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Il QTSP è garante che il documento sottoposto a firma, non contenga macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati, in aderenza con l'Art.4 comma 3 del DPCM 22 febbraio 2013 [24].

Il QTSP stabilisce che una chiave privata corrispondente ad un certificato scaduto, revocato o sospeso, non deve essere utilizzata per la creazione di una firma elettronica qualificata.

Il sottoscrittore deve garantire adeguata protezione dei dati di attivazione della firma elettronica qualificata in particolare al verificarsi delle seguenti condizioni

- Perdita controllo degli strumenti di sblocco della firma;
- Perdita di possesso del cellulare o cambio del numero fornito;
- Cambio di numero cellulare.

A seguito degli eventi sopra menzionati, il titolare è tenuto a richiedere la revoca e la conseguente riemissione del certificato.

4.5.2 Parti interessate – Chiave pubblica e utilizzo del certificato

Le parti interessate alla verifica di una firma elettronica qualificata, devono procedere secondo quanto contenuto nel presente CPS con particolare riferimento a quanto di seguito:

- Le parti interessate devono verificare la validità e lo stato di revoca del certificato; in particolare si raccomanda che la verifica del certificato sia eseguita attraverso la validazione completa della catena dei certificati, accertando che il certificato di firma elettronica qualificata sia stato emesso da Lottomatica Holding S.r.l. mediante riconoscimento del certificato di root CA di Lottomatica Holding S.r.l. stessa, pubblicato da AgID sul proprio sito;
- Il certificato di firma elettronica qualificata e la corrispondente chiave pubblica, deve esclusivamente essere utilizzato per la validazione della firma stessa;
- Le parti interessate devono tenere conto delle limitazioni d'uso indicate nel certificato, in accordo con quanto contenuto nel capitolo 1.4.

Il QTSP espone servizi per consentire a sottoscrittori e parti interessate la verifica dei certificati rilasciati, in accordo con quanto specificato nel cap. 4.9.

4.6 RIEMISSIONE

Per riemissione del certificato si intende la rigenerazione delle chiavi e del certificato, previsto nei casi specificati in 4.6.1.

4.6.1 Requisiti per la riemissione del certificato

La riemissione del certificato può essere eseguita esclusivamente quando sono verificate le seguenti condizioni:

- Il precedente certificato di firma elettronica qualificata è revocato;
- Il precedente certificato di firma elettronica qualificata sia scaduto.
- L'identità del titolare indicata nel certificato è ancora valida;
- Sia effettuato quanto previsto dal 3.3.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

4.6.2 Sottomissione richiesta di riemissione

Richiesta di Riemissione

La richiesta di riemissione del certificato deve essere avviata o approvata dal Titolare.
L'attivazione del certificato può essere fatta esclusivamente dal Titolare, con le stesse modalità descritte per la prima emissione, attraverso i dati di contatto dallo stesso forniti.
Dopo che il QTSP ha autorizzato la richiesta di certificato è il Titolare che procede alla sua attivazione.

4.6.3 Processo della richiesta di riemissione

Nel processo di valutazione della richiesta di riemissione, il QTSP assicura che:

- La richiesta di riemissione sia autentica;
- Il richiedente sia autorizzato a procedere;
- Sia stata eseguita una corretta valutazione dei dati anagrafici presenti a sistema.

I metodi utilizzati per l'identificazione e l'autenticazione per il processo di riemissione, sono descritti nel cap. 3.3.

L'autorizzazione della richiesta di certificato avviene nelle stesse modalità della prima emissione, così come specificato nel par. 4.1

4.6.4 Registrazione sulla piattaforma del QTSP e Autorizzazione del certificato

In caso di riemissione il titolare risulta essere già censito nella piattaforma del QTSP. In questo caso, in caso di modifica dei dati del titolare, si provvede ad un aggiornamento dell'anagrafica prima dell'autorizzazione della richiesta di certificato.

L'RA Admin provvede all'aggiornamento dell'anagrafica, se necessario, per i seguenti sottoscrittori:

- Master-RAO;
- RAO;
- Utente Interno;
- Utente Firma Automatica.

Il RAO attraverso l'apposito applicativo di contrattualizzazione provvede all'aggiornamento dell'anagrafica, se necessario, per il sottoscrittore B2B.

In seguito tramite la piattaforma del QTSP o tramite applicativo di contrattualizzazione/Portale Rivenditori si avvia l'autorizzazione della richiesta certificato come previsto per la prima emissione.

4.6.5 Attivazione del Certificato

Il processo di attivazione del Certificato da parte del Titolare prevede quanto specificato per la prima emissione, descritti nel par. 4.1.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

4.6.6 Notifiche relative al rilascio del certificato

Il QTSP notifica al sottoscrittore l'emissione del certificato attraverso l'indirizzo e-mail fornito dal titolare in fase di gestione della richiesta.

4.6.7 Condotta sulla accettazione della riemissione del certificato

Una volta rilasciato il certificato, il sottoscrittore è chiamato alla conferma dei dati in esso contenuti attraverso la firma elettronica qualificata a cui il certificato è connesso (firma della CGS).

4.6.8 Pubblicazione del certificato rimesso da parte della CA

Il QTSP non pubblica i certificati di sottoscrizione, ma li rende disponibili esclusivamente al titolare.

4.7 MODIFICHE AL CERTIFICATO

Il QTSP non effettua né permette di effettuare modifiche al certificato.

4.8 REVOCA E SOSPENSIONE DEL CERTIFICATO

Per revoca del certificato si intende la procedura con la quale il QTSP termina la validità di un certificato, prima della sua naturale scadenza. La revoca di un certificato è permanente, e non reversibile; un certificato revocato non può tornare valido.

Nel caso di revoca del certificato, il QTSP può eliminare le chiavi del sottoscrittore utilizzando le procedure in accordo con il manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione.

In seguito alla revoca del certificato il QTSP notifica al titolare l'avvenuta modifica dello stato del certificato.

Il QTSP non effettua la sospensione del certificato.

4.8.1 Circostanze di revoca

Il QTSP può revocare il certificato del sottoscrittore nelle seguenti casistiche:

- Cambiamento dei dati del Subject del certificato;
- Cambio di e-mail e cellulare associati al certificato;
- Cambiamento delle limitazioni di uso del certificato;
- Il QTSP verifica che i dati relativi al certificato non corrispondono alla realtà;
- Il titolare richiede la revoca del certificato per iscritto o per via telematica;
- Il QTSP verifica che la chiave privata non è sotto il controllo esclusivo del sottoscrittore;
- Il QTSP verifica che il certificato viene utilizzato al di fuori degli scopi consentiti;
- Il QTSP verifica che la chiave pubblica contenuta nel certificato non è compatibile con quanto specificato nei capitoli 6.1.5 e 6.1.6;
- Il QTSP verifica che il certificato non è stato rilasciato in conformità con il presente CPS;
- Il QTSP verifica che la chiave privata del sottoscrittore è stata o potrebbe essere stata compromessa;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Il QTSP verifica la cessazione delle motivazioni del rilascio (ad esempio cessazione rapporto di lavoro per utente interno)
- Il QTSP termina la propria attività di QTSP;
- La legge in vigore richiede obbligatoriamente la revoca.

Il numero di cellulare fornito dal sottoscrittore in fase di richiesta/registrazione della anagrafica deve rimanere invariato durante tutto il periodo di validità del certificato, in quanto utilizzato come strumento di comunicazione del secondo fattore di autenticazione generato dal QTSP, ed inviato al momento della operazione di firma qualificata.

Al verificarsi di tale evento (il cambio di numero cellulare), il sottoscrittore è tenuto a darne comunicazione al QTSP al fine di procedere con le variazioni anagrafiche del caso, anche tramite funzione di revoca accessibile da link preposto sul **Piattaforma del QTSP**.

La mancata comunicazione della variazione, in virtù della perdita del controllo sul secondo fattore di autenticazione, consente al QTSP di rendere applicabile quanto previsto per la revoca del certificato.

4.8.2 Sottomissione della richiesta di revoca

La richiesta di revoca può essere richiesta da:

- Il sottoscrittore;
- Il legale rappresentante del sottoscrittore;
- Il QTSP.

4.8.3 Processo per la richiesta della revoca

Il QTSP fornisce uno strumento di revoca del certificato, attraverso la relativa funzione *Revoca del certificato* accessibile, previa autenticazione, sul **Piattaforma del QTSP**.

La procedura per la richiesta di revoca prevede che:

- Il Titolare del Certificato acceda al Piattaforma del QTSP, attraverso le proprie credenziali generate al momento del rilascio del certificato;
- Il Titolare accede alla sezione di Revoca, e compila il form preposto;
- Il Titolare visualizza i dati relativi all'operazione di revoca, e ne conferma l'operazione sottomettendo la richiesta;
- Il Titolare, in caso di revoca del certificato per l'utilizzo dei servizi di Firma Digitale, se in possesso di dispositivi Token fisici per la generazione di codici OTP deve provvedere alla restituzione degli stessi presso le sedi del QTSP dislocate su tutto il territorio nazionale. Il QTSP provvederà ad attuare l'iter interno per procedere alla revoca del certificato e alla riconsegna del dispositivo;
- Il sistema sottomette la richiesta alla CA e, non appena evasa, invia un'e-mail di conferma al Titolare.

La procedura di revoca può essere sottomessa anche da personale preposto dal QTSP, previa autenticazione, sulla **Piattaforma del QTSP**, secondo le circostanze definite in 4.8.1.

Il QTSP prende in lavorazione automaticamente tutte le richieste ricevute, processandole entro un tempo massimo di 24 ore.

In caso di smarrimento del Token (se assegnati):

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Il Titolare segnala l'evento al QTSP alla casella di posta **firmaqualificata@pec.lottomatica.it** → dal **01 Marzo 2021** l'indirizzo di riferimento sarà **caigt@pec.it**;
- Il QTSP verifica l'identità del titolare attraverso la Registration Authority (RAA, Master-RAO, RAO);
- Il QTSP procede alla disabilitazione del Token fisico del Titolare e provvede ad associare allo stesso un nuovo metodo di generazione del codice OTP (metodo via SMS) per garantire la continuità del servizio offerto.

4.8.4 Grace Period richiesta di revoca

Il "grace period" associato alla verifica sulla validità del certificato, è pari al valore massimo previsto per l'aggiornamento della CRL, ed è pari a 4 ore (vedi cap. 4.8.7).

4.8.5 Tempo entro il quale la CA deve processare la richiesta di revoca

Il QTSP deve elaborare le richieste di revoca in conformità con lo standard ETSI 319 411-1 v.1.2.2 Clausola 6.2.4 [3].

4.8.6 Requisiti sul controllo della revoca da parte delle parti interessate

Al fine di ottemperare al controllo sulla revoca, viene raccomandato di verificare tutti i certificati inclusi nella catena di certificazione. La verifica deve includere il controllo sulla validità dei certificati, le policy contenute nel certificato unitamente al key usage, il controllo sullo stato dei certificati sulla base delle informazioni contenute nella CRL o nell'OCSP.

4.8.7 Frequenza emissione della CRL

La frequenza di pubblicazione della CRL è di 4 ore con validità di 24 ore.

4.8.8 Massima latenza sulla CRL

La latenza massima legata alla pubblicazione della CRL è di 5 minuti.

4.8.9 Disponibilità del servizio OCSP

Il QTSP fornisce un servizio OCSP per la validazione del certificato. Il servizio è disponibile sulla base di quanto specificato in 4.9.2.

4.8.10 Requisiti servizio OCSP

Il servizio OCSP del QTSP è compatibile con i requisiti specificati nel cap. 4.9. Il servizio OCSP è interrogabile tramite metodo HTTP GET.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

4.8.11 Requisiti particolari sulla compromissione della chiave

In caso di compromissione della chiave privata, il QTSP pubblica il cambio di stato del certificato e ne notifica l'evento alle parti interessate.

Nel caso di compromissione della chiave privata di un end-user, il QTSP revoca il certificato specificando come reasonCode il valore "keyCompromise (1)".

4.9 SERVIZI PER LA VERIFICA DELLO STATO DEL CERTIFICATO

Il QTSP, al fine di accertare la validità di un certificato, fornisce i seguenti servizi:

- OCSP – Online Certificate Revocation Status;
- CRL – Certificate Revocation Lists.

I certificati revocati sono inclusi nella CRL.

I certificati revocati non possono essere cancellati dalla CRL, anche dopo la scadenza.

In caso di cambio di stato (attivo, sospeso, revocato), al completamento del processo, il QTSP aggiorna istantaneamente la CRL la quale viene successivamente pubblicata in accordo con i tempi di frequenza e massima latenza specificati nei cap. 4.8.7 e 4.8.8. Da quel momento, il servizio OCSP fornisce informazioni circa il nuovo stato del certificato.

Il servizio OCSP contiene il valore "UNKNOWN" nel caso in cui il certificato non sia presente nella lista di revoca, o non sia stato emesso dal QTSP.

Il QTSP pubblica altresì un portale (verificatore online) per la convalida di un documento sottoscritto con firma digitale, disponibile pubblicamente al seguente URL:
<https://ver.ca.firmadigitale.lottomaticaitalia.it>

L'utente che necessita di verificare la validità della firma elettronica qualificata di un documento, accede al servizio sopra indicato ed effettua il caricamento (o upload) del file. Il servizio restituisce l'esito della verifica di validità.

Il verificatore online è una componente web-based implementata in linguaggio Java, basato sul progetto DSS raccomandato dalla Commissione Europea per il pieno riconoscimento dei documenti informatici sottoscritti nei diversi Stati Membri.

4.9.1 Caratteristiche operazionali

La CA del QTSP aggiorna la lista di revoca compatibilmente con quanto specificato in 4.8.7.

Per ragioni operative, la CRL può avere una validità che supera la validità predefinita specificata nel presente CPS (vedi cap. 4.8.7); tale valore non deve in ogni caso superare le 24 ore.

Il servizio OCSP è aggiornato sulla base delle policy di pubblicazione legate all'aggiornamento della CRL.

La CRL è disponibile al seguente URL:

<https://ca.firmadigitale.lottomaticaitalia.it/qtspcacr1h2020.crl>

4.9.2 Disponibilità del servizio

L'accesso alla CRL e al servizio OCSP è disponibile in modo continuo 24 ore su 24.

Il QTSP deve assicurare la disponibilità della CRL pubblicata e dei termini e condizioni dei certificati rilasciati al 99,7% su base annua, garantendo che l'indisponibilità non programmata del sistema non superi le 8 ore.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Il QTSP deve assicurare la disponibilità dei servizi connessi con la verifica della revoca dei certificati rilasciati, al 99,7% su base annua, garantendo che l'indisponibilità del servizio non superi le 8 ore.

4.10 FINE DELLA SOTTOSCRIZIONE

Il QTSP revoca il certificato del sottoscrittore nel caso di scadenza degli accordi contrattuali con il titolare o laddove siano verificate le condizioni del cap. 4.8.1

4.11 KEY ESCROW E RECOVERY

Il QTSP non fornisce strumenti di key escrow applicati alla chiave privata appartenente ad un sottoscrittore.

4.11.1 Policy e Pratiche Key Escrow e Recovery

Il QTSP non fornisce strumenti di key escrow applicati alla chiave privata appartenente ad un sottoscrittore.

4.11.2 Incapsulamento chiave Cifratura simmetrica Politiche di Recovery

Il QTSP non fornisce strumenti di key escrow applicati alla chiave privata appartenente ad un sottoscrittore.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

5 FACILITY, MANAGEMENT, E CONTROLLI OPERATIVI

5.1 CONTROLLI FISICI

Il QTSP adotta un insieme di misure tecniche ed organizzative che permettono il controllo degli accessi alle sedi e la salvaguardia dei beni aziendali da furti/sparizioni e/o danneggiamenti volontari ed involontari. La definizione delle politiche di sicurezza fisica si inserisce all'interno di un più ampio processo che ha come obiettivo la protezione dei supporti informativi e che ha come presupposto un'attività di risk assessment che individui i rischi associati ai beni censiti.

5.1.1 Locazione del sito e Caratteristiche

I sistemi CED relativi agli ambienti di produzione, sono in esecuzione su un'infrastruttura HW dislocata su due siti distinti:

- Il Sito A è ubicato in Roma, viale del campo Boario, 56d; i sistemi sono ubicati all'interno di una cage dedicata;
- Il Sito B è ubicato in Roma, via dello Scalo Prenestino, 15 all'interno del Data Center di AlmaViva; all'interno del quale Lottomatica Holding S.r.l. ha una sala macchine ad uso esclusivo, i sistemi sono quindi ubicati all'interno di una cage dedicata.

I Data Center sono interconnessi da una rete *backbone* privata ed entrambi connessi alle reti di accesso internet con capacità di banda tali da fornire i servizi qualificati con le stesse prestazioni. L'interconnessione dei singoli DC sia verso la rete pubblica che quella privata è implementata attraverso connessioni ridondate. Tale infrastruttura garantisce il rispetto degli indicatori descritti nel cap. 4.9.2.

L'area del CED del sito A è realizzata con adeguati criteri costruttivi. Gli ambienti che ospitano gli apparati sono provvisti di contro-pavimenti e contro-soffitti (Sito B), nel rispetto delle norme e degli *standard* di riferimento. Le infrastrutture sono tutte realizzate con l'utilizzo di materiali incombustibili.

Nella sala di elaborazione è presente un sistema di illuminazione conforme alle normative, e corredato da un adeguato sistema di emergenza.

5.1.2 Accessi fisici

Sito A

L'edificio e le aree sicure di Lottomatica Holding S.r.l. sono protette da un sistema di controllo degli accessi al fine di garantire l'ingresso al solo personale autorizzato.

Lottomatica Holding S.r.l. definisce procedure di security policy interne che regolano l'accesso fisico alla sede ed alle aree riservate sia per i dipendenti che per i visitatori occasionali o abituali.

In particolare, sono previste una serie di norme comportamentali di seguito riportate:

È obbligatorio:

- Accedere al luogo di lavoro utilizzando le proprie credenziali di accesso (es.: badge magnetico) dai varchi predisposti e con le modalità stabilite dall'azienda;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Attenersi alle norme di volta in volta impartite per iscritto o verbalmente dai responsabili sull'accesso alle aree riservate;
- Rispettare le procedure aziendali per la richiesta di accesso a personale esterno (consulenti, visitatori abituali e occasionali);
- Comunicare tempestivamente eventuali violazioni alle norme al proprio Responsabile, alla vigilanza della sede o direttamente all'Area Security.

È vietato:

- Cedere a terzi le proprie credenziali di accesso, anche temporaneamente, e nel caso ne venga meno il possesso deve esserne data tempestiva comunicazione all'Area Security;
- Accedere alle aree riservate se non in possesso di specifica autorizzazione.

Relativamente al controllo degli accessi fisici, Lottomatica Holding S.r.l. ha implementato seguenti controlli:

- L'accesso è consentito soltanto ai possessori di badge non scaduto rilasciato dall'Area Security;
- Il badge viene assegnato ai dipendenti ed ai visitatori, previa identificazione ed autorizzazione di un referente interno a Lottomatica Holding S.r.l.;
- Il rilascio del badge è coerente con il profilo aziendale del dipendente e consente l'accesso solamente alle aree di stretta competenza dello stesso;
- In qualsiasi momento gli addetti alla vigilanza possono effettuare verifiche sulla validità del badge e quindi, se da loro richiesto, deve essere prontamente esibito;
- Gli eventi di accesso (entrata e uscita) sono registrati.

Sito B

L'edificio e le aree sicure del sito B sono protette da un sistema di controllo degli accessi al fine di garantire l'ingresso al solo personale autorizzato.

L'intero perimetro esterno del Data Center, completamente recintato, è illuminato in orario notturno e costantemente sorvegliato da un sistema TVCC costituito da telecamere fisse e DOM, tutte portate ad un sistema di schermi installato nella sala regia della Vigilanza e sorvegliato H24x7. Le immagini sono registrate su un dispositivo digitale per controlli e verifiche ex post.

5.1.3 Alimentazione ed Aria condizionata

Sito A

Tutti gli ambienti del CED sono adeguatamente climatizzati attraverso sistemi dedicati. Come già accennato, l'impianto di condizionamento dell'area CED è a espansione diretta. Ogni unità è a sua volta costituita da due circuiti separati. La modularità, insieme alla riserva di potenza totale, consente di far fronte ai fermi per manutenzione programmata e ai guasti temporanei.

Le procedure interne garantiscono un'adeguata manutenzione dei sistemi.

L'alimentazione elettrica è fornita dalla rete di distribuzione a media tensione mediante doppio collegamento ad anello. La cabina di consegna di media tensione è fisicamente separata dalla cabina che ospita i due trasformatori, posti in configurazione ridondata.

Il sito A dispone anche di gruppi di continuità in grado di sopperire a temporanee esigenze sulla erogazione

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

della alimentazione.

Tutti gli allarmi provenienti dai sistemi rilevanti per la continuità di servizio del CED (tra cui alimentazione elettrica, condizionamento, antincendio, antiallagamento) sono gestiti da un sistema di supervisione.

Sito B

Tutte le sale di elaborazione del Data Center sono climatizzate mediante utilizzo di condizionatori di precisione ad acqua refrigerata.

La potenza refrigerante è prodotta da due gruppi frigoriferi in configurazione *active-standby* situati in zone distanti.

Tutti gli allarmi provenienti dai sistemi rilevanti per la continuità di servizio del CED (tra cui alimentazione elettrica, condizionamento, antincendio, antiallagamento) sono gestiti da un sistema di supervisione.

5.1.4 Esposizione all'acqua

Sito A

Il CED è mantenuto a livelli di temperatura e umidità che impediscono la formazione di condensa. Oltre al sistema di condensa e di adduzione di acqua agli umidificatori dell'impianto di condizionamento è presente l'impianto di raffreddamento della cage. Questi tre sistemi sono dotati di appositi accorgimenti al fine di evitare perdite di acqua. Per ogni evenienza è installato un sistema di allarme che segnala e localizza eventuali improbabili versamenti di acqua al di sotto del pavimento rialzato, permettendo al personale di controllo di verificarne le cause ed eliminarle.

Sito B

La sala di elaborazione in prossimità delle terminazioni di distribuzione del fluido refrigerante che serve i condizionatori è attrezzata con sensori di rilevazione di acqua che riportano al sistema di monitoraggio degli impianti, presidiato 24x7x365.

5.1.5 Prevenzione e protezione antincendio

Sito A

La sede in cui si trova il CED è dotata di sistemi di protezione antincendio a norma di legge. Il sistema di antincendio del CED è costituito da un impianto di rilevazione fumi e spegnimento incendio a gas FM200. Il sistema può funzionare sia in maniera automatica che manuale. I sensori del sistema di rilevazione sono inseriti sia a soffitto che al di sotto del pavimento tecnico con gemme di ripetizione dello stato di funzionamento del singolo sensore.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Sito B

Il CED è dotato di un sistema centralizzato di rilevazione dei fumi, facente capo alla sala controllo della Vigilanza presidiata.

Le sale di elaborazione e i locali degli impianti tecnologici hanno il sistema centralizzato di rilevazione dei fumi esteso anche allo spazio sotto il pavimento flottante e sono dotati di sistemi automatici di estinzione a gas nel controsoffitto, in ambiente e sotto il pavimento flottante, asserviti al sistema di rilevazione e compartimentati in modo da confinare le aree di attivazione.

L'attivazione del sistema di estinzione è automatica, e comandata da centraline asservite al sistema di rilevazione.

5.1.6 Media Storage

Le attività di media storage sono definite all'interno di procedure interne di sicurezza.

5.1.7 Disposizioni sulla dismissione di apparati

A seguito di valutazioni interne o segnalazioni relative a guasti, obsolescenza o necessità di manutenzione di hardware e/o supporti media, il personale tecnico addetto identifica gli asset da verificare.

Qualora l'hardware o supporto media risulti funzionante e riutilizzabile si può procedere alla cancellazione delle informazioni in esso presenti, avvalendosi anche di opportuni prodotti che effettuano lo shredding dei dati o formattazioni a basso livello ed al riutilizzo dell'hardware o supporto media secondo necessità.

Qualora risulti impossibile ripristinare il corretto funzionamento dell'hardware o del supporto media si procede con l'eliminazione sicura dei dati in esso contenuti tramite distruzione fisica (CD,DVD resi illeggibili con incisioni profonde, taglio dei nastri dat) o profonda alterazione dell'hardware e con la successiva richiesta di dismissione del bene presso strutture interne deputate in osservanza delle procedure interne sulla dismissione beni aziendali.

5.1.8 Off-Site Backup

Le attività di backup sono definite all'interno di procedure interne di sicurezza.

5.2 CONTROLLI PROCEDURALI

Il QTSP applica processi interni finalizzati affinché i suoi sistemi siano gestiti in modo sicuro.

Precauzioni procedurali hanno l'obiettivo di integrare l'efficacia delle misure di sicurezza fisiche, insieme a quelle che si applicano al personale, mediante la nomina e l'identificazione di ruoli (non ambigui) di fiducia, ed all'applicazione informatica dei meccanismi di identificazione e autenticazione connessi.

Il QTSP garantisce che il suo funzionamento è conforme alle leggi in vigore ed ai suoi regolamenti interni.

5.2.1 Ruoli

Nell'esercizio delle proprie funzioni, il QTSP crea ruoli riconosciuti, a cui sono applicati meccanismi di autorizzazione commisurati alle responsabilità connesse.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

In osservanza del DPCM 22 febbraio 2013 [24], art. 38, il QTSP ha definito la struttura organizzativa che presidia i principali Ruoli definiti per la gestione dei servizi di firma digitale qualificata e marcatura temporale che prevede l'esistenza delle seguenti figure:

- Responsabile del servizio di certificazione e validazione temporale;
- Responsabile della Registration Authority (Registration Authority Manager);
- Responsabile della sicurezza;
- Responsabile delle verifiche e delle ispezioni (auditing);
- Responsabile della conduzione tecnica dei sistemi;
- Responsabile servizi tecnici e logistici;
- Responsabile servizi tecnici di validazione temporale.

5.2.2 Numero di persone richieste per task

Il QTSP assicura la contemporanea presenza di almeno 2 persone, con ruoli appositamente approvati, durante lo svolgimento delle seguenti operazioni critiche di sicurezza:

- La generazione della chiave privata della CA del QTSP;
- Il backup della chiave privata della CA del QTSP;
- L'attivazione della chiave privata della CA del QTSP;
- La distruzione della chiave privata della CA del QTSP.

Almeno una delle persone presenti, deve ricoprire un ruolo amministrativo.

Le operazioni sopra menzionate, devono avvenire alla sola presenza delle persone appositamente autorizzate.

5.2.3 Identificazione ed Autenticazione per Ruoli

Gli utenti che gestiscono i servizi IT del QTSP hanno una identificazione univoca e personale.

Gli utenti possono esclusivamente avere accesso ai sistemi critici, esclusivamente dopo l'identificazione e l'autenticazione.

Le autorizzazioni di accesso sono immediatamente revocate, nel caso di cessazione di incarico da parte dell'utente.

Ogni utilizzo dei sistemi IT ed ogni attore che gestisce i processi, è identificato individualmente.

L'accesso fisico agli ambienti dove sono collocati i sistemi è protetto compatibilmente con quanto specificato in 5.1.2.

L'accesso logico è controllato da un sistema interno di monitoraggio, per la tracciatura degli accessi e la notifica di non conformità.

5.2.4 Ruoli che richiedono segregazione

Il QTSP applica quanto previsto nel DPCM 22 febbraio 2013 [24], art. 38 comma 3 e 4.

In questo ambito:

- Responsabile della sicurezza non può assumere altri ruoli fra quelli definiti in 5.2.1;
- Il Responsabile delle verifiche e delle ispezioni (auditing) non può assumere altri ruoli fra quelli definiti in 5.2.1.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

5.3 CONTROLLO DEL PERSONALE

Lottomatica Holding S.r.l. definisce ed applica criteri e modalità attraverso cui:

- Tenere in considerazione gli aspetti connessi alla sicurezza delle informazioni nel processo di gestione delle risorse umane;
- Migliorare la sensibilità e i livelli di consapevolezza del personale circa le problematiche di sicurezza delle informazioni.

Tali criteri e modalità si applica alle attività di selezione, inserimento in azienda, formazione del personale e cessazione del rapporto di lavoro.

5.3.1 Qualifiche, esperienze e chiarezza dei requisiti

Nell'ambito di applicazione sui processi di selezione, formazione e gestione risorse umane, Lottomatica Holding S.r.l. assicura:

- Che tutto il personale possieda le necessarie competenze, affidabilità, esperienza e qualifiche e che abbia ricevuto adeguata formazione in materia di sicurezza e di norme sulla protezione dei dati personali, a seconda della funzione svolta;
- Che, ove possibile, il personale soddisfi requisiti di esperienza e qualifica tramite titoli di studio, corsi di formazione e/o dimostrata esperienza;
- Che ai pertinenti livelli dell'organizzazione siano resi disponibili a cadenza almeno annuale aggiornamenti su eventuali nuove minacce, metodologie e strumenti a tutela della sicurezza.

5.3.2 Procedure di verifica di Background

Nell'ambito dell'attività di *recruiting* i selezionatori prestano attenzione, oltre alla potenziale compatibilità dei candidati con le esigenze professionali di Lottomatica Holding S.r.l., agli elementi rilevanti in termini di sicurezza, quali:

- La durata delle precedenti esperienze professionali e i motivi portati a giustificazione della conclusione del rapporto;
- Il settore di attività e le imprese all'interno delle quali sono state condotte le precedenti attività professionali (con particolare attenzione a quelle che possono essere considerate fornitrici, clienti o, eventualmente, concorrenti);
- In caso di lavoratore extracomunitario, copia del permesso di soggiorno in corso di validità, ovvero, qualora questo sia scaduto, copia della richiesta di rinnovo formulata nei termini di legge.

5.3.3 Requisiti di formazione

Lottomatica Holding S.r.l. si fa carico di attuare tra il personale dipendente, un opportuno piano formativo mirato al miglioramento dei processi legati alla attività del QTSP.

Pur nel rispetto di quelle che possono essere le esigenze contingenti che portano a pianificare un corso di formazione, gli obiettivi comuni a tutti i corsi sono:

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Incrementare il livello di consapevolezza circa le problematiche di sicurezza connesse con l'attività del QTSP;
- Rendere il personale consapevole delle politiche e delle linee guida dell'Azienda, dei ruoli e delle responsabilità aziendali per la sicurezza.

Lottomatica Holding S.r.l. svolge l'attività di formazione nel rispetto dei seguenti requisiti:

- Il personale incaricato della preparazione ed erogazione della formazione deve possedere le necessarie qualifiche ed esperienze in termini di formazione aziendale;
- Gli incaricati Master-RAO/RAO ricevono il manuale formativo e l'adeguata formazione per svolgere correttamente le attività di identificazione e registrazione dei Clienti e svolgono la verifica dell'efficacia della formazione;
- Ove ritenuto necessario, l'attività formativa può essere estesa anche a fornitori e collaboratori;
- Deve essere garantita la programmazione e l'erogazione di tutti i corsi previsti dalle normative applicabili all'attività dell'Azienda;
- Si deve assicurare la conoscenza della normativa vigente in materia di Servizi Fiduciari Qualificati, nonché di best practices e standard;
- La definizione di piani di formazione in materia di Servizi Fiduciari Qualificati deve essere conforme a quanto previsto dal Regolamento EU n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali [25]

5.3.4 Frequenza di aggiornamento

Lottomatica Holding S.r.l. programma l'attività di formazione con cadenza periodica, sulla base dei risultati di test dei partecipanti ai corsi e/o sulla base delle esigenze interne.

5.3.5 Sanzioni su azioni non autorizzate

In relazione alle sanzioni previste in caso di comportamento difforme rispetto a quanto richiesto dalla società nei documenti afferenti la sicurezza (Istruzioni di lavoro, policy, procedure ecc.), Lottomatica Holding S.r.l. farà riferimento al sistema sanzionatorio previsto dal CCNL.

5.3.6 Requisiti su consulenti

Gli aspetti connessi con il controllo del Personale appartenente all'area consulenti e collaboratori esterni, è disciplinato da procedure aziendali interne, che definiscono i criteri ed i processi per l'identificazione di norme e requisiti che Lottomatica Holding S.r.l. considera rilevanti nell'ambito dell'approvvigionamento e della stipula dei contratti con Terze Parti, tenendo conto delle caratteristiche della relazione che Lottomatica Holding S.r.l. instaura con le stesse.

5.3.7 Documentazione fornita al personale

Nel momento in cui un candidato viene selezionato e inserito nell'organico di Lottomatica Holding S.r.l., l'area Human Resources Management garantisce:

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Lettera di assunzione;
- Eventuale lettera di distacco c/o altre società di Lottomatica Holding S.r.l.;
- Informativa sul trattamento dati personali raccolti (Ctrl.2);
- Informativa ai lavoratori in merito alla salute e sicurezza sul lavoro;
- Codice di condotta;
- Norme comportamentali per la gestione sicura dei beni aziendali.

Il "Codice di condotta", nello specifico, include:

- I riferimenti a tutte le norme a cui si è aderito e quali violazioni o infrazioni del Codice potrebbero comportare un'azione disciplinare;
- Indicazioni secondo cui agli impiegati è richiesto di dichiarare qualsiasi conflitto di interesse con il lavoro che svolgono, non appena questo si verifichi;
- Specifici esempi di conflitto di interesse;
- Indicazioni relative a ospitalità/donazioni/regali forniti dalle Terze Parti con le quali Lottomatica Holding S.r.l. intrattiene rapporti contrattuali ed economici.

5.4 PROCEDURE DI AUDIT

Il QTSP adotta strumenti IT che assicurano la raccolta degli eventi connessi con l'attività di Certificazione.

5.4.1 Tipologie di eventi memorizzati

Il QTSP, attraverso strumenti specializzati, attua una azione di monitoraggio degli eventi associati alla attività del QTSP, in conformità di quanto specificato nel cap. 6.4.5 dello standard EN 319 411 2 v2.1.1 [4].

5.4.2 Frequenza dei processi di Audit

Audit tecnico

Lottomatica Holding S.r.l. attiva i processi di test e verifiche tecniche di sicurezza a fronte delle seguenti casistiche:

- Nuovi rilasci;
- Pianificazione periodica;
- Richieste o eventi specifici.

La tipologia di tali test e verifiche dipende dalla casistica che attiva il processo

Audit di sistema

Tutte le strutture aziendali interessate dalle attività di QTSP sono oggetto di verifica ispettiva almeno una volta l'anno relativamente alle attività prescritte dal Sistema di Gestione per la Sicurezza delle Informazioni. La frequenza delle verifiche è definita in funzione:

- Dell'importanza e/o della criticità delle attività svolte dalle singole strutture;
- Dei risultati di precedenti verifiche ispettive;
- Di eventuali modifiche significative dell'organizzazione aziendale e/o delle attività svolte.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

5.4.3 Periodo di retention dei log di Audit

Il periodo di retention dei log di Audit è di 20 anni, in accordo con il DPCM 22 febbraio 2013 [24].

5.4.4 Protezione dei log di audit

La protezione dei log di Audit deve garantire:

- Protezione: solo personale autorizzato può accedere agli eventi conservati;
- Disponibilità: gli eventi sono conservati in maniera da poterne verificare il contenuto e l'integrità nel tempo, prevenendo la corruzione del dato;
- Integrità: il dato è conservato al fine di impedire l'alterabilità del dato.

La protezione dei log di Audit è in accordo con quanto specificato nel cap. 7.10 dello standard EN 319 401 v 2.1.1 [1].

5.4.5 Procedure di backup log di Audit

Le procedure di backup dei sistemi di log management assicurano la memorizzazione dei log in conformità a quanto specificato nel cap. 5.4.3.

5.4.6 Sistemi di raccolta eventi di Audit

Il QTSP adotta sistemi automatizzati che assicurano l'attività di raccolta su base continua. Ogni sistema IT coinvolto, colleziona e spedisce gli eventi al sistema di log.

5.4.7 Notifica in caso di identificazione di eventi sospetti -

Il QTSP adotta procedure interne di comunicazione, a seguito del rilevamento di un messaggio di errore nel sistema.

5.4.8 Vulnerability Assessment

L'attività di Vulnerability Assessment consiste nel valutare il livello e l'efficacia della sicurezza del sistema ICT attraverso scansioni automatiche finalizzate a individuare vulnerabilità note dei sistemi ICT relativamente alle componenti di sistema operativo ed al software di *middleware* (es. Application Server) ed Infrastrutturale (es. monitoraggio del sistema) ivi residente. Tale attività è realizzata attraverso l'utilizzo di strumenti automatici specifici che, a partire da un determinato insieme di test (*Baseline/Template*):

- Conducono le verifiche tecniche relative alle vulnerabilità note¹ dei sistemi ICT;
- Producono report in cui sono dettagliati gli esiti dei test e le vulnerabilità rilevate.

¹ Periodicamente aggiornate mediante servizi di update automatici erogati dai fornitori degli strumenti di scansione.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Considerando l'intero insieme di test tecnici che lo specifico strumento automatico di scansione può operare, vengono definiti e adottati particolari sottoinsiemi di queste verifiche tecniche, denominati appunto *baseline/template*, che risultano adatti e applicabili alla tipologia di sistemi *target* da verificare.

Lottomatica Holding S.r.l. attiva i processi di VA a fronte delle seguenti casistiche:

- Nuovi rilasci;
- Pianificazione periodica (almeno 1 volta per quarter per sito A e B);
- Richieste o eventi specifici.

Sono inoltre svolte con cadenza almeno annuale le attività di Penetration Test.

5.5 ARCHIVIAZIONE DEI RECORD

L'archiviazione dei record è conforme con quanto specificato nel cap. 7.10 dello standard EN 319 401 v 2.1.1 [1]. Il periodo di retention applicato è conforme a quanto specificato nel cap. 5.4.3.

5.6 CA KEY CHANGEOVER

Al fine di garantire la propria operatività, il QTSP assicura che il rinnovo del proprio certificato sia effettuato sufficiente tempo prima della scadenza dello stesso.

Il QTSP assicura che in caso di rinnovo, una nuova coppia di chiavi viene generata in accordo con i regolamenti vigenti.

Si specifica inoltre che:

- Il nuovo certificato viene pubblicato nel repository pubblico dei certificati, in aderenza con quanto specificato nel presente documento nel capitolo 6.1.4;
- I nuovi certificati di sottoscrizione degli utenti, siano emessi utilizzando il nuovo certificato rinnovato;
- Che le vecchie chiavi ed il relativo certificato sono conservati a termini di legge.

5.7 COMPROMISSIONE E DISASTER RECOVERY

In caso di un disastro, il QTSP adotta tutte le misure necessarie al fine di ridurre al minimo il danno derivante dalla carenza del servizio, ripristinando i servizi entro i tempi dichiarati nel presente CPS, in coerenza con le procedure di Business Continuity interne al QTSP stesso.

Il Recovery Point Objective (RPO) deve consentire una perdita limitata di dati, commisurata con gli obiettivi di business. L'RPO fissato per la presente infrastruttura, è di 5 minuti.

Sulla base della valutazione dell'incidente, il QTSP adotta tutte le misure correttive per evitare in futuro il verificarsi dell'incidente.

Il QTSP adotta un piano interno per la sicurezza volto ad assicurare che test di DR vengano svolti con regolarità, assicurando che le osservazioni derivanti da problemi tecnici o non conformità connesse con la riattivazione dei servizi, siano oggetto di revisione e miglioramento del suddetto piano.

Il QTSP indirizza la risoluzione di ogni vulnerabilità considerata critica entro 48 ore dalla sua scoperta, tramite un opportuno piano di rientro.

Il QTSP prevede, all'interno di procedure interne per la gestione degli incidenti e l'attuazione di un piano d'emergenza nel caso si rilevi una violazione della sicurezza o una perdita dell'integrità dei dati con un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi ("data breach"). In particolare, in coerenza con l'articolo 19 del Regolamento eIDAS [27] gli incidenti di sicurezza sono classificati con 5 livelli di severità (in linea con le Linee Guida Enisa):

1. Nessun impatto;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

2. Impatto non significativo (impatto sugli asset ma non sui servizi core);
3. Impatto significativo (impatto su una parte della clientela);
4. Impatto grave (impatto su una larga parte della clientela);
5. Disastroso (impatto sull'intera organizzazione e su tutti i certificati emessi).

Tale piano d'emergenza permette di limitare l'impatto della violazione di sicurezza e di notificare:

- Alle parti interessate (AgID, il Garante Privacy e i titolari) entro 24 ore dalla rilevazione della violazione, in caso di incidenti di sicurezza classificati con un livello di severità 3, 4 e 5 ed entro 5 giorni per quelli di severità 1 e 2.

5.7.1 Incident e procedure di gestione della compromissione

Il QTSP ha un Business Continuity Plan (BCP) che adotta in caso di incident e gestione della compromissione.

Il QTSP adotta criteri prevenzione, attuando sistemi di progettazione volti ad impedire il single point of failure, assicurando nel contempo la continuità operativa dei siti, anche in situazioni di fault di un sistema o di un apparato.

5.7.2 Computing Resources, Software, e/o dati corrotti

Il QTSP adotta criteri di progettazione di sistema ridondanti in modo da evitare la perdita di servizio in caso di single point of failure.

Il QTSP adotta e mantiene medesimi sistemi HW/SW tra sito A e sito di B, in maniera da evitare problemi nel restore dei dati dei servizi fra i siti.

Il QTSP adotta politiche di backup volte ad assicurare l'RPO dichiarato nel presente documento. Le attività di backup sono eseguite dal personale autorizzato ("system operators"), in coerenza con la clausola 6.4.8 dello standard ETSI EN 319411-1.

5.7.3 Procedure di compromissione chiave privata

Il QTSP prevede l'attuazione di un piano d'emergenza nel caso nel quale si verifichi la compromissione delle chiavi. Tale piano d'emergenza rivela le circostanze di compromissione e prevede:

- La notifica di tutte le parti interessate;
- Qualora necessario, revoca il certificato compromesso e ne genera uno nuovo con nuove chiavi associate al servizio.

5.7.4 Capacità di Business Continuity in caso di disastro

I compiti da eseguire in caso di disastro sono definiti nel piano di Business Continuity del QTSP.

5.8 CESSAZIONE DELLA ATTIVITÀ

La cessazione dell'attività del QTSP è conforme a quanto specificato nel Codice dell'Amministrazione digitale, pubblicato con D.Lgs. Del 7 marzo 2005, n.82 ed aggiornato con il D.Lgs 179/2016.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

6 CONTROLLI TECNICI DI SICUREZZA

Il QTSP utilizza sistemi predisposti con criteri di alta affidabilità applicati al singolo elemento, o connessi con il servizio erogato. I sistemi prevedono protezioni sulla gestione delle chiavi crittografiche, e sui dati di attivazione per l'intero ciclo di vita degli stessi. In particolare, il QTSP utilizza HSM per la gestione del ciclo di vita delle chiavi, ed assicura che le stesse siano trattate in conformità con i manuali di gestione forniti dal vendor, ed in conformità dei traguardi di certificazione sotto il quale sono configurati ed operano gli apparati.

I controlli tecnici di sicurezza applicati ai sistemi IT coinvolti nei processi interni al QTSP, prevedono una copertura di certificazione conforme allo standard ISO 27001.

La capacità dei sistemi è connessa con la domanda, ed è monitorata su base continua. La crescita è stimata così da assicurare la disponibilità dei sistemi e dei supporti di memorizzazione.

6.1 GENERAZIONE ED INSTALLAZIONE COPPIA DI CHIAVI

Il QTSP assicura che la produzione e la gestione delle chiavi private sia conforme agli standard previsti dalle norme in vigore.

In particolare, il QTSP utilizza HSM per la gestione del ciclo di vita delle chiavi, ed assicura che le stesse siano trattate in conformità con i manuali di gestione forniti dal vendor, ed in conformità del traguardo di certificazione sotto il quale sono configurati ed operano gli apparati.

6.1.1 Generazione coppia di chiavi

Il QTSP è responsabile sulla generazione delle seguenti tipologie di chiavi:

1. Chiavi di certificazione, associate al servizio di CA;
2. Chiavi di sottoscrizione, destinate ai Titolari.

Tutte le chiavi sono generate attraverso un dispositivo di tipo HSM, conforme agli standard di certificazione riportati nel cap. 6.2.1 e in stretta osservanza di quanto specificato nei rispettivi traguardi di sicurezza.

Il QTSP conferma che il processo di generazione delle chiavi della CA e di quello dei titolari, viene eseguito conformemente alle regole tecniche rispetto a quanto vigente, come specificato nello standard EN 319 411 01 v1.2.2, con particolare riferimento ai capitoli 6.5.1, 6.5.2 e 6.5.3.

Il processo di generazione delle chiavi della CA è conforme con quanto specificato nello standard EN 319 411 01 v1.2.2, con particolare riferimento ai capitoli 6.5.1, 6.5.2 e 6.5.3.

6.1.2 Rilascio della chiave privata ai sottoscrittori

Nel contesto di un servizio di Firma remota qualificata, il rilascio della chiave privata di sottoscrizione consiste nel rilascio delle credenziali per l'uso della stessa.

Il QTSP garantisce che le credenziali connesse con lo sblocco della chiave privata, siano rilasciate in maniera sicura solo ed esclusivamente al titolare sottoscrittore.

6.1.3 Rilascio della chiave pubblica al QTSP

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Le chiavi del QTSP vengono generate all'atto della inizializzazione del sistema (Key Ceremony). La generazione delle chiavi e della richiesta di Certificato, vengono gestite direttamente dal sistema di CA, attraverso le modalità specificate nei manuali di prodotto.

6.1.4 Rilascio della chiave pubblica di CA alle parti interessate

Compatibilmente con quanto specificato nel cap. 2.2, il QTSP rende disponibile il certificato contenente la chiave pubblica sul proprio **Piattaforma del QTSP**.

In osservanza di quanto contenuto al punto h dell'allegato I del Regolamento europeo 910/2014 [27], il link di pubblicazione di tale certificato è inserito anche all'interno dei certificati di sottoscrizione emessi dal QTSP (vedi cap. 7.1.2).

6.1.5 Lunghezza chiavi

Il QTSP utilizza algoritmi e policy sulla lunghezza chiave secondo quanto specificato nello standard ETSI TS 119 312.

In particolare:

- La chiave RSA di root CA è di lunghezza 4096 bit.

6.1.6 Parametri di generazione chiavi e controllo della qualità

I requisiti sui parametri di generazione delle chiavi sono riportati nel cap. 6.1.1.

Il QTSP assicura che gli HSM coperti da Certificazione, operano in conformità rispetto a quanto previsto dal raggiunto traguardo di sicurezza.

6.1.7 Scopi del Key Usage (vedi campo Key Usage X.509 v3)

Il certificato di CA può essere utilizzato in conformità con quanto specificato di seguito:

- Certificate Signing;
- CRL Signing;
- Offline CRL Signing.

Il certificato di Firma Elettronica Qualificata del titolare viene generato in conformità di quanto previsto per la firma elettronica qualificata, il cui key-usage prevede quanto segue:

- Non-ripudio.

Maggiori dettagli sono riportati nel cap. 7.1.2.

6.2 PROTEZIONE DELLA CHIAVE PRIVATA E CONTROLLI SULLA COMPONENTE CRITTOGRAFICA

Il QTSP deve assicurare una gestione sicura delle chiavi private e deve prevenire la pubblicazione, la copia, la cancellazione, la modifica e l'utilizzo non autorizzato.

6.2.1 Standard e controlli dei Moduli crittografici

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

La CA presente nella infrastruttura di certificazione, che assicura l'emissione dei certificati di sottoscrizione, la firma dei response OCSP, la firma della CRL, memorizza le proprie chiavi private all'interno di un dispositivo sicuro certificato come segue:

- Attestato di Certificazione OCSI di conformità ISO/IEC 15408 (Common Criteria) versione 3.1 per il livello di garanzia EAL4+;
- Certificazione FIPS 140-2 Level 3.

Si specifica che il dispositivo HSM utilizzato dal QSCD è incluso nella lista dei dispositivi pubblicata dalla Commissione Europea con titolo "**Compilation of Member States notification on SSCDs and QSCDs**". Il QTSP protegge il funzionamento degli apparati in un Datacenter sicuro, accessibile solo da personale autorizzato.

Il QTSP attua un controllo continuo mirato ad assicurare il rispetto degli standard in vigore. In caso di modifica normativa a seguito di vulnerabilità o rafforzamento degli standard, il QTSP assicura la compliance attuando un piano di manutenzione o di aggiornamento rispetto a quanto normativamente richiesto

6.2.2 Controllo segregazione chiave privata (MofN)

Il QTSP assicura la contemporanea presenza di almeno 2 persone che operano sull'HSM, con ruoli appositamente approvati, durante lo svolgimento di operazioni critiche di sicurezza, in accordo con quanto specificato in 5.2.2.

6.2.3 Key Escrow della chiave privata

Il QTSP non fornisce strumenti di key escrow applicati alla chiave privata della CA.

6.2.4 Backup chiave privata

Il QTSP effettua copie di sicurezza della chiave privata della CA, e almeno una copia viene custodita in un luogo differente da quello di esercizio del QTSP.

Le procedure di backup avvengono rispettando i criteri di segregazione specificati nel cap. 6.2.2.

Le misure di sicurezza applicate ai sistemi di produzione, sono le stesse che si applicano ai backup.

Il QTSP non effettua copie delle chiavi private dei sottoscrittori.

6.2.5 Archiviazione della chiave

Il QTSP non effettua l'archiviazione della chiave privata della CA.

6.2.6 Trasferimento della chiave privata da/per il modulo crittografico

La chiave privata della CA del QTSP è mantenuta in modo sicuro attraverso i meccanismi di protezione forniti dall'HSM, coperti dalle certificazioni specificate nel cap. 6.2.1.

La chiave privata della CA non è mai custodita in chiaro.

Il QTSP può esportare la chiave privata al di fuori del perimetro dell'HSM solo ed esclusivamente per scopi di backup.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

In caso di trasferimento fisico della chiave privata di CA, il QTSP assicura tutti i criteri di segregazione e di sicurezza volti ad assicurare l'integrità della operazione di restore. La procedura viene eseguita sotto la stretta osservanza del manuale di prodotto, e delle configurazioni previste dai traguardi di certificazione. I criteri di segregazione sono volti ad assicurare l'eventuale spedizione separata delle componenti HW di trasporto della chiave, e dei segreti per il restore.

6.2.7 Memorizzazione della chiave privata sul modulo crittografico

La CA memorizza la chiave privata utilizzata per i servizi previsti, in accordo con il presente documento, esclusivamente su HSM.

Gli aspetti di tecnici e di sicurezza legati alla memorizzazione della chiave privata, sono definiti dalle specifiche tecniche del prodotto, e verificati dai test di certificazione.

6.2.8 Metodi di attivazione della chiave privata

La chiave privata della CA del QTSP è attivata in accordo con le procedure e i requisiti definiti nei manuali di prodotto, e con quanto specificato nei documenti di certificazione.

Nel caso di chiave privata del sottoscrittore, il QTSP assicura che i dati di attivazione siano generati e gestiti in maniera sicura in modo da impedire l'utilizzo non autorizzato della chiave privata.

Il QTSP assicura inoltre che:

- La chiave privata destinata al sottoscrittore non è utilizzata per firma elettronica qualificata, prima della consegna al titolare;
- Prima della esecuzione della procedura di firma, al sottoscrittore è richiesta l'autenticazione allo slot protetto dall'HSM.

6.2.9 Metodo di disattivazione della chiave privata

CA Private Keys

La chiave di CA del QTSP viene disattivata in accordo con le procedure specificate nel manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione.

Chiave privata del sottoscrittore

La chiave privata rilasciata al sottoscrittore viene disattivata in accordo con le procedure specificate nel manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione.

L'HSM deve assicurare la disattivazione delle chiavi nei seguenti casi:

- Mancata alimentazione elettrica del device;
- Il sottoscrittore chiuda l'applicazione di firma;
- Per qualche motivo, la connessione all'applicazione di firma chiuda la connessione inaspettatamente.

La chiave così disattivata può essere riutilizzata solo dopo una nuova autenticazione del sottoscrittore al dispositivo.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

6.2.10 Metodo di distruzione della chiave privata

Chiave di CA del QTSP

La chiave di CA del QTSP può essere cancellata in accordo con le procedure specificate nel manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione. Le procedure devono assicurare che non sia possibile recuperare in alcun modo la chiave privata così cancellata.

L'operazione di cancellazione avviene sotto il controllo di operatori autorizzati e compatibilmente con i criteri di segregazione specificati nel cap. 6.2.2.

Ogni copia di backup della chiave privata è distrutta in accordo con le procedure specificate nel manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione. Tale procedura impedisce la possibilità di recupero della chiave privata.

Chiave privata del sottoscrittore

La chiave privata del sottoscrittore viene cancellata in accordo con le procedure specificate nel manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione.

6.2.11 Valutazione del modulo crittografico

La valutazione delle certificazioni associate al modulo crittografico utilizzato dal QTSP, sono compatibili con quanto specificato nel cap. 6.2.1.

6.2.12 Validità del certificato e delle chiavi

Certificato e chiavi della root CA

Il periodo di validità del certificato di CA del QTSP, e della relativa coppia di chiavi, è di 30 anni.

Il periodo di validità del certificato e delle relative chiavi non deve in ogni caso essere superiore alla validità degli algoritmi utilizzati secondo quanto stabilito dalle autorità preposte.

Certificato e chiavi sottoscrittori

La validità del certificato di sottoscrizione rilasciato all'utente finale:

- Ha validità di 3 anni;
- Non deve in ogni caso essere superiore alla validità degli algoritmi utilizzati secondo quanto stabilito dalle autorità preposte;
- Non deve in ogni caso essere superiore alla validità del certificato della CA del QTSP che lo ha rilasciato.

6.3 DATI DI ATTIVAZIONE

6.3.1 Generazione ed installazione dati di attivazione

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

La chiave di CA del QTSP è protetta in accordo con le procedure specificate nel manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione.

Nell'ambito della gestione della password, il QTSP applica criteri di complessità sufficienti al fine di assicurare un adeguato livello di protezione.

In caso di attivazione di chiavi destinate al sottoscrittore, il QTSP assicura:

- Che i dati di attivazione utilizzati per l'attivazione della chiave privata, sono creati utilizzando criteri di generazione di numeri/lettere di adeguata qualità;
- Che i dati di attivazione sono comunicati al sottoscrittore in maniera sicura.

Il meccanismo di autenticazione utilizzato come secondo fattore di autenticazione, è di tipo OTP inviato via SMS o generato tramite Token fisici. L'OTP inviato/generato, è basato sulla delivery di un codice one shot al cellulare/display Token del titolare al momento della firma.

Il motore di generazione dei codici è basato sullo sviluppo di "Initiative for Open Authentication", ed utilizza in particolare il meccanismo TOTP specificato nell'RFC 6238.

6.3.2 Protezione dei dati di attivazione

I dati di attivazione delle chiavi private associate al certificato del sottoscrittore, vengono memorizzati dal QTSP al solo scopo di delivery al titolare. La memorizzazione dei dati viene effettuata in maniera sicura attraverso la cifratura delle informazioni di sicurezza.

L'invio dell'SMS viene effettuato tramite un SMS Gateway e connessione protetta SSL. L'applicazione di delivery adotta opportuni meccanismi di cifratura del repository, impedendo in qualsiasi momento il mantenimento in chiaro del dato.

I meccanismi di protezione dei dati di attivazione delle chiavi vengono applicati anche per quanto concerne l'uso dei dispositivi Token OTP fisici.

6.3.3 Altri aspetti sui dati di attivazione

Non applicabile.

6.4 CONTROLLI DI SICUREZZA SU COMPUTER

6.4.1 Requisiti Tecnici di sicurezza specifici su sistemi IT

Le operazioni di configurazione, manutenzione o consultazione sui sistemi IT del QTSP, sono effettuati assicurando i seguenti requisiti:

- Che l'identità dell'utente sia verificata prima dell'accesso al sistema o all'applicazione;
- Che i ruoli siano assegnati agli utenti al fine di assicurare che gli stessi abbiano permessi appropriati;
- Che siano registrati eventi di log di sicurezza rilevanti, che siano successivamente archiviati secondo le norme in vigore, con specifico riferimento a quanto contenuto nello standard EN 319 411 02 v1.2.2 cap. 6.4.5;
- Che i processi critici del QTSP siano protetti da adeguate policy di rete, al fine di prevenire accessi non autorizzati;
- Che ci siano adeguati sistemi di recovery che garantiscano la continuità operativa a seguito di malfunzionamento dei sistemi primari.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

6.4.2 Valutazione della Sicurezza dei sistemi IT

Al fine di assicurare la sicurezza e la qualità dei sistemi, il QTSP adotta sistemi di controllo ispirati a standard internazionali globalmente accettati, la cui adeguatezza sia certificata da un assessor indipendente.

6.5 CICLO DI VITA DEI CONTROLLI TECNICI

6.5.1 Controllo dei sistemi di sviluppo

Il QTSP, nei propri sistemi, adotta soluzioni di tipo commerciale. Tali soluzioni non sono utilizzati per altri scopi oltre a quelli previsti per l'attività di certificazione del QTSP Lottomatica Holding S.r.l..

Lottomatica Holding S.r.l. adotta altresì strumenti di prevenzione in grado di proteggere i propri sistemi dall'esecuzione di codice pericoloso. La ricerca di codice pericoloso viene effettuata su base continua, attraverso gli assessment interni di sicurezza.

Il QTSP utilizza personale adeguato e aggiornato per le attività di installazione o manutenzione dei propri sistemi SW/HW.

6.5.2 Controlli di gestione della sicurezza

Il QTSP assicura che i programmi, o le patch di sicurezza, siano installate nella versione corretta e che non contengano modifiche non autorizzate.

Lottomatica Holding S.r.l. definisce applica e verifica criteri e procedure per la pianificazione, lo sviluppo sicuro, il test, l'accettazione e la gestione operativa dei sistemi ICT.

Le aree tecniche di Lottomatica Holding S.r.l.:

- Monitorano l'uso delle risorse garantendo, mediante opportune proiezioni e stime, le prestazioni attuali e future dei sistemi ICT. Tali stime indirizzano il reperimento di nuove risorse che garantiscano la futura operatività;
- In collaborazione con le aree che richiedono lo sviluppo o l'acquisizione di nuovi sistemi o funzionalità, stabiliscono i criteri di accettazione, comprensivi di specifici criteri di sicurezza, per i nuovi sistemi ICT, per gli aggiornamenti e per le nuove versioni. Tali criteri supportano e guidano i test di collaudo;
- Effettuano un'attività di Code Review (analisi statica del codice) finalizzata ad identificare vulnerabilità all'interno del codice sorgente seguita dalle eventuali attività di remediation con modifica del codice;
- Effettuano attività di test dei sistemi, in ambiente di test dedicato utilizzando dati opportunamente selezionati e separati da quelli utilizzati negli ambienti di produzione;
- Effettuano attività di analisi dinamica analisi delle reazioni del software a vari tipi di input per applicazioni web;
- Definiscono e valutano i criteri di accettazione dei sistemi ICT in base a requisiti e risorse utilizzate, procedure di ripristino, misure di emergenza, condizioni di business continuity ed analisi di impatto;
- Effettuano attività di Patch management, a seguito delle attività di individuazione delle vulnerabilità, della comunicazione di rilascio patch dai fornitori di software o dai principali enti di settore accreditati, al fine di mitigare, dove ritenuto necessario, le vulnerabilità dei sistemi;
- Gestiscono le attività di Change Management e Capacity Management al fine di garantire che l'applicazione delle modifiche necessarie sugli ambienti ICT tengano in dovuta considerazione i rischi potenziali introdotti dalle modifiche stesse, garantire le disponibilità/performance dei sistemi

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

e degli apparati di rete e sicurezza utilizzati di individuare eventuali problemi sui tali sistemi o gli apparati, al, definendo al tempo stesso le relative azioni correttive, ed ottimizzare le risorse fisiche di sistemi ed apparati.

Gli ambienti di produzione sono opportunamente separati e isolati dagli ambienti dedicati a test e collaudo. Tale separazione viene realizzata a livello fisico, logico, procedurale ed organizzativo attraverso una chiara attribuzione delle responsabilità.

6.5.3 Ciclo di vita dei controlli di sicurezza

Il QTSP assicura la protezione delle componenti di sicurezza nel loro ciclo di vita. In particolare, per quanto riguarda l'HSM:

- Che abbia le corrette certificazioni;
- Che alla ricezione degli apparati, gli stessi non risultino in stato "tampered";
- Che la protezione dal tampering sia assicurata durante l'esercizio;
- Che continui ad essere osservato quanto contenuto nel manuale utente o nei documenti di certificazione;
- Che le chiavi private siano cancellate da apparati non in uso, in una maniera che non sia possibile il ripristino.

6.6 CONTROLLI DI SICUREZZA DELLA RETE

Al fine di garantire un livello di sicurezza della rete aziendale Lottomatica Holding S.r.l.:

- Stabilisce responsabilità e le procedure per la gestione degli apparati di rete;
- Implementa controlli per garantire la sicurezza del transito dei dati attraverso la rete e la protezione da accessi non autorizzati dei servizi connessi. Tale obiettivo è raggiunto attraverso la divisione logica in reti separate e il corretto utilizzo di strumenti per la gestione avanzata della sicurezza (es. Firewall, Sonde di monitoraggio del traffico, ...);
- Definisce ed implementa controlli specifici per la salvaguardia dell'integrità e della confidenzialità dei dati critici in transito sulla rete pubblica ed in particolare su reti wireless;
- Attiva funzionalità di monitoring e di logging al fine di controllare e registrare eventuali anomalie. Le attività di gestione della rete sono coordinate sia per ottimizzare i servizi di business, sia per assicurare che i controlli siano efficacemente applicati sull'intera infrastruttura;
- Configura opportunamente i dispositivi firewall e router in modo da lasciare aperte soltanto le porte strettamente necessarie ai servizi di esercizio;
- Adotta regole per l'attribuzione dei privilegi al personale che accede alle porte di configurazione e diagnostica. La configurazione dei dispositivi di sicurezza logica perimetrale è soggetta ad attività periodiche di revisione ed aggiornamento;
- Adotta principi di segregazione delle reti secondo criteri seguenti:
 - Una segregazione logica tra la rete che offre servizi Corporate e la rete che ospita i sistemi del QTSP;
 - Una segregazione logica di tipo dipartimentale all'interno di ciascuna delle due sottoreti in base alla tipologie di servizio offerto.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Utilizzo di canali protetti, o di strumenti per lo scambio cifrato delle informazioni per proteggere le comunicazioni tra reti fisicamente separate che utilizzano Internet come mezzo di comunicazione (HTTPS over Internet o tunnel VPN cifrati);
- Garantisce che i dispositivi che gestiscono dati o infrastrutture ad elevata criticità risiedano su hardware dedicato, ed in particolar modo non convivano con servizi di altra natura che possano comprometterne la sicurezza;
- I dispositivi di test e di esercizio siano dimensionati correttamente in base alle specifiche dei servizi che dovranno erogare e alla quantità di dati/traffico che dovranno gestire.

Le reti siano essere fisicamente sicure per quanto concerne cablaggio (elettrico e di trasporto dati), collocazione delle macchine e presenza di gruppi di continuità.

6.7 TIME-STAMPING

Il QTSP utilizza propri sistemi di Timestamp in accordo con il presente documento rilasciato specificatamente e separatamente per questo servizio.

Inoltre, ai sensi dell'articolo 41, comma 3, del DPCM 22 Febbraio 2013 [24] l'ora assegnata ai riferimenti temporali deve corrispondere alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

7 CERTIFICATI, CRL, E PROFILI OCSP

7.1 PROFILO DI CERTIFICATO

Il QTSP dispone di una root CA destinata alla emissione dei certificati di firma elettronica qualificata, ed ai servizi di certificazione connessi.

Il certificato di CA e il certificato del sottoscrittore rilasciati dal QTSP, sono compatibili con i seguenti standard:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Publickey and attribute certificate frameworks [19];
- RFC 5280 [16];
- RFC 6818 [17];
- ETSI EN 319 412-1 [5];
- ETSI EN 319 412-2 [6];
- ETSI EN 319 412-5 [9].

7.1.1 Specifica X509

Lo standard X.509 adottato per la CA di root e per i certificati di sottoscrizione, sono di tipo "v3".

Il QTSP utilizza le seguenti estensioni di base:

- Version
Il certificato è compatibile con la versione "v3"
- Serial Number
L'applicazione del campo Serial Number è in accordo con quanto specificato nel documento EN 319 412 01 v1.1.1
- Algorithm Identifier
L'OID dell'algoritmo utilizzato per la certificazione del Certificato;
- Il QTSP adotta il seguente algoritmo:
"sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
- Signature
Firma elettronica eseguita dal QTSP per la certificazione del Certificato, eseguita compatibilmente con quanto specificato nel campo "Algorithm Identifier";
- Issuer
Il Distinguish Name dell'entità che ha rilasciato il Certificato.
- Valid From & Valid To
Periodo di validità del certificato. Il tempo è registrato in accordo con il riferimento UTC in accordo con quanto specificato nell' RFC 5280.
- Subject
L'identificativo univoco del soggetto.
- Subject Public Key Identifier:
Il QTSP supporta l'algoritmo RSA nei certificati di sottoscrizione. La lunghezza della chiave di sottoscrizione è di 2048 bit.
- Il valore incluso in questo campo corrisponde al valore:
 - "rsaEncryption" (1.2.840.113549.1.1.1)
- Subject Public Key Value

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

La chiave pubblica associata al Subject.

7.1.2 Estensioni di certificato

Il QTSP utilizza estensioni di certificato compatibili con lo standard X.509 [19].
Si riportano di seguito i requisiti specifici riguardanti le suddette estensioni:

Certificato di root CA

| Nome | Valore |
|---|---|
| Version | Versione 3 |
| Serial Number | (Attribuito a runtime) |
| Signature | sha256, RSA |
| Issuer (ETSI 319 412-2 par. 4.2.3.1) | DN del QTSP: countryName : "IT" organizationName: "Lottomatica Holding S.r.l." organizationIdentifier : "VATIT- 02611940038 " commonName : "Lottomatica EU Qualified Certificates CA" |
| Validity | 30 Anni (scadenza 30 anni dalla data di emissione) |
| Subject | Vedi Issuer |
| SubjectPublicKeyInfo | Chiave pubblica 4096 bit Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| Basic Constraint (critica) | Subject Type: CA Path Length Constraint:0 |
| KeyUsage (critica) | Certificate Signing, Offline CRL Signing, CRL Signing (06) |
| Authority Information Access | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it |
| Certificate Policies (non critico) | OID della policy: 1.3.76.49 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti |
| crlDistributionPoint (non critico) | http://ca.firmadigitale.lottomaticaitalia.it/qtspcacrlh2020.crl |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Certificato del sottoscrittore B2B - Area Giochi/Servizi (IGTCP01)

| Campi Base | |
|--|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |
| SubjectPublicKeyInfo | RSA (2048 bits) Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|---|
| REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280) | URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.20.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacr1h2020.crl |

Certificato del sottoscrittore Utente Interno - Area Giochi/Servizi (IGTCP03)

| Campi Base | |
|--|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |
| SubjectPublicKeyInfo | RSA (2048 bits) |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|---|
| | Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access REGOLAMENTO (UE) N. 910/2014 ALLEGATO I, h) (RFC 5280) | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.22.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Certificato del sottoscrittore Firma Automatica – Area Giochi/Servizi (IGTCP04)

| Campi Base | |
|---|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |
| SubjectPublicKeyInfo | RSA (2048 bits) Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|---|
| REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i> (RFC 5280) | (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.23.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il presente certificato è valido solo per firme apposte con procedura automatica The certificate may only be used for unattended/automatic digital signature |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacr1h2020.crl |

Certificato del sottoscrittore Master-RAO, RAO - Area Giochi/Servizi (IGTCP05)

| Campi Base | |
|--|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |
| SubjectPublicKeyInfo | RSA (2048 bits) |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|--|
| | Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access REGOLAMENTO (UE) N. 910/2014 ALLEGATO I, h) (RFC 5280) | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.24.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Certificato del sottoscrittore B2B - Area Servizi (IGTCP06)

| Campi Base | |
|---|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |
| SubjectPublicKeyInfo | RSA (2048 bits) Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access REGOLAMENTO (UE) N. 910/2014 | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|---|
| ALLEGATO I, h) (RFC 5280) | |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.25.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrlh2020.crl |

Certificato del sottoscrittore Master-RAO, RAO - Area Servizi (IGTCP07)

| Campi Base | |
|--|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|--|
| SubjectPublicKeyInfo | RSA (2048 bits) Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access REGOLAMENTO (UE) N. 910/2014 ALLEGATO I, h) (RFC 5280) | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.26.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il titolare del certificato deve utilizzare il certificato solo ai fini di registration authority officer per i quali esso è rilasciato The certificate holder must use the certificate only for the registration authority officer purposes for which it is issued |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Certificato dell'utente interno – Area Servizi (IGTCP08)

| Campi Base | |
|---|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |
| SubjectPublicKeyInfo | RSA (2048 bits) Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access REGOLAMENTO (UE) N. 910/2014 | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|---|
| ALLEGATO I, h) (RFC 5280) | |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.27.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Uso limitato a rapporti del Titolare con soggetti connessi con attività riconducibili o veicolate da Lottomatica Holding Srl o LIS Spa o società sottoposte al comune controllo Usage limited to the relations by the Owner with subjects connected with activities attributable or conveyed by Lottomatica Holding Srl or LIS Spa or companies under common control |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrhlh2020.crl |

Certificato del sottoscrittore Firma Automatica – Area Servizi (IGTCP09)

| Campi Base | |
|---|---|
| Version | Versione 3 |
| Serial Number | (attribuito a runtime) |
| Signature Algorithm | sha256, RSA |
| Issuer | countryName : "IT" organizationName: "Lottomatica Holding S.r.l. " organizationIdentifier : "VATIT-02611940038" commonName : "Lottomatica EU Qualified Certificates CA" |
| Validità | 3 anni |
| Subject_DN (ETSI 319 412-2 par. 4.2.4 - Subject) (ETSI 319 412 -1 par.5.1.3 - Natural person semantics identifier) | C = IT, SN = <cognome titolare>, G = <nome titolare>, SERIALNUMBER = TINIT-<CF del titolare>, CN = <nome e cognome titolare>, dnQualifier = <identificativo della richiesta> |
| SubjectPublicKeyInfo | RSA (2048 bits) |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

| | |
|--|---|
| | Algoritmo utilizzato: RSA |
| Estensioni | |
| Authority Key Identifier | SHA-1 160 bit |
| Subject Key Identifier | SHA-1 160 bit |
| QC_Statements (non critico) (ETSI 319 412-5 par. 4.2, 4.3 e 5) | qcStatements-1 QcCompliance (0.4.0.1862.1.1) qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" qcStatements-4 QcSSCD (0.4.0.1862.1.4) qcStatements-5 QcEuPDS (0.4.0.1862.1.5): https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh2020.pdf qcStatements-6 QcEuPDS (0.4.0.1862.1.6):id-etsi-qct-esign |
| KeyUsage (critica) | Non Repudiation |
| Authority Information Access REGOLAMENTO (UE) N. 910/2014 ALLEGATO I, h) (RFC 5280) | Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.ca.firmadigitale.lottomaticaitalia.it Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/CAH2020.crt |
| Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3) | 1.3.76.16.6 1.3.76.49.1.1.1.28.1.0 Cp: URL: https://ca.firmadigitale.lottomaticaitalia.it/documenti Notice Text: Il presente certificato è valido solo per firme apposte con procedura automatica The certificate may only be used for unattended/automatic digital signature |
| crlDistributionPoint (non critico) | https://ca.firmadigitale.lottomaticaitalia.it/qtspcacr1h2020.crl |

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

7.1.2.1 Gestione in continuità dei certificati di Lottomatica S.p.A

Lottomatica Holding S.r.l. prende in carico la gestione delle CA di Lottomatica S.p.A. garantendo la continuità di tutti i servizi relativi alla vecchia CA non dismettendo quindi i seguenti link:

- Ocsp – <http://ocsp.ca.firmadigitale.lottomaticaitalia.it>
- Verificatore – <https://ver.ca.firmadigitale.lottomaticaitalia.it>
- Documenti – <https://ca.firmadigitale.lottomaticaitalia.it/documenti>
- CRL TSA – <https://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrl.crl>
- CRL CA – <https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrl.crl>
- PDS TSA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qsptsapds.pdf>
- PDS CA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapds.pdf>

che rimarranno disponibili ed utilizzabili anche dopo il passaggio societario e relativo cambio CA.

Tutti i certificati rilasciati da Lottomatica S.p.A. sono da considerarsi validi in continuità con Lottomatica Holding S.r.l. anche rispetto alle attuali limitazioni di uso.

7.1.2.2 Gestione in continuità dei certificati di Lottomatica Holding a seguito di cambio di P.IVA

Lottomatica Holding S.r.l. prende in carico la gestione delle precedenti CA di Lottomatica Holding garantendo la continuità di tutti i servizi relativi alla precedente CA non dismettendo quindi i non dismettendo quindi i seguenti link:

- Ocsp – <http://ocsp.ca.firmadigitale.lottomaticaitalia.it>
- Verificatore – <https://ver.ca.firmadigitale.lottomaticaitalia.it>
- Documenti – <https://ca.firmadigitale.lottomaticaitalia.it/documenti>
- CRL TSA – <https://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh.crl>
- CRL CA – <https://ca.firmadigitale.lottomaticaitalia.it/qtspcacrlh.crl>
- PDS TSA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qsptsapdsh.pdf>
- PDS CA – <https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtspcapdsh.pdf>

che rimarranno disponibili ed utilizzabili anche dopo il cambio di P.IVA e relativo cambio CA.

Tutti i certificati rilasciati da Lottomatica Holding S.r.l. (P.IVA 13044331000) sono da considerarsi validi in continuità con Lottomatica Holding S.r.l. anche rispetto alle attuali limitazioni di uso.

7.1.3 Object Identifier Algoritmi

Solo l'identificativo (OID) degli algoritmi utilizzati devono essere utilizzati, in accordo con quanto specificato nel capitolo 6.1.5.

Gli algoritmi che possono essere utilizzati dalla CA sono elencati nel presente Documento.

7.1.4 Composizione del nome

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

La composizione del nome identificante il distinguish name, viene composto compatibilmente con quanto specificato dagli standard RFC 5280 [16], ETSI EN 319 412-2 [6].

Il Certificato deve contenere un OID univoco del Subject come definito nel cap. 3.1.1.

Il SubjectDN del titolare include il campo serialNumber specificato come di seguito:

- "TIN": campo identificativo univoco associato alla persona; il codice fiscale del titolare;
- "IT": codifica ISO 3166 del country code per L'Italia;
- "- ": carattere 0x2D (ASCII);
- Identificativo: il valore del codice fiscale del titolare.

Il campo dnQualifier, contiene il riferimento univoco relativo alla richiesta creata dal QTSP ed associata alla emissione del certificato.

7.1.5 Vincoli sul nome

Non presenti.

7.1.6 Object Identifier policy di certificato

Il QTSP include nei certificati rilasciati la policy di certificato in accordo con il cap. 7.1.2.

7.1.7 Utilizzo dell'estensione Policy Constraint

Non presente.

7.1.8 Sintassi e semantica dei qualificatori della Policy

Specificato in 7.1.2.

7.1.9 Gestione della semantica per estensioni di certificate policy critiche

Specificato in 7.1.2.

7.2 PROFILO CRL

7.2.1 Versione

Il QTSP rilascia una Certificate Revocation List (CRL) con versione "v2", in accordo con lo standard l'RFC 5280 [16].

7.2.2 Specifica delle estensioni della CRL

In accordo con l'RFC 5280 [16], la CRL rilasciata dalla CA può includere le seguenti estensioni:

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Version
Il valore del campo è "v2".
- Signature Algorithm Identifier
L'identificativo (OID) dell'algoritmo utilizzato per la creazione della firma elettronica che certifica la CRL. L'algoritmo previsto è "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).
- Signature
La firma elettronica che certifica la CRL.
- Issuer
L'entità che rilascia la CRL.
- This Update
La data di entrata in vigore della CRL. Il valore deve essere in accordo con lo standard UTC in accordo con l'RFC 5280 [16].
- Next Update
La data di prossimo rilascio della CRL. Il valore deve essere in accordo con lo standard UTC in accordo con l'RFC 5280 [16].
- Revoked Certificates
La lista dei seriali dei certificati revocati comprensiva dell'orario.

Le estensioni obbligatorie che devono essere presenti nella CRL sono:

- CRL number – non critica
Un numero serial progressivo identificante la singola CRL

La seguente estensione può essere usata dalla CA:

- expiredCertsOnCRL – non critica
La CA indica attraverso la presente estensione che i certificati scaduti non sono rimossi dalla CRL (si veda cap. 4.9). La notazione è in accordo alla specifica X.509.

L'elenco dei certificati revocati include le seguenti estensioni:

- Reason Code – non critica
Il motivo di revoca del certificato.

Il riferimento orario a partire dal quale la chiave è ritenuta compromessa.

- Hold Instruction – non critica

7.3 PROFILO OCSP

Il QTSP fornisce un servizio OCSP compliant agli standard RFC 2560 [13] e RFC 6960 [18].

7.3.1 Versione

Il servizio OCSP fornito è compatibile con la versione "v1" in accordo con quanto specificato negli standard RFC 2560 [13] e RFC 6960 [18].

7.3.2 Estensioni OCSP

Le estensioni presenti nel protocollo OCSP, sono quelle previste in accordo con l'RFC 6960 [18].

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

8 COMPLIANCE AUDIT E ALTRI ASSESSMENTS

L'operato del QTSP nei confronti della compliance in vigore è sotto la vigilanza dell'**AgID, Agenzia per l'Italia Digitale**.

L'attività di verifica della compliance è condotta in fase di Certificazione del QTSP e, successivamente, con cadenza annuale, attraverso ispezione nei siti presso i quali il QTSP eroga i propri servizi.

L'attività di Audit è volta ad accertare che l'operato del QTSP sia conforme al Regolamento eIDAS [27], e la compliance verso le applicabili leggi nazionali e le specifiche di erogazione del servizio enunciate nel presente documento.

L'attività di Audit è conforme ai seguenti documenti di riferimento:

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [27];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers [2];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [1];
- ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [3];
- ETSI EN 319 411-2 v2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [4].

Il risultato dell'attività di Audit è confidenziale ed è accessibile solo da persone autorizzate.

8.1 FREQUENZE O REQUISITI DI ASSESSMENT

L'attività di Audit sulla compliance del QTSP è condotta su base biennale con sorveglianza annuale.

8.2 IDENTITÀ/QUALIFICA DEGLI ASSESSOR

Le verifiche di conformità sulla CA sono svolte da un organismo di valutazione di conformità (Conformity Assessment Body – CAB).

L'assessor deve essere in possesso della Certificazione della conformità dei prestatori di servizi fiduciari e dei servizi da essi prestati a fronte del Regolamento (UE) 910/2014 e del Regolamento (UE) 765/2008.

L'organismo unico di accreditamento degli attestatori di conformità per l'Italia, è **Accredia**.

8.3 INDIPENDENZA DELL'ASSESSOR

Il QTSP garantisce che la persona/società che esegue l'assessment, sia indipendente dalla proprietà e dal management del QTSP.

8.4 ARGOMENTI COPERTI DALL' ASSESSMENT

L'attività di Audit è condotta sulle seguenti aree:

- Conformità con le norme in vigore;
- Conformità con gli standard tecnici;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Conformità con il presente documento;
- Adeguatezza dei processi coperti;
- Documentazione;
- Sicurezza fisica;
- Adeguatezza del personale;
- Sicurezza IT;
- Compliance con i ruoli sulla protezione dei dati.

8.5 AZIONI INTRAPRESE IN CASO DI NON CONFORMITÀ

L'Auditor compila un report sulla base dei controlli effettuati. Eventuali non conformità possono essere gestite come segue:

- Suggerimenti su modifiche da prendere in considerazione;
- Deroghe che costituiscono un avvertimento obbligatorio.

8.6 COMUNICAZIONE DEI RISULTATI

L'Auditor comunica l'esito del report all'AgID che certifica/conferma lo stato di QTSP, attraverso il rilascio dell'attestato di Conformità per Prestatori di Servizi Fiduciari Qualificati.

Il certificato X.509 della CA del QTSP viene pubblicato nelle liste dei Prestatori di Servizi Fiduciari Qualificati.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

9 ASPETTI ECONOMICO LEGALI

9.1 TARIFFE

Il servizio di Firma elettronica qualificata è erogato da Lottomatica Holding S.r.l. a titolo gratuito. Pertanto, non è prevista l'applicazione di tariffe.

9.2 RESPONSABILITÀ FINANZIARIE

Lottomatica Holding S.r.l. è responsabile della erogazione dei servizi connessi con l'attività del QTSP. Ai fini della Qualificazione e dell'accreditamento, in compliance con l'Art 29 del CAD [26] comma 3a, Lottomatica Holding S.r.l. ha capitale sociale di Euro 88.392.200,00.

9.2.1 Copertura assicurativa

Lottomatica Holding S.r.l. ha stipulato una polizza assicurativa tale da garantire un limite di indennizzo pari ad € 5.000.000,00.

9.3 CONFIDENZIALITÀ DELLE INFORMAZIONI DI BUSINESS

La confidenzialità delle informazioni legate al business, è gestita in compatibilità con la vigente normativa.

9.4 TUTELA DEI DATI PERSONALI

In Lottomatica Holding S.r.l. è operativo un sistema organizzativo e normativo per garantire che tutti i trattamenti di dati personali si svolgano nel rispetto delle disposizioni del Regolamento UE 2016/679 (di seguito "Regolamento" o anche "GDPR") [25] e dell'applicabile normativa Italiana di coordinamento sulla tutela dei dati personali nonché nel pieno rispetto dei principi di correttezza e liceità dichiarati nel codice etico.

Tale sistema si caratterizza per alcune importanti elementi di base, fra i quali si ricordano i seguenti:

- I dipendenti che hanno ricevuto la nomina di Incaricati / Persone autorizzate al trattamento dei dati personali ai sensi dell'art. 4 n. 10 del Regolamento [25], hanno ricevuto dettagliate istruzioni circa le modalità e le misure di sicurezza da adottare per il trattamento dei dati personali;
- Il trattamento dei dati personali avviene sotto la supervisione di responsabili del trattamento, anch'essi formalmente nominati, i quali hanno a loro volta ricevuto le necessarie istruzioni ed indicazioni operative;
- Apposite funzioni aziendali hanno il compito di definire le policy per la sicurezza delle informazioni e di verificare, con l'ausilio di funzioni di auditing interno, che esse siano effettivamente applicate;
- Il sistema di policy si basa sulla corretta classificazione degli asset. Con l'ausilio di strumenti di risk assessment, sono individuate le misure di sicurezza più idonee alla tutela dei singoli asset, alla definizione dei controlli e all'applicazione dei sistemi di monitoraggio e verifica più appropriati;
- La tutela dei dati personali non si configura come un processo indipendente, ma risulta del tutto integrato nella gestione corrente della sicurezza degli asset aziendali;
- Le politiche di sicurezza fisica e di tutela del patrimonio materiale dell'azienda e le politiche di gestione degli incidenti di sicurezza e delle crisi sono definite tenendo presenti i principi di tutela dei dati personali e le necessità di protezione di questi dati fissate dalla legge.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Nell'ambito delle policy di sicurezza aziendale sono state sviluppate soluzioni tecniche ed organizzative per la protezione dei dati trasmessi e conservati sulla rete e sui sistemi aziendali, fra cui rientrano, a titolo esemplificativo e non esaustivo:

- Protezione dai virus con aggiornamento continuo;
- Hardening dei sistemi utilizzati;
- Software distribution per l'aggiornamento automatico delle patch di sicurezza sui sistemi aziendali;
- Tool e metodologie di vulnerability assessment e risk analysis;
- Protezione informatica e dei punti di accesso alla rete aziendale (ad esempio: Controllo Accessi, Credenziali di autenticazione, ecc.);
- Partizionamento e protezione delle reti interne;
- Monitoraggio della rete e dei sistemi per la prevenzione ed il contrasto degli incidenti di sicurezza.

9.4.1 Modalità di protezione dei dati personali

Il presente capitolo ha lo scopo di illustrare le procedure e le modalità operative adottate dal QTSP per il trattamento dei dati personali, nello svolgimento della propria attività di certificazione.

I dati personali relativi al richiedente la registrazione, al Titolare di certificati, al terzo interessato e a chiunque acceda al servizio, sono trattati, conservati e protetti dal QTSP conformemente a quanto previsto dal Regolamento e dall'applicabile normativa Italiana di coordinamento sulla tutela dei dati personali nonché nel rispetto dei provvedimenti del Garante per la protezione dei dati personali.

La terminologia utilizzata nel presente capitolo è conforme a quella adottata dal Regolamento. In particolare:

- a. Per Titolare del trattamento, si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali;
- b. Per Responsabile del trattamento si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- c. Per Incaricato si intende la persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- d. Per Interessato, si intende la persona fisica identificata o identificabile cui si riferiscono i dati personali (ovvero il richiedente la registrazione, il Titolare di certificati, o chiunque acceda al servizio);

In particolare, il QTSP:

- Nomina, se del caso, un Responsabile del trattamento dei dati interno alla propria organizzazione aziendale, comunicandogli analiticamente e per iscritto i compiti che dovrà assolvere ai sensi dell'Art. 28 comma 3 del Regolamento. In particolare, se designato, il responsabile del trattamento:
 - È individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza (comma 2);
 - Effettua il trattamento attenendosi alle istruzioni impartite dal Titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni in materia di trattamento e delle proprie istruzioni (comma 5).
- Individua e nomina i funzionari Incaricati del trattamento dei dati (ovvero gli Incaricati dell'Identificazione e quanti altri tratteranno i dati attinenti il servizio), che operano sotto la diretta autorità del Responsabile del Servizio, attenendosi alle istruzioni impartite;

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Nomina eventuali Responsabili esterni per il trattamento dei dati specificando analiticamente i compiti per iscritto ed effettua, anche tramite verifiche periodiche, controlli sulla puntuale osservanza delle disposizioni di legge e delle proprie istruzioni ai sensi dell'art. 28 del Regolamento.

Definizione e identificazione di "Dati personali"

Ai sensi dell'Art. 4 n. 1) del Regolamento, per *dato personale* si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; pertanto sono dati personali anche i codici identificativi e di sicurezza forniti dal QTSP.

Dati personali, potranno inoltre essere, quelli relativi all'utente, ovvero, ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi – elettronici o cartacei – di registrazione, di revoca, di cambio anagrafica e nei certificati, di cui ai relativi capitoli del presente documento. Al fine di garantirne un trattamento adeguato, le misure di sicurezza predisposte dal QTSP e analiticamente descritte nel Piano per la Sicurezza, sono realizzate conformemente a quanto previsto dal Regolamento e dall'applicabile normativa Italiana di coordinamento sulla tutela dei dati personali.

Tutela e diritti degli interessati

In materia di trattamento dei dati personali il QTSP garantisce la tutela dei diritti degli interessati in ottemperanza al Regolamento. In particolare:

- Agli interessati sono fornite le necessarie informazioni ai sensi dell'Art. 13 del Regolamento (quali ad esempio il Titolare, le modalità e finalità del trattamento, l'ambito di comunicazione e di diffusione, nonché tutti i diritti previsti dagli articoli da 15 a 22 del Regolamento, ove applicabili, ed in particolare: il diritto di accesso ai propri dati (art. 15), il diritto di rettifica dei propri dati (art. 16), il diritto alla cancellazione/diritto all'oblio (art. 17), il diritto alla limitazione del trattamento (art. 18), il diritto alla portabilità dei dati (art. 20), il diritto di opposizione (art. 21), il diritto a non essere sottoposto a processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (art. 22);
- Agli interessati viene richiesto, laddove necessario, il consenso al trattamento dei propri dati personali per una o più specifiche finalità ai sensi dell'art. 6 comma 1 del Regolamento.

Applicazione del Regolamento

Adempimenti generali

Dal punto di vista generale, il QTSP:

- Predisporre, conserva e aggiorna, nell'ambito delle attività di certificazione, un Registro dei certificati ed un Registro degli Archivi Cartacei, contenenti dati personali, incorporati nelle Banche Dati del Titolare e utilizzati nella gestione di tutte le fasi dell'attività di certificazione.

In particolare, il Registro degli Archivi Cartacei è costituito dalle copie della documentazione ottenuta in fase di identificazione dei sottoscrittori RAO e dei sottoscrittori Uso Interno. Tale registro è conservato all'interno di una cassaforte disposta nell'area della Funzione CTO Italy and Global Communication, il cui accesso è consentito ad un ristretto numero di dipendenti Lottomatica Holding S.r.l. autorizzati a svolgere

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

tale mansione. La chiave della cassaforte è custodita presso l'Ufficio Vigilanza (presente h24) ubicato all'interno dell'edificio di via Campo Boario 56. Per ottenere la chiave di accesso alla cassaforte è necessario essere inseriti nella lista del personale autorizzato e viene registrata la presa in carico e la riconsegna della chiave.

Per quanto concerne al Registro dei Certificati, è una funzione interna alla RA e non pubblicamente esposta, contenente tutti i certificati emessi. L'interfaccia (di tipo web accessibile via https) richiede credenziali di accesso, ed applica policy basate su ruolo, che abilitano l'operatore all'accesso dei dati richiesti, fornisce funzioni di ricerca per agevolare l'esigenza. I certificati sono fisicamente memorizzati su media Database, presente all'interno dei CED nei quali è ospitata l'infrastruttura del QTSP, a cui accede esclusivamente il personale autorizzato.

Adempimenti tecnici ed organizzativi

Dal punto di vista tecnico il QTSP, (il Responsabile se nominato) tramite i suoi Incaricati, adotta gli opportuni provvedimenti in relazione alla registrazione, elaborazione, conservazione, protezione dei dati personali, cancellazione/distruzione, secondo le modalità indicate qui di seguito.

1. Registrazione

- Garantisce la conservazione dei dati tecnici relativi a struttura e formato degli archivi informatici e cartacei contenenti dati personali, nonché alla loro locazione fisica;
- Supervisiona l'organizzazione e classificazione in maniera univoca degli archivi, nonché delle loro copie di sicurezza (backup) curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del QTSP. In proposito, si precisa che, a fronte di eventi che dovessero compromettere la capacità operativa del QTSP presso la principale sede di attività, garantisce la disponibilità del Registro dei Certificati e le funzionalità di revoca dei certificati in corso di validità, in coerenza con le procedure di Business Continuity interne al QTSP;
- Supervisiona l'organizzazione e classificazione in maniera univoca dei moduli di registrazione, accettazione, richiesta revoca, cambio anagrafica e qualsivoglia altro documento contenente dati personali, curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del QTSP.

2. Elaborazione

- Controlla che l'elaborazione dei suddetti archivi e dei dati personali in essi contenuti sia effettuata esclusivamente per le finalità indicate nell'informativa resa ai sensi dell'Art. 13 del Regolamento [25];
- Verifica, in funzione del tipo di elaborazione, i formati di output e la destinazione finale dei dati al fine di garantirne la protezione, secondo quanto previsto nel seguito;
- Rileva l'eventuale generazione di nuovi archivi nell'ambito delle fasi di elaborazione, supervisionando la loro classificazione

3. Conservazione

| | | | | |
|---|------------------|---|------------------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- Supervisiona la classificazione degli eventuali archivi – e dei dati in essi contenuti – soggetti a pura e semplice conservazione (archivi storici e/o di backup), riportando la durata della conservazione (inclusa data iniziale e finale), la natura del supporto e la sede di conservazione;
- Si assicura che siano trattati come archivi di conservazione dei dati personali tutti gli archivi appartenenti a procedure temporaneamente bloccate o sospese;
- Verifica che le procedure di conservazione di tutti i documenti utilizzati all'interno dell'attività di certificazione siano coerenti con la tutela dei dati personali.

4. Cancellazione/Distruzione

- Verifica la registrazione – eventualmente in maniera automatizzata – della cancellazione/distruzione di singoli dati personali dagli archivi, riportando la tipologia dei dati, l'archivio interessato, la data di cancellazione/distruzione, nonché l'origine della cancellazione/distruzione (su richiesta dell'interessato, procedurale, accidentale, ecc.);
- Verifica la registrazione della cancellazione/distruzione di archivi interi, secondo le modalità illustrate al punto precedente ed in conformità a quanto previsto dal Regolamento e dall'applicabile normativa Italiana di coordinamento sulla tutela dei dati personali curando inoltre l'aggiornamento del Registro degli Archivi Informatici e Cartacei.

5. Protezione

- Protegge la confidenzialità dei dati personali stabilendo le modalità di accesso agli archivi informatici e cartacei da parte dei soggetti abilitati appartenenti all'organizzazione del QTSP. In particolare:
 - Classifica i soggetti abilitati all'accesso in funzione delle loro mansioni. In particolare, si precisa che il QTSP ha definito ed attua specifiche policy di gestione delle credenziali di autenticazione e per la costruzione e l'utilizzo delle password;
 - Registra le modalità di protezione dei dati, sia per quanto concerne la sicurezza logica degli archivi informatici (software di sicurezza, modalità di generazione del log delle elaborazioni, ecc.) che fisica (vigilanza dei locali, archiviazione documenti, gestione delle copie di sicurezza);
 - Assicura la confidenzialità dei dati personali contenuti nei diversi formati di output delle fasi di elaborazione (cartacei, su terminale, ecc.) stabilendo le modalità operative necessarie, sia manuali che automatizzate;
 - Supervisiona la circolazione interna delle informazioni contenute negli stampati (tabulati) o in altri supporti;
 - Assicura la distribuzione degli output su terminale in accordo con i profili utente designati dal responsabile della sicurezza.
- Protegge l'integrità dei dati singolarmente considerati e degli archivi nel loro insieme, durante tutte le fasi di trattamento, stabilendo le modalità operative necessarie, sia manuali che automatizzate;
- Garantisce la disponibilità dei dati, affinché il Titolare possa adempiere alle richieste di consultazione/verifica da parte degli interessati previste dalla normativa vigente.

Ulteriori modalità di trattamento dei dati, oltre quella prevista dal Regolamento e dall'applicabile normativa Italiana di coordinamento sulla tutela dei dati personali potranno essere previste a livello contrattuale tra il

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

QTSP e l'organizzazione, pubblica o privata che richieda il rilascio di più certificati, per conto di sottoscrittori a lei afferenti. In questo caso, tali accordi sono riportati all'interno del contratto di acquisto dei certificati da parte dell'organizzazione medesima.

Circostanze di rilascio di dati personali

Fermo restando il diritto dell'interessato di richiedere ed ottenere dal QTSP informazioni relative ai propri dati personali, secondo quanto previsto dall'Art. 15 del Regolamento [25], il QTSP, nello svolgimento delle proprie attività di certificazione, può effettuare operazioni di comunicazione e diffusione dei dati personali. In particolare:

- I dati personali possono essere comunicati all'Autorità Giudiziaria, in conformità con quanto previsto dalla normativa vigente;
- Particolari accordi contrattuali possono prevedere destinatari e forme di comunicazione ulteriori rispetto a quanto previsto dalla normativa in vigore. Tali comunicazioni avverranno comunque nel rispetto della normativa vigente.

9.5 DIRITTI DI PROPRIETÀ INTELLETTUALE

Il presente documento è di proprietà di Lottomatica Holding S.r.l. che si riserva tutti i diritti ad esso relativi. Relativamente alla proprietà di altri dati ed informazioni si applicano le leggi vigenti.

9.6 DICHIARAZIONI E GARANZIE

9.6.1 Dichiarazioni e garanzie della CA

Il QTSP è responsabile sugli obblighi contenuti nel presente documento e nei servizi contrattualmente erogati verso i sottoscrittori.

Il QTSP è responsabile:

- Per la conformità con le procedure dichiarate nel presente documento;
- Per la copertura dei danni derivanti da non conformità rispetto a quanto contenuto nei termini e condizioni del servizio accettato dal sottoscrittore, attraverso le coperture specificate nel presente documento.

Il QTSP non è responsabile:

- Per la copertura dei danni derivanti dal non rispetto da parte del sottoscrittore di quanto contenuto nei termini e condizioni del servizio accettato dallo stesso.

Stante la natura e le limitazioni d'uso del servizio di firma elettronica qualificata, il QTSP sta avviando un piano per migliorare l'accessibilità del servizio per le persone disabili, attraverso soluzioni di Web Content Accessibility.

Il QTSP è responsabile sugli obblighi richiamati dall'Art.32 del CAD (Obblighi del titolare e del prestatore di Servizi di firma elettronica qualificata).

9.6.2 Dichiarazioni e garanzie della RA

Il QTSP attraverso i servizi erogati dalla RA, è responsabile sulla compliance dei requisiti contenuti nel presente documento.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Dichiarazione del RAO

L'operatore RAO attenendosi alle istruzioni ricevute da Lottomatica Holding S.r.l. dichiara quanto segue:

1. Di essersi attenuto alle istruzioni ricevute da Lottomatica Holding S.r.l. per effettuare le attività di cui è incaricato;
2. Di aver fornito al Titolare, in modo compiuto e chiaro, tutte le informazioni sulle procedure di certificazione e sui requisiti tecnici per accedervi nonché le ulteriori informazioni necessarie all'utilizzo del Servizio, di essersi assicurato che lo stesso abbia compreso le procedure per il corretto utilizzo del Servizio, e gli obblighi che assumerà relativamente alla protezione della chiave privata e di quanto previsto nelle Condizioni Generali del Servizio, e nei Documenti descrittivi del Servizio di Lottomatica Holding S.r.l.;
3. Di aver svolto le attività di identificazione e di registrazione con modalità tali e nel rispetto degli adempimenti previsti dalla normativa antiriciclaggio (D.Lgs. 231/2007 e ss. mm. e relativa normativa di attuazione) e dal Regolamento UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito "Regolamento"), avendo verificato che il documento di identità presentato dal Titolare è in corso di validità e non presenta segni tali da far dubitare della sua autenticità;
4. Di aver svolto le attività di registrazione in coerenza con i documenti esibiti dal Titolare e nel rispetto delle norme del Regolamento;
5. Di aver avvisato il Titolare che l'emissione del certificato richiesto è subordinato alla esattezza e completezza delle informazioni da lui fornite;
6. Di aver informato il Titolare in merito alle modalità di trattamento dei suoi dati personali descritte nell'Informativa sul trattamento dei dati personali resagli disponibile, ai sensi dell'art. 13 del Regolamento, da Lottomatica Holding S.r.l. – in qualità di titolare del trattamento dei dati personali - prima della sottoscrizione della presente richiesta e delle condizioni generali del servizio e disponibile sul portale <https://ca.firmadigitale.lottomaticaitalia.it>.

Dichiarazione del Master-RAO

L'operatore Master-RAO attenendosi alle istruzioni ricevute da Lottomatica Holding S.r.l. dichiara quanto segue:

1. Di essersi attenuto alle istruzioni ricevute da Lottomatica Holding S.r.l. per effettuare le attività di cui è incaricato;
2. Di aver fornito al Titolare, in modo compiuto e chiaro, tutte le informazioni sulle procedure di certificazione e sui requisiti tecnici per accedervi nonché le ulteriori informazioni necessarie all'utilizzo del Servizio, di essersi assicurato che lo stesso abbia compreso le procedure per il corretto utilizzo del Servizio, e gli obblighi che assumerà relativamente alla protezione della chiave privata e di quanto previsto nelle Condizioni Generali del Servizio, e nei Documenti descrittivi del Servizio di Lottomatica Holding S.r.l.;
3. Di aver svolto le attività di identificazione e di richiesta di registrazione con modalità tali e nel rispetto degli adempimenti previsti dalla normativa antiriciclaggio (D.Lgs. 231/2007 e ss. mm. e

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

relativa normativa di attuazione) e dal Regolamento UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito "Regolamento"), avendo verificato che il documento di identità presentato dal Titolare è in corso di validità e non presenta segni tali da far dubitare della sua autenticità;

- Di aver svolto le attività di richiesta di registrazione in coerenza con i documenti esibiti dal Titolare e nel rispetto delle norme del Regolamento;
- Di aver avvisato il Titolare che l'emissione del certificato richiesto è subordinato alla esattezza e completezza delle informazioni da lui fornite;
- Di aver informato il Titolare in merito alle modalità di trattamento dei suoi dati personali descritte nell'Informativa sul trattamento dei dati personali resagli disponibile, ai sensi dell'art. 13 del Regolamento, da Lottomatica Holding S.r.l. – in qualità di titolare del trattamento dei dati personali - prima della sottoscrizione della presente richiesta e delle condizioni generali del servizio e disponibile sul portale <https://ca.firmadigitale.lottomaticaitalia.it>.

9.6.3 Dichiarazioni e Garanzie del sottoscrittore

Dichiarazione del RAO

Il titolare RAO in fase di accettazione:

- Attesta la veridicità e l'esattezza dei dati inseriti nelle presenti Condizioni Generali, assumendosi ogni responsabilità ai sensi e per gli effetti dell'art. 46 del D.P.R. 445 del 28 dicembre 2000;
- Conferma che i dati utilizzati per la registrazione al Servizio di firma elettronica qualificata sono esatti e veritieri e sono stati correttamente registrati.
- Conferma la propria volontà di voler attivare ed utilizzare il servizio che ha richiesto a Lottomatica Holding S.r.l.
- Dichiara di aver ricevuto le informazioni necessarie all'utilizzo del servizio e di aver consultato i Documenti descrittivi del servizio pubblicati sul portale <https://ca.firmadigitale.lottomaticaitalia.it>.
- Dichiara di essere stato informato da Lottomatica Holding S.r.l., in qualità di Titolare del Trattamento, circa le finalità primarie e la base giuridica del trattamento dei propri dati personali, tramite apposita informativa privacy resa, ai sensi dell'art. 13 del Regolamento UE 2016/679 (di seguito il "Regolamento" o anche "GDPR"), in fase di identificazione. La suddetta informativa privacy è, comunque, sempre disponibile sul sito <https://ca.firmadigitale.lottomaticaitalia.it>;
- Dichiara di aver ricevuto e letto, prima della sottoscrizione, i termini e le condizioni di utilizzo del Servizio di firma elettronica qualificata e di approvare quanto riportato nelle Condizioni Generali e nei documenti descrittivi del Servizio, avendo pienamente compreso le modalità di utilizzo del servizio e gli effetti giuridicamente vincolanti che derivano dal suo utilizzo.

Dichiarazione del Master-RAO

Il titolare Master-RAO in fase di accettazione:

- Attesta la veridicità e l'esattezza dei dati inseriti nelle presenti Condizioni Generali, assumendosi ogni responsabilità ai sensi e per gli effetti dell'art. 46 del D.P.R. 445 del 28 dicembre 2000;
- Conferma che i dati utilizzati per la registrazione al Servizio di firma elettronica qualificata sono esatti e veritieri e sono stati correttamente registrati.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

3. Conferma la propria volontà di voler attivare ed utilizzare il servizio che ha richiesto a Lottomatica Holding S.r.l.
4. Dichiaro di aver ricevuto le informazioni necessarie all'utilizzo del servizio e di aver consultato i Documenti descrittivi del servizio pubblicati sul portale <https://ca.firmadigitale.lottomaticaitalia.it>.
5. Dichiaro di essere stato informato da Lottomatica Holding S.r.l., in qualità di Titolare del Trattamento, circa le finalità primarie e la base giuridica del trattamento dei propri dati personali, tramite apposita informativa privacy resa, ai sensi dell'art. 13 del Regolamento UE 2016/679 (di seguito il "Regolamento" o anche "GDPR"), in fase di identificazione. La suddetta informativa privacy è, comunque, sempre disponibile sul sito <https://ca.firmadigitale.lottomaticaitalia.it>;
6. Dichiaro di aver ricevuto e letto, prima della sottoscrizione, i termini e le condizioni di utilizzo del Servizio di firma elettronica qualificata e di approvare quanto riportato nelle Condizioni Generali e nei documenti descrittivi del Servizio, avendo pienamente compreso le modalità di utilizzo del servizio e gli effetti giuridicamente vincolanti che derivano dal suo utilizzo.

Dichiarazione del B2B

Il titolare B2B in fase di accettazione:

1. Attesta la veridicità e l'esattezza dei dati inseriti nelle presenti Condizioni Generali, assumendosi ogni responsabilità ai sensi e per gli effetti dell'art. 46 del D.P.R. 445 del 28 dicembre 2000;
2. Conferma che i dati utilizzati per la registrazione al Servizio di firma elettronica qualificata sono esatti e veritieri e sono stati correttamente registrati.
3. Conferma la propria volontà di voler attivare ed utilizzare il servizio che ha richiesto a Lottomatica Holding S.r.l.
4. Dichiaro di aver ricevuto le informazioni necessarie all'utilizzo del servizio e di aver consultato i Documenti descrittivi del servizio pubblicati sul portale <https://ca.firmadigitale.lottomaticaitalia.it>.
5. Dichiaro di essere stato informato da Lottomatica Holding S.r.l., in qualità di Titolare del Trattamento, circa le finalità primarie e la base giuridica del trattamento dei propri dati personali, tramite apposita informativa privacy resa, ai sensi dell'art. 13 del Regolamento UE 2016/679 (di seguito il "Regolamento" o anche "GDPR"), in fase di identificazione. La suddetta informativa privacy è, comunque, sempre disponibile sul sito <https://ca.firmadigitale.lottomaticaitalia.it>;
6. Dichiaro di aver ricevuto e letto, prima della sottoscrizione, i termini e le condizioni di utilizzo del Servizio di firma elettronica qualificata e di approvare quanto riportato nelle Condizioni Generali e nei documenti descrittivi del Servizio, avendo pienamente compreso le modalità di utilizzo del servizio e gli effetti giuridicamente vincolanti che derivano dal suo utilizzo.

Dichiarazione dell'Utente Interno/Utente firma automatica

L'Utente Interno/Utente firma automatica in fase di accettazione:

1. Attesta la veridicità e l'esattezza dei dati inseriti nelle presenti Condizioni Generali, assumendosi ogni responsabilità ai sensi e per gli effetti dell'art. 46 del D.P.R. 445 del 28 dicembre 2000;
2. Conferma che i dati utilizzati per la registrazione al Servizio di firma elettronica qualificata sono esatti e veritieri e sono stati correttamente registrati.
3. Conferma la propria volontà di voler attivare ed utilizzare il servizio che ha richiesto a Lottomatica Holding S.r.l.
4. Dichiaro di aver ricevuto le informazioni necessarie all'utilizzo del servizio e di aver consultato i Documenti descrittivi del servizio pubblicati sul portale <https://ca.firmadigitale.lottomaticaitalia.it>.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

5. Dichiara di essere stato informato da Lottomatica Holding S.r.l., in qualità di Titolare del Trattamento, circa le finalità primarie e la base giuridica del trattamento dei propri dati personali, tramite apposita informativa privacy resa, ai sensi dell'art. 13 del Regolamento UE 2016/679 (di seguito il "Regolamento" o anche "GDPR"), in fase di identificazione. La suddetta informativa privacy è, comunque, sempre disponibile sul sito <https://ca.firmadigitale.lottomaticaitalia.it>;
6. Dichiara di aver ricevuto e letto, prima della sottoscrizione, i termini e le condizioni di utilizzo del Servizio di firma elettronica qualificata e di approvare quanto riportato nelle Condizioni Generali e nei documenti descrittivi del Servizio, avendo pienamente compreso le modalità di utilizzo del servizio e gli effetti giuridicamente vincolanti che derivano dal suo utilizzo.

9.7 DICHIARAZIONI DI GARANZIA

Il QTSP esclude proprie responsabilità connesse con quanto seguente:

- Sottoscrittori che non rispettano quanto contenuto nei termini e condizioni d'uso del servizio;
- Mancata erogazione di informazioni o obblighi di comunicazione dovuti a problemi associati alla disponibilità della rete Internet, o parte di essa;
- Vulnerabilità o errori associati agli algoritmi di crittografia utilizzati per compliance normativa.

9.8 LIMITE DI RESPONSABILITÀ

Il QTSP Lottomatica Holding S.r.l. non sarà in alcun modo responsabile per quanto di seguito indicato:

- Danni di qualsiasi natura, diretti e/o indiretti, o pregiudizi da chiunque patiti causati da:
 - a) Comunicazione da parte del Titolare di informazioni incomplete, false o contenenti errori, per le quali il QTSP non abbia dichiarato o non sia altrimenti obbligato ad effettuare specifici controlli e verifiche;
 - b) Manomissioni o interventi sul Servizio effettuati da parte del Titolare ovvero da terzi non autorizzati dal QTSP;
 - c) Impossibilità di fruire del Servizio determinata da una interruzione, totale o parziale, dei servizi di terminazione delle chiamate o di trasporto dei dati forniti da operatori di telecomunicazioni, esclusivamente per fatti non imputabili al QTSP;
 - d) Erroneo utilizzo di codici identificativi da parte del Titolare;
 - e) Ritardi, interruzioni, errori o malfunzionamenti del Servizio non imputabili al QTSP o derivanti dall'errata utilizzazione del Servizio da parte del Titolare;
 - f) Impiego del Servizio al di fuori di previsioni normative vigenti;
 - g) Mancata comunicazione di informazioni che il Titolare avrebbe dovuto comunicare al QTSP e/o all'Incaricato in virtù degli obblighi previsti dal Contratto;
 - h) Violazione di obblighi che, in virtù di quanto previsto dal presente documento ovvero dalle vigenti disposizioni di legge, sono posti a carico del Titolare;
 - i) Danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti, nella misura in cui avrebbero potuto essere evitati o limitati dai Titolari mediante un corretto utilizzo del Servizio.

Ad eccezione dei casi previsti dalla legge applicabile, Lottomatica Holding S.r.l. non sarà in nessun caso responsabile per i danni diretti e/o danni indiretti e/o consequenziali (ivi inclusi a mero titolo esemplificativo e non esaustivo, perdita di profitto, perdita di produttività, spese generali, mancati guadagni, perdita di informazioni e qualunque altra perdita economica) subiti dal Titolare a seguito e/o in occasione dell'utilizzo del Servizio e dovuti a malfunzionamento del Servizio non imputabile a Lottomatica Holding S.r.l..

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

Fermo restando quanto precede, la responsabilità complessiva di Lottomatica Holding S.r.l. è limitata al risarcimento dei danni diretti e/o danni indiretti e/o consequenziali nei casi di dolo, colpa o negligenza, nei limiti di indennizzo previsti nei cap.9.2 e 9.2.1.

9.9 INDENNITÀ

La copertura delle indennità associate ai danni a tutte le parti (Titolari, Terzi Interessati, Destinatari), è garantita nel presente CPS nella misura stabilita da quanto specificato nel cap. 9.2.1.

9.10 DURATA E CESSAZIONE DEL SERVIZIO

9.10.1 Durata

La durata del servizio è allineata alla durata del termine di durata dei certificati emessi dal QTSP (rif. par. 6.3.2).

9.10.2 Risoluzione

In caso di violazione anche di uno soltanto degli obblighi che gravano sul Titolare, il Contratto relativo al servizio si intenderà automaticamente risolto ai sensi e per gli effetti di cui all'art. 1456 c.c., con contestuale revoca dei certificati emessi, fatta salva ogni eventuale azione di rivalsa nei riguardi dei responsabili delle violazioni.

Il Contratto relativo al servizio si intenderà, altresì, automaticamente risolto, in tutte le ipotesi di revoca del certificato.

Il QTSP ha diritto di recedere in qualsiasi momento dal Contratto relativo al servizio dandone comunicazione al Titolare con un preavviso di 10 (dieci) giorni e, conseguentemente, di revocare i certificati emessi.

9.10.3 Effetti della cessazione

Con il termine "cessazione", si intende il processo attraverso il quale il QTSP cessa la propria attività di Prestatore di Servizi Fiduciari Qualificati.

Il QTSP pubblica nel CPS i dettagli delle informazioni connesse con le procedure di cessazione, per effetto del quale il certificato di CA viene revocato insieme a tutti i certificati in quel momento validi.

9.11 NOTIFICHE E COMUNICAZIONI CON GLI UTENTI

Tutte le comunicazioni di carattere generale, e quelle eventualmente a carattere urgente, sono comunicate dal QTSP attraverso il **Piattaforma del QTSP**.

Tutte le notifiche a carattere personale (emissione certificato, cambio di stato, ecc.), sono notificate ai sottoscrittori attraverso comunicazione inoltrata tramite e-mail personale, confermata dal titolare al momento della registrazione.

9.12 MODIFICHE AL CPS

Il QTSP si riserva il diritto di modificare i termini inclusi nel presente CPS in caso di:

- Modifica di norme;
- Modifiche a requisiti di sicurezza;
- Varie ed eventuali.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

In casi eccezionali le eventuali modifiche possono essere intraprese con effetto immediato.

9.12.1 Procedure per la diffusione del CPS

Il QTSP revisiona il presente CPS su base annuale.

Al documento modificato viene associata una nuova versione, e viene modificata la data di validità tenendo in considerazione eventuali processi connessi con l'approvazione dello stesso.

Il nuovo documento, così modificato, viene inviato anche all'organo di vigilanza, per l'Italia, l'AgID.

Una volta approvato viene pubblicato sul **Piattaforma del QTSP**

Il QTSP può accettare osservazioni connesse con quanto pubblicato, attraverso l'indirizzo e-mail:

firmaqualificata@pec.lottomatica.it → dal **01 Marzo 2021** l'indirizzo di riferimento sarà **caigt@pec.it**

9.12.2 Meccanismi di notifica e tempi

Il QTSP notifica alle parti interessate la pubblicazione della nuova versione del documento, come specificato nel cap. 9.12.1.

9.12.3 Circostanze sotto le quali è necessario il cambio di OID

Il QTSP rilascia una nuova versione nel caso di integrazione degli OID specificati nel presente CPS.

9.13 RISOLUZIONE DELLE CONTROVERSIE

Il QTSP mira ad una soluzione pacifica e negoziata delle controversie derivanti dall'erogazione dei propri servizi.

Tuttavia, ogni controversia che dovesse insorgere fra le Parti in relazione al Contratto relativo al servizio sarà di competenza esclusiva del foro di Roma. Nel caso in cui il Titolare sia qualificato quale consumatore ai sensi del Codice del Consumo (D.Lgs. n.206 del 2005), le controversie inerenti il presente Contratto relativo al Servizio saranno di competenza del giudice del luogo di residenza o domicilio del Titolare qualificato come Consumatore.

9.14 LEGGI GOVERNATIVE

Il QTSP opera in ogni momento in accordo con le leggi Italiane ed Europee in materia.

9.15 COMPLIANCE CON LEGGI IN VIGORE

Il presente CPS è conforme con le seguenti normative in vigore:

- REGULATION (EU) No 910/2014 of the EUROPEAN PARLIAMENT AND OF THE
- COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [27];
- DPCM 22 Febbraio 2013 [24];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [1];
- Regolamento (UE) 2016/679 (GDPR) [25].

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

10 RIFERIMENTI

- [1] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- [2] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;
- [3] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [4] ETSI EN 319 411-2 v2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; (Replaces ETSI TS 101 456).
- [5] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- [6] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; (Replaces ETSI TS 102 280).
- [7] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (Replaces ETSI TS 101 861).
- [8] ETSI EN 319 412-4 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- [9] ETSI EN 319 412-5 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- [10] ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- [11] ISO/IEC 15408-2002 "Information Technology - Methods and Means of a Security Evaluation Criteria for IT Security".
- [12] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".
- [13] IETF RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999.
- [14] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.
- [15] IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.
- [16] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.
- [17] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- [18] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.
- [19] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks.
- [20] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.
- [21] Common Criteria for Information Technology Security Evaluation, Part 1 - 3.

| | | | | |
|---|-----------|---|-----------|------------------|
|  | Tipologia | REGISTRAZIONE | Codice | LTIS-05-00001/18 |
| | Titolo | QTSP SERVIZI QUALIFICATI DI CERTIFICAZIONE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY | Revisione | 5.0 |
| | | | Data | 08/02/2021 |
| Classificazione: Pubblico | | | | |

- [22] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.
- [23] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.
- [24] DPCM 22 Febbraio 2013.
- [25] Regolamento nazionale Applicabile e Regolamento EU n.2016/679.
- [26] Codice dell'Amministrazione Digitale (CAD) d.lgs. n.82 7 marzo 2005, e successive modificazioni (d.lgs. 179/2016).
- [27] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.