

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

QTSP

SERVIZI QUALIFICATI DI MARCATURA TEMPORALE CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

INDICE

1	INTRODUZIONE	6
1.1	PANORAMICA	6
1.2	NOME DEL DOCUMENTO ED IDENTIFICAZIONE	6
1.2.1	Identificazione del documento	6
1.3	PKI PARTICIPANTS	7
1.3.1	Provider	7
1.3.2	Client	7
1.4	UTILIZZO DELLA MARCATURA	8
1.5	AMMINISTRAZIONE DELLA POLICY	8
1.5.1	Amministrazione del documento	8
1.5.2	Responsabilità dell'Idoneità	8
1.5.3	Procedure di approvazione del documento	8
1.6	DEFINIZIONI ED ACRONIMI	9
1.6.1	Definizioni	9
1.6.2	Acronimi	11
2	PUBBLICAZIONE	13
2.1	REPOSITORY	13
2.2	PUBBLICAZIONE DI INFORMAZIONI DI CERTIFICAZIONE	13
2.2.1	Pubblicazione di informazioni sul QTSP	13
2.3	FREQUENZA DI PUBBLICAZIONE	13
2.3.1	Frequenza di pubblicazione dei Termini e Condizioni	13
2.3.2	Frequenza di pubblicazione dei certificati	13
2.4	REGISTRAZIONE DELLE MARCHE GENERATE	13
3	CERTIFICATO DELLA TSU E MARCATURA	14
3.1	IDENTIFICAZIONE DELL'UTENTE	14
3.2	CERTIFICATO DELLA TSU	14
3.3	LA MARCATURA (TIMESTAMP)	14
3.3.1	La richiesta di marcatura (timestamp request)	15
3.3.2	La marcatura (timestamp response)	15
3.4	ACCURATEZZA DELLA MARCATURA	16
3.5	SINCRONIZZAZIONE	17
3.5.1	Gestione del leap second	17
3.5.2	Management dell'ora legale	17
3.6	VALIDAZIONE DELLA MARCATURA	17
3.7	DISPONIBILITÀ DEL SERVIZIO DI MARCATURA	17
3.8	RILASCIO DI MARCATURE NON QUALIFICATE	17
3.9	GESTIONE DELLE CHIAVI DELLA TSU	17
3.10	PROTOCOLLO DI MARCATURA	17
4	REQUISITI CICLO DI VITA DEL CERTIFICATO	18
4.1	COPPIA DI CHIAVI E UTILIZZO DEL CERTIFICATO	18

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

4.1.1	Chiave privata del sottoscrittore e utilizzo del certificato.....	18
4.1.2	Parti interessate – Chiave pubblica e utilizzo del certificato.....	18
5	FACILITY, MANAGEMENT, E CONTROLLI OPERATIVI	19
5.1	CONTROLLI FISICI	19
5.1.1	Locazione del sito e Caratteristiche	19
5.1.2	Accessi fisici	19
5.1.3	Alimentazione ed Aria condizionata	20
5.1.4	Esposizione all'acqua	21
5.1.5	Prevenzione e protezione antincendio	21
5.1.6	Media Storage.....	22
5.1.7	Disposizioni sulla dismissione di apparati.....	22
5.1.8	Off-Site Backup	22
5.2	CONTROLLI PROCEDURALI	22
5.2.1	Ruoli	23
5.2.2	Numero di persone richieste per task	23
5.2.3	Identificazione ed Autenticazione per Ruoli	23
5.2.4	Ruoli che richiedono segregazione.....	23
5.3	CONTROLLO DEL PERSONALE.....	24
5.3.1	Qualifiche, esperienze e chiarezza dei requisiti	24
5.3.2	Procedure di verifica di Background	24
5.3.3	Requisiti di formazione	25
5.3.4	Frequenza di aggiornamento.....	25
5.3.5	Sanzioni su azioni non autorizzate.....	25
5.3.6	Requisiti sui consulenti.....	25
5.3.7	Documentazione fornita al personale.....	26
5.4	PROCEDURE DI AUDIT	26
5.4.1	Tipologie di eventi memorizzati.....	26
5.4.2	Frequenza dei processi di Audit	27
5.4.3	Periodo di retention dei log di Audit	27
5.4.4	Protezione dei log di audit	27
5.4.5	Procedure di backup log di Audit	27
5.4.6	Sistemi di raccolta eventi di Audit	28
5.4.7	Verbosità di Notifica degli errori.....	28
5.4.8	Vulnerability Assessment	28
5.5	ARCHIVIAZIONE DEI RECORD	28
5.6	TSA KEY CHANGEOVER.....	28
5.7	COMPROMISSIONE E DISASTER RECOVERY	29
5.7.1	Incident e procedure di gestione della compromissione.....	29
5.7.2	Computing Resources, Software, e/o dati corrotti.....	30
5.7.3	Procedure di compromissione chiave privata	30
5.7.4	Capacità di Business Continuity in caso di disastro	30
5.8	CESSAZIONE DELLA ATTIVITÀ	30
6	CONTROLLI TECNICI DI SICUREZZA	30
6.1	GENERAZIONE ED INSTALLAZIONE COPPIA DI CHIAVI	30
6.1.1	Generazione coppia di chiavi.....	31
6.1.2	Dimensione delle chiavi	31
6.1.3	Parametri di generazione chiavi e controllo della qualità.....	31
6.1.4	Scopi del Key Usage (vedi campo Key Usage X.509 v3).....	32

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

6.2	PROTEZIONE DELLA CHIAVE PRIVATA E CONTROLLI SULLA COMPONENTE CRITTOGRAFICA	32
6.2.1	Standard e controlli dei Moduli crittografici	32
6.2.2	Controllo segregazione chiave privata (MofN)	32
6.2.3	Key Escrow della chiave privata	32
6.2.4	Backup chiave privata	33
6.2.5	Archiviazione della chiave	33
6.2.6	Trasferimento della chiave privata da/per il modulo crittografico	33
6.2.7	Memorizzazione della chiave privata sul modulo crittografico	33
6.2.8	Metodi di attivazione della chiave privata	33
6.2.9	Metodo di disattivazione della chiave privata	34
6.2.10	Metodo di distruzione della chiave privata	34
6.2.11	Valutazione del modulo crittografico	34
6.3	ALTRI ASPETTI SULLA GESTIONE DELLE CHIAVI	34
6.3.1	Archiviazione chiave pubblica	34
6.3.2	Validità del certificato e delle chiavi	35
6.4	DATI DI ATTIVAZIONE	35
6.4.1	Generazione ed installazione dati di attivazione	35
6.4.2	Protezione dei dati di attivazione	35
6.5	CONTROLLI DI SICUREZZA SU COMPUTER	35
6.5.1	Requisiti Tecnici di sicurezza specifici su sistemi IT	35
6.5.2	Valutazione della Sicurezza dei sistemi IT	36
6.6	CICLO DI VITA DEI CONTROLLI TECNICI	36
6.6.1	Controllo dei sistemi di sviluppo	36
6.6.2	Controlli di gestione della sicurezza	36
6.6.3	Ciclo di vita dei controlli di sicurezza	37
6.7	CONTROLLI DI SICUREZZA DELLA RETE	37
6.8	TIME-STAMPING	38
7	CERTIFICATI, CRL, E PROFILI OCSP	39
7.1	PROFILO DI CERTIFICATO	39
7.1.1	Specifica X509	39
7.1.2	Estensioni di certificato	39
7.1.2.1	Gestione in continuità dei certificati di Lottomatica S.p.A.	41
7.1.2.2	Gestione in continuità dei certificati di Lottomatica Holding a seguito di cambio di P.IVA	41
7.1.3	Object Identifier Algoritmi	42
7.1.4	Composizione del nome	42
7.1.5	Vincoli sul nome	42
7.1.6	Object Identifier policy di certificato	42
7.1.7	Utilizzo dell'estensione Policy Constraint	42
7.1.8	Sintassi e semantica dei qualificatori della Policy	43
7.1.9	Gestione della semantica per estensioni di certificate policy critiche	43
7.2	PROFILO CRL	43
7.2.1	Versione	43
7.2.2	Specifiche delle estensioni della CRL	43
8	COMPLIANCE AUDIT E ALTRI ASSESSMENTS	45
8.1	FREQUENZE O REQUISITI DI ASSESSMENT	45
8.2	IDENTITÀ/QUALIFICA DEGLI ASSESSOR	45
8.3	INDIPENDENZA DELL'ASSESSOR	46

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

8.4	ARGOMENTI COPERTI DALL' ASSESSMENT	46
8.5	AZIONI INTRAPRESE IN CASO DI NON CONFORMITÀ.....	46
8.6	COMUNICAZIONE DEI RISULTATI	46
9	ASPETTI ECONOMICO LEGALI.....	47
9.1	TARiffe.....	47
9.2	RESPONSABILITÀ FINANZIARIE	47
9.2.1	Copertura assicurativa.....	47
9.3	CONFIDENZIALITÀ DELLE INFORMAZIONI DI BUSINESS	47
9.4	TUTELA DEI DATI PERSONALI	47
9.4.1	Modalità di protezione dei dati.....	48
9.5	DIRITTI DI PROPRIETÀ INTELLETTUALE	52
9.6	DICHIARAZIONI E GARANZIE.....	52
9.6.1	Dichiarazioni e garanzie della TSA.....	52
9.7	DICHIARAZIONI DI GARANZIA.....	53
9.8	LIMITE DI RESPONSABILITÀ	53
9.9	INDENNITÀ.....	54
9.10	DURATA E CESSAZIONE DEL SERVIZIO.....	54
9.10.1	Durata	54
9.10.2	Risoluzione.....	54
9.10.3	Effetti della cessazione.....	54
9.11	NOTIFICHE E COMUNICAZIONI CON GLI UTENTI.....	54
9.12	MODIFICHE AL CPS.....	54
9.12.1	Procedure per la diffusione del CPS	55
9.12.2	Meccanismi di notifica e tempi	55
9.12.3	Circostanze sotto le quali è necessario il cambio di OID	55
9.13	RISOLUZIONE DELLE CONTROVERSIE	55
9.14	LEGGI GOVERNATIVE.....	55
9.15	COMPLIANCE CON LEGGI IN VIGORE	55
10	RIFERIMENTI	57

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

1 INTRODUZIONE

Questo documento contiene le specifiche relative alla policy per l'emissione di marcature qualificate (Certificate Policy – in seguito CP) e descrive i processi e le metodologie nonché i processi operativi (Certification Practice Statement – in seguito CPS) utilizzati da Lottomatica Holding S.r.l. per l'erogazione del servizio di marcatura qualificata, nell'ambito della sua funzione di prestatore di servizi fiduciari qualificati.

Tale metodologia è descritta nel presente documento (in seguito, documento).

Tale documento è compatibile ai requisiti espressi nel regolamento europeo 910/2014 – eIDAS [28], 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 del sistema di Marcatura Temporale contiene un "insieme di regole che specificano l'usabilità di un servizio di Marcatura temporale per una comunità e / o di una classe di applicazioni con requisiti comuni di sicurezza".

Il presente documento è costituito da 9 capitoli che contengono i requisiti di sicurezza, i processi e le pratiche definite dal QTSP da seguire durante l'erogazione del servizio.

Il presente documento definisce requisiti di base relativi alla Marcatura Temporale ed in particolare per la TSA e per la TSU. La maniera attraverso cui questi requisiti sono rispettati, la descrizione dettagliata dei metodi menzionati sono inclusi nel presente documento rilasciato da Lottomatica Holding S.r.l..

1.2 NOME DEL DOCUMENTO ED IDENTIFICAZIONE

1.2.1 Identificazione del documento

Questo documento è denominato "*QTSP Servizi Qualificati di Marcatura Temporale – Certification Practice Statement e Certificate Policy*" ed è caratterizzato dal codice documento: LTIS-05-00002/18. La versione e il livello di rilascio sono identificabili sul frontespizio in calce ad ogni pagina.

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..

1-3-76-49

La marcatura temporale rilasciata in accordo con il presente documento è conforme con lo standard seguente:

- ETSI EN 319 421 [25]
BTSP: a best practices policy for time-stamp
OID: itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1)
best-practices-ts-policy (1);

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- DPCM 22 febbraio 2013.

Il sopramenzionato OID è incluso nelle marcature rilasciate dal QTSP. Gli OID specifici dell'organizzazione ed utilizzati nel profilo del certificato, sono dettagliati in questo paragrafo.

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

Il presente documento include requisiti specifici relativi a servizi forniti per clienti Italiani, operanti con la legge Italiana in linguaggio Italiano.

Si riporta di seguito l'identificativo univoco del presente documento:

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.
(2)	Lottomatica Holding S.r.l. Time Stamp Authority
(1)	Documenti
(1)	Documenti pubblici
(51)	Lottomatica Holding S.r.l. Autorità di Certificazione servizi di Marcatura Temporale Qualificata – Certification Practice Statement and Certificate Policy

1.3 PKI PARTICIPANTS

1.3.1 Provider

Il provider di servizio di marcatura qualificata è un prestatore di servizi fiduciari qualificato (d'ora in avanti QTSP), che emette data e ora all'interno nell'ambito di un servizio di fiducia qualificato.

Il QTSP eroga il servizio attraverso una componente di CA (TSA) che emette certificati per le componenti TSU, e le componenti TSU che erogano fisicamente le marcature temporali.

Le informazioni anagrafiche di contatto di Lottomatica Holding S.r.l. sono riportate in 1.5.1.

1.3.2 Client

Con il termine client si intende l'insieme delle applicazioni che utilizzano il servizio di marcatura fornito dal QTSP.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

1.4 UTILIZZO DELLA MARCATURA

Attraverso l'apposizione di una marcatura temporale, è possibile associare ad un documento informatico una data ed un orario giuridicamente certi ed opponibili ai terzi in conformità alla vigente normativa europea e nazionale.

Il servizio descritto nel presente documento viene utilizzato da Lottomatica Holding S.r.l. per l'integrazione di una marcatura temporale qualificata nell'ambito della firma elettronica qualificata emessa da Lottomatica Holding S.r.l. e/o comunque nell'ambito di 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.

1.5 AMMINISTRAZIONE DELLA POLICY

1.5.1 Amministrazione del documento

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

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

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 CP-CPS.

I servizi di certificazione e le relative procedure riportate nel presente CP-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 del documento

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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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, Art 3 [28]:

- 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;
- 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 (1);
- 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;

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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;
- 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 colleghino altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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

QTSP	Qualified Trust Service Provider – Prestatore di Servizi Fiduciari Qualificato
CA	Certification Authority
HSM	Hardware Security Module
HA	High Availability (Alta affidabilità)
CRL	Certificate Revocation List
OCSP	Online Certificate Protocol Status
TSA	Time Stamp Authority
TSU	Time Stamp Unit
QSCD	Qualified Signature Creation Device
RAO	Registration Authority Officer
RAA	Registration Authority Administrator
RA	Registration Authority (Autorità di Registrazione)
PKI	PKI Public Key Infrastructure - Infrastruttura a chiave pubblica. Con questo termine si intende una serie di accordi che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un utente, oltre che di associare una chiave pubblica ad un utente, normalmente per mezzo di software distribuito in modo coordinato su diversi sistemi. Le chiavi pubbliche tipicamente assumono la forma di certificati digitali.
PIN	Personal Identification Number – Numero di identificazione personale
PUK	Personal Unlock Key – Chiave personale di sblocco
SN	Serial Number.
SSL	Secure Socket Layer – Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica.
WS	Web Service
ICT	Information and Communication Technology
VPN	Virtual Private Network
PdV	Punti vendita
CAB	Conformity Assessment Body – Organismo di valutazione conformità

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

AgID Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari
 CAD Codice dell'Amministrazione Digitale
 HTTP HyperText Transfer Protocol
 OID Object Identifier
 OTP One Time Password

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

2 PUBBLICAZIONE

2.1 REPOSITORY

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

2.2 PUBBLICAZIONE DI INFORMAZIONI DI CERTIFICAZIONE

I certificati della TSA sono altresì disponibili sul **Portale Del QTSP**.

Certificati della TSA

Il QTSP pubblica le informazioni relative ai propri certificati attraverso:

- I documenti CPS;
- Sul **Portale Del QTSP**.

Certificati dei TSU

Il QTSP pubblica le informazioni relative allo stato del certificato dei TSU attraverso la lista di revoca (CRL).

2.2.1 Pubblicazione di informazioni sul QTSP

Il QTSP pubblica le condizioni e le policy contrattuali elettronicamente sul **Portale Del QTSP**.

Nuovi documenti afferenti il servizio sono divulgati sul sito 14 giorni dell'entrata in vigore.

I documenti in vigore sono disponibili sul sito, oltre a tutte le versioni precedenti di tutti documenti.

2.3 FREQUENZA DI PUBBLICAZIONE

2.3.1 Frequenza di pubblicazione dei Termini e Condizioni

La pubblicazione di nuove versioni del presente documento è conforme con le modalità descritte nel paragrafo 9.12.

2.3.2 Frequenza di pubblicazione dei certificati

Il QTSP pubblica il certificato di root TSA prima dell'avvio operativo.

2.4 REGISTRAZIONE DELLE MARCHE GENERATE

In aderenza con quanto specificato nel Titolo IV del DPCM 22 Febbraio 2013, art. 53, "Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal QTSP."

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

3 CERTIFICATO DELLA TSU E MARCATURA

3.1 IDENTIFICAZIONE DELL'UTENTE

Il servizio di marcatura temporale qualificata erogato dal QTSP viene utilizzato secondo le limitazioni descritte nel par. 1.4.

A tale scopo, non vi è una identificazione dell'utente finale, ma una erogazione del servizio a fronte di meccanismi di autenticazione gestiti dai sistemi IT che implementano la suddetta contrattualizzazione.

3.2 CERTIFICATO DELLA TSU

Al fine di assicurare integrità ed autenticità della chiave pubblica:

- La chiave pubblica della TSU è pubblicata come Certificato; dal certificato relativo alla coppia di chiavi utilizzate per la validazione temporale deve essere possibile individuare il sistema di validazione temporale;
- Il certificato della TSU è rilasciato dalla TSA del QTSP in accordo con quanto specificato nello standard ETSI EN 319 411-1 [3];
- Il certificato della TSU che rilascia la marcatura qualificata in accordo con il regolamento 910/2014/EU [28], deve essere emesso da una CA (TSA) che eroga servizio in accordo con quanto specificato nello standard ETSI EN 319 411-2 [4];
- La TSU può rilasciare le marcature solo quando possiede un certificato per la verifica della marcatura, la cui relativa firma è verificata attraverso il riconoscimento della catena di certificati che punta alla TSA;
- Al fine di limitare il numero di marcature, il certificato della TSU viene rinnovato entro un limite massimo di mesi 3 (DPCM 22 febbraio 2013 art 49 comma 2);
- Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale sono utilizzate chiavi di certificazione appositamente generate.

3.3 LA MARCATURA (TIMESTAMP)

L'operazione di marcatura (o timestamp):

- Deve essere conforme allo standard IETF RFC 3161 [13] e allo standard ETSI EN 319 422 [26];
- È rilasciato in un ambiente sicuro e deve contenere un riferimento orario corretto;
- L'orologio interno della TSU utilizzato per il rilascio del timestamp deve essere connesso ad una fonte accurata;
- Il riferimento orario fornito nel timestamp deve essere conforme al valore di tempo fornito da UTC, e la differenza non deve superare la precisione indicata nella policy e nel timestamp stesso;
- La TSU non deve erogare il timestamp allorquando la precisione rilevata al momento della elaborazione della marcatura, non superi il valore dichiarato;
- Le chiavi private utilizzate per la certificazione del timestamp, non devono essere utilizzate per altri scopi;
- La TSU deve rifiutare ogni tentativo di richiesta di marcatura qualora sia superata la durata delle chiavi di sottoscrizione.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

3.3.1 La richiesta di marcatura (timestamp request)

Il client di timestamp supporta la richiesta di marcatura in accordo con quanto specificato nello standard IETF RFC 3161 [13] section 2.4.1.

In particolare, è raccomandato l'utilizzo dei seguenti campi:

- reqPolicy;
- nonce;
- certReq.

Il QTSP supporta l'utilizzo di qualsiasi estensione.

Il QTSP accetta gli algoritmi di hash nella richiesta di timestamp conformi a quanto specificato nello standard ETSI TS 119 312 [10]. Nel dettaglio:

sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }
--------	--

Struttura della richiesta di marcatura

La richiesta di marcatura richiede i seguenti campi:

- Version; la versione è la v1 specificata in IETF RFC 3161, e contenente il valore 1;
- MessageImprint: il dato oggetto di marcatura, e contenente;
 - Hashing Algorithm, l'OID dell'algoritmo di hash utilizzato nell'hash;
 - Hash, il valore dell'hash applicato al documento originale;
- Certificate Request: impostato a FALSE.

Valori opzionali:

- reqPolicy, riferimento alla Policy per la quale è richiesta la marcatura;
- nonce, un valore di tipo 64-bit integer, che serve per comprovare l'unicità del timestamp. Se utilizzato, il response contenuto nel timestamp deve contenere lo stesso valore;
- extensions, campo utilizzato per specificare informazioni di estensione.

3.3.2 La marcatura (timestamp response)

Il QTSP supporta il timestamp response conformemente a quanto specificato nello standard IETF RFC 3161 [13] capitolo 2.4.2, con i seguenti requisiti aggiuntivi:

- "accuracy";
- "nonce".

Nel caso di utilizzo del campo "nonce" nella richiesta di timestamp, la marcatura di risposta deve contenere lo stesso valore contenuto nella richiesta.

Il QTSP utilizza policy legate all'uso di algoritmi crittografici e di lunghezza delle chiavi di firma dei timestamp conformi a quanto specificato nello standard ETSI TS 119 312 [10].

Nel dettaglio, gli algoritmi di hash supportati sono:

sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }
--------	--

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

Struttura del timestamp

La struttura del timestamp include i seguenti campi:

- Status, l'informazione di stato inerente il rilascio, in accordo con lo standard pubblico IETF RFC 3161, cap. 2.4.2;

Valori opzionali:

- Timestamp token, valorizzato nel campo status valga 0 o 1, altrimenti non è incluso nel response.

Struttura del timestamp token

La struttura del timestamp token include la firma della TSU ed è in accordo con quanto specificato nello standard pubblico IETF RFC 3161, cap. 2.4.2.

Sono inclusi nel TST:

- Version, la versione è la v1 specificata in IETF RFC 3161, e contenente il valore 1;
- Policy, specifica la policy a cui la marcatura risulta compliance. Il valore contenuto deve essere quello corrispondente a quanto indicato nel reqPolicy della request corrispondente;
- MessageImprint, i dati di marcatura contenente lo stesso valore della request;
- SerialNumber, seriale univoco di marcatura, rilasciato dalla TSU (massimo 160 bit di lunghezza);
- GenTime: orario di rilascio del timestamp in formato UTC; il riferimento orario deve essere in accordo con il valore di precisione dichiarato in 3.4;
- Accuracy, accuratezza della marcatura, in accordo con il valore di precisione dichiarato in 3.4.

Valori opzionali:

- Nonce, un valore di tipo 64-bit integer, che serve per comprovare l'unicità del timestamp. Se utilizzato, il response contenuto nel timestamp deve contenere lo stesso valore;
- Ordering, valore di default: FALSE;
- TSA, il valore della subject contenuto nel certificato della TSU che ha rilasciato la marcatura;
- Extensions, il QTSP utilizza la presente estensione per indicare lo stato Qualificato del timestamp in accordo con il regolamento eIDAS, come segue:

Qualified Certificate Statements – non critical

OID: 1.3.6.1.5.5.7.1.3

The extension contains one statement: "esi4-qtstStatement-1"

3.4 ACCURATEZZA DELLA MARCATURA

L'accuratezza contenuta nella marcatura deve essere massimo di 1 secondo.

L'orologio della TSU deve essere protetto da minacce che potrebbero pregiudicarne l'accuratezza.

Il QTSP Time-Stamping deve tenere sotto controllo l'accuratezza dichiarata; se il valore supera il valore di accuratezza dichiarato, il QTSP sospende l'erogazione del servizio.

L'accuratezza dell'orologio del QTSP viene esaminato annualmente.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

3.5 SINCRONIZZAZIONE

La componente TSU è sincronizzata con fonti NTP, come definito all'interno del Piano di Sicurezza del QTSP. La sincronizzazione ha il principale compito di mantenere costante il valore di accuratezza specificato in 3.4.

3.5.1 Gestione del leap second

Il QTSP deve eseguire la sincronizzazione dell'orologio in base alla notifica dell'organo competente rispetto all'occorrenza legata al leap second. L'applicazione dell'orario deve essere modificata all'ultimo minuto del giorno stabilito in base alle specifiche contenute nello standard ETSI 319 421 [25] allegato C, e come definito nella raccomandazione ITU-R TF.460-6 [17].

3.5.2 Management dell'ora legale

L'orario fornito in UTC all'interno del timestamp può essere interpretato da applicazioni client in formato differente, spesso in formato dell'orario locale.

Per questo motivo il QTSP richiede attenzione alle parti interessate, affinché l'orario contenuto nella marcatura erogata dal servizio oggetto del presente documento, sia interpretata come formato UTC.

3.6 VALIDAZIONE DELLA MARCATURA

Durante la verifica della validità della firma elettronica presente nel timestamp, le parti coinvolte devono rispettare quanto specificato nello standard ETSI EN 319 102-1 [8].

Durante la verifica del timestamp:

- Si deve verificare che il timestamp contenuto nel documento, sia riconducibile al certificato rilasciato dalla TSA;
- Si deve verificare la firma sul timestamp;
- Si deve verificare che il timestamp rispetti i requisiti specifici legati alla accuratezza del riferimento orario, ed alla affidabilità del certificato rilasciato QTSP.

3.7 DISPONIBILITÀ DEL SERVIZIO DI MARCATURA

Il QTSP garantisce che la disponibilità dei propri sistemi almeno al 99,7% su base annua, mentre i tempi di fermo dei servizi non può superare 8 ore in ogni caso.

3.8 RILASCIO DI MARCATURE NON QUALIFICATE

Il QTSP non eroga marcature temporali non qualificate.

3.9 GESTIONE DELLE CHIAVI DELLA TSU

Le chiavi di sottoscrizione delle TSU sono gestite in accordo con il DPCM del 22 febbraio 2013, Titolo IV, art. 49.

3.10 PROTOCOLLO DI MARCATURA

Il servizio è esposto unicamente attraverso il protocollo HTTPS. Il canale sicuro è stabilito sulla base del certificato installato sulla TSU. L'accesso al servizio richiede username e password.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

4 REQUISITI CICLO DI VITA DEL CERTIFICATO

4.1 COPPIA DI CHIAVI E UTILIZZO DEL CERTIFICATO

4.1.1 Chiave privata del sottoscrittore e utilizzo del certificato

La chiave privata della TSU deve essere utilizzata esclusivamente per la certificazione della marcatura (timestamp) rilasciata dal servizio, ed è proibito l'utilizzo della stessa per altri scopi. Lottomatica Holding S.r.l. è garante che il documento sottoposto a marcatura temporale, 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].

4.1.2 Parti interessate – Chiave pubblica e utilizzo del certificato

Le parti interessate alla verifica di una marcatura qualificata, devono procedere secondo quanto contenuto nel presente documento con particolare riguardo a quanto seguente:

- Le parti interessate devono verificare la validità e lo stato di revoca del certificato di marcatura;
- Le parti interessate devono validare il certificato verificando opportunamente tutta la catena dei certificati;
- Le parti interessate devono tenere conto delle eventuali limitazioni d'uso indicate nel certificato, e specificate dal presente documento.

Il QTSP rende disponibili servizi per consentire la verifica dei certificati rilasciati.

Il QTSP pubblica altresì un portale (verificatore online) per la convalida di un documento sottoscritto con firma digitale e marcatura temporale, 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, e la relativa marcatura temporale, 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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			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 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. 4.10.2.

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, fonoassorbenti e antisfondamento.

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-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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 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

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

inseriti sia a soffitto che al di sotto del pavimento tecnico con gemme di ripetizione dello stato di funzionamento del singolo sensore.

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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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.

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;
- 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 applica una politica mirata ad assicurare 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 TSA del QTSP;
- Il backup della chiave privata della TSA del QTSP;
- L'attivazione della chiave privata della TSA del QTSP;
- La distruzione della chiave privata della TSA 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:

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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;

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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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:

- 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;
- 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 [27] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

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 sui 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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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:

- 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 il Lottomatica Holding S.r.l. intrattiene rapporti contrattuali ed economici.

5.4 PROCEDURE DI AUDIT

Al fine di mantenere un ambiente IT sicuro, il QTSP implementa un sistema di gestione degli eventi che copre i sistemi IT coinvolti nella erogazione del servizio.

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 v1.1.1 [4]. Per lo specifico servizio di marcatura qualificata, sono inoltre implementati i controlli specificati nello standard EN 319 421 v2.1.1 cap. 7.7.2 e 7.12 e riportati di seguito:

- Gestione delle chiavi di TSU:
 - Registrazione degli eventi legati al ciclo di vita delle chiavi;
 - Registrazione degli eventi legati al ciclo di vita del certificato.
- Sincronizzazione oraria:
 - Registrazione degli eventi connessi con la sincronizzazione della TSU all'orologio UTC, inclusi gli eventi di ricalibrazione e sincronizzazione;
 - Registrazione degli eventi di perdita di sincronizzazione;
 - Registrazioni degli eventi connessi con la gestione del leap second.

Tutti gli eventi sono memorizzati ed archiviati in accordo con quanto specificato in 5.4.3.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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.

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 è in accordo con quanto specificato nel cap. 7.10 dello standard EN 319 401 v 1.1.1 [28]. In particolare il QTSP garantisce che gli eventi connessi con l'erogazione del servizio, sono memorizzati in una maniera che assicura la protezione della modifica, l'inserimento o la cancellazione delle entry.

I log archiviati sono protetti da backup che assicurano il ripristino a seguito di cancellazione accidentale (o malevola), o perdita del dato.

Opportune regole di protezione assicurano che solo personale in carica può accedere ai dati, o eseguire operazioni di backup o di archiviazione.

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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

5.4.6 Sistemi di raccolta eventi di Audit

Il QTSP adotta sistemi automatizzati che assicurano l'attività di raccolta su base continua.

5.4.7 Verbose di Notifica degli errori

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.

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 (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 ai log è di anni 20.

Il QTSP implementa meccanismi che assicurano:

- Il rispetto sulla conformità della policy di mantenimento dei log;
- Il rispetto dei requisiti di confidenzialità ed integrità dei dati, fornendo procedure a garanzia della verifica della autenticità dei dati;
- Il rispetto dei requisiti sulla disponibilità delle informazioni, garantendo la fruibilità delle stesse nel tempo.

5.6 TSA 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.

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

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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;
- Che le vecchie chiavi ed il relativo certificato sono conservati a termini di legge, garantendo meccanismi di verifica fino alla naturale scadenza degli stessi.

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 documento, 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 che in futuro il riverificarsi 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, 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 [28] gli incidenti di sicurezza sono classificati con 5 livelli di severità:

1. Nessun impatto;
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.

5.7.1 Incident e procedure di gestione della compromissione

Il QTSP ha un business continuity plan 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, anche in situazioni di fault di un sistema o di un apparato.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

5.7.2 Computing Resources, Software, e/o dati corrotti

Il QTSP adotta e mantiene medesimi sistemi HW/SW tra sito A e sito 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 c dello standard ETSI EN 319411-1.

5.7.3 Procedure di compromissione chiave privata

Il QTSP ha un piano di Disaster Recovery che segue in condizioni di emergenza scaturite dalla compromissione della chiave privata.

Il piano d'azione indirizza:

- Le circostanze della compromissione oltre alla revoca della chiave pubblica del QTSP;
- Organizza le notifiche di tutte le parti interessate;
- Cessa immediatamente di usare quella chiave particolare, fornendo una nuova chiave al unità di servizio.

Le informazioni connesse con la revoca del certificato di TSA, vengono pubblicate sul **Portale Del QTSP**.

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.

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, sono coperti da 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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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.

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 TSA;
2. Chiavi di sottoscrizione, destinate ai TSU.

Tutte le chiavi sono generate attraverso un dispositivo di tipo HSM, conforme agli standard di certificazione riportati nel cap. 6.2.1.

Il processo di generazione delle chiavi della TSA è conforme con quanto specificato nello standard EN 319 411 01 v1.2.2 [3], con particolare riferimento ai capitoli 6.5.1, 6.5.2 e 6.5.3.

Il processo di generazione delle chiavi della TSU è conforme con quanto specificato nello standard EN 319 421 v1.1.1 [25], con particolare riferimento al capitolo 7.6.2.

Lottomatica Holding S.r.l. conferma che il processo di generazione delle chiavi viene eseguito conformemente alla regole tecniche rispetto a quanto vigente; in particolare: il processo di generazione delle chiavi della TSA è conforme con quanto specificato nello standard EN 319 411 01 v1.2.2 [3], con particolare riferimento ai capitoli 6.5.1, 6.5.2 e 6.5.3; il processo di generazione delle chiavi della TSU è conforme con quanto specificato nello standard EN 319 421 v1.1.1 [25], con particolare riferimento al capitolo 7.6.2

6.1.2 Dimensione delle chiavi

Il QTSP utilizza policy relative all'uso di algoritmi e di dimensione delle chiavi secondo quanto specificato nello standard ESTSI TS 119 312[10].

In particolare:

- La chiave RSA di root TSA è di lunghezza 4096 bit;
- Le chiavi RSA delle TSU sono di lunghezza 2048 bit.

6.1.3 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 tutte le operazioni di sicurezza effettuate con HSM, con particolare riferimento alla generazione delle chiavi, sono eseguite in conformità rispetto a quanto previsto dal raggiunto traguardo di sicurezza.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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

Il certificato di TSA include i seguenti keyUsage:

- Digital Signature
- Certificate Signing
- Off-line CRL Signing,
- CRL Signing (86)

Il certificato di sottoscrizione rilasciato alla TSU contiene i seguenti Enhanced keyUsage:

- Timestamp.

6.2 PROTEZIONE DELLA CHIAVE PRIVATA E CONTROLLI SULLA COMPONENTE CRITTOGRAFICA

Il QTSP assicura la gestione sicura delle chiavi private prevenendone la pubblicazione, la copia, la cancellazione, la modifica e l'utilizzo non autorizzato.

6.2.1 Standard e controlli dei Moduli crittografici

La TSA presente nella infrastruttura di certificazione, che assicura l'emissione dei certificati di sottoscrizione, la firma della CRL, e le componenti TSU che erogano la marcatura Qualificata, 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.

6.2.3 Key Escrow della chiave privata

Il QTSP non fornisce strumenti di key escrow applicati alla chiave privata della propria TSA, e delle TSU.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

6.2.4 Backup chiave privata

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

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 di sottoscrizione associate alle TSU.

6.2.5 Archiviazione della chiave

Il QTSP non effettua l'archiviazione della chiave privata delle rispettive componenti TSA/TSU.

6.2.6 Trasferimento della chiave privata da/per il modulo crittografico

La chiave privata delle rispettive componenti TSA/TSU del QTSP sono mantenute in modo sicuro attraverso i meccanismi di protezione forniti dall'HSM, coperti dalle certificazioni specificate nel cap. 6.2.1.

La chiave privata delle rispettive componenti TSA/TSU 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.

In caso di trasferimento fisico della chiave privata di TSA, 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

Il QTSP memorizza la chiave privata delle rispettive componenti TSA/TSU utilizzate per i servizi previsti, in accordo con il presente documento, esclusivamente su HSM.

Gli aspetti 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 delle rispettive componenti TSA/TSU del QTSP deve essere attivata in accordo con le procedure e i requisiti definiti nei manuali di prodotto, e con quanto specificato nei documenti di certificazione.

I servizi associati alle chiavi contenute negli HSM, possono essere attivati solo quando quest'ultimi risultano attivi. Le chiavi che consentono l'attivazione degli apparati, sono custodite in maniera sicura e protette da adeguati meccanismi di accesso.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

6.2.9 Metodo di disattivazione della chiave privata

La chiave privata delle rispettive componenti TSA/TSU del QTSP, deve essere disattivata in accordo con le procedure e i requisiti definiti nei manuali di prodotto, e con quanto specificato nei documenti di certificazione.

In particolare, la chiave può essere disattivata:

- Quando gli operatori attuano la procedura di disattivazione della chiave;
- Quando l'erogazione della corrente elettrica è interrotta;
- Quando il device va' in errore.

6.2.10 Metodo di distruzione della chiave privata

TSA Private Keys

La chiave di TSA 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 assicurano 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 viene 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.

TSU Private Keys

La chiave private di sottoscrizione è 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.

6.3 ALTRI ASPETTI SULLA GESTIONE DELLE CHIAVI

6.3.1 Archiviazione chiave pubblica

Il QTSP pubblica su archivio ogni certificato rilasciato dalla propria TSA.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

6.3.2 Validità del certificato e delle chiavi

Certificati e chiavi della TSA

Il periodo di validità del certificato di TSA del QTSP, e della relativa coppia di chiavi, è di 25 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.

Certificati e chiavi della TSU

La validità del certificato di sottoscrizione rilasciato alle componenti TSU:

- Ha validità non superiore a 3 anni, con rinnovo delle chiavi entro un limite massimo di 3 mesi, in conformità al DPCM 22 febbraio 2013 [24];
- 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 TSA del QTSP che lo ha rilasciato.

6.4 DATI DI ATTIVAZIONE

6.4.1 Generazione ed installazione dati di attivazione

La chiave privata delle rispettive componenti TSA/TSU, è protetta in accordo con le procedure specificate nel manuale utente dell'HSM, e con quanto specificato nei documenti di certificazione.

6.4.2 Protezione dei dati di attivazione

Il QTSP definisce misure interne volte ad assicurare che i dati di attivazione delle chiavi private, siano protette da meccanismi di autenticazione e autorizzazione, in maniera da assicurare che solo personale nominato può accedervi.

6.5 CONTROLLI DI SICUREZZA SU COMPUTER

6.5.1 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 319 421 [25] cap. 7.12;

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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.

6.5.2 Valutazione della Sicurezza dei sistemi IT

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.

6.6 CICLO DI VITA DEI CONTROLLI TECNICI

6.6.1 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.

6.6.2 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;

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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 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.

6.6.3 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:

- Verifica le certificazioni di ambito;
- 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 applicato 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;

6.7 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;
- Configurazione 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;

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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 tipologia di servizio offerto.
- 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.

6.8 TIME-STAMPING

Lottomatica Holding S.r.l. garantisce l'integrità e la protezione dei file di log, attraverso la gestione degli stessi in un sistema tipo log management interno all'infrastruttura ICT.

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-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

7 CERTIFICATI, CRL, E PROFILI OCSP

7.1 PROFILO DI CERTIFICATO

Il QTSP dispone di una root TSA destinata alla emissione dei certificati per i servizi di marcatura temporale TSU, ed ai servizi di certificazione connessi.

Il certificato di TSA e il certificato della componente TSU, sono compatibili con i seguenti standard:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks [19];
- RFC 5280 [16];
- RFC 6818 [17];
- ETSI EN 319 421 [25];
- 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 TSA 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 [5]

- Algorithm Identifier

L'OID dell'algoritmo utilizzato per la certificazione del Certificato;

- 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 Value

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:

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

Certificato di root TSA

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 Timestamp Authority"
Validity	25 Anni (scadenza 25 anni dalla data di emissione)
Subject	come 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, CRL Signing, Offline CRL Signing (06)
Authority Information Access	Access Method : On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Certificate Policies (non critico)	OID della policy: 1.3.76.49 Cp: URL: http://ca.firmadigitale.lottomaticaitalia.it/documenti
crlDistributionPoint (non critico)	http://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh2020.crl

Certificato di TSU

Nome	Valore
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 Timestamp Authority"
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" O = "Lottomatica Holding S.r.l." organizationIdentifier : "VATIT-02611940038" CN = TSU <identificativo tsu>

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

Nome	Valore
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-5 QcEuPDS (0.4.0.1862.1.5) https://ca.firmadigitale.lottomaticaitalia.it/documenti/qtsptsapds2020.pdf
enhancedKeyUsage (critica)	Time Stamping (1.3.6.1.5.5.7.3.8)
KeyUsage (critica)	Digital Signature
Authority Information Access REGOLAMENTO (UE) N. 910/2014 <i>ALLEGATO I, h)</i>	Access Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: https://ca.firmadigitale.lottomaticaitalia.it/strumenti/TSAH2020.crt
Certificate Policies (non critico) (ETSI 319 411-1 par.5.3) (ETSI 319 411-2 par.5.3)	OID della policy 0.4.0.2023.1.1 https://ca.firmadigitale.lottomaticaitalia.it/documenti
crlDistributionPoint (non critico)	https://ca.firmadigitale.lottomaticaitalia.it/tsaqtspcrlh2020.crl

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 alle vecchie 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/qtsptsapds.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 seguenti link:

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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/qtsptsapdsh.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

Il QTSP adotta il seguente algoritmo:

- "sha256WithRSAEncryption" (1.2.840.113549.1.1.11).

7.1.4 Composizione del nome

La composizione del nome identificante il distinguish name, viene composto compatibilmente con quanto specificato dagli standard RFC 5280 [16], ETSI EN 319 421 [25], ETSI EN 319 422 [26].

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

Il CN viene specializzato con un progressivo numerico, ed assegnato a ciascun responder (TSU1, TSU2 ecc.).

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, marcata non critica.

7.1.7 Utilizzo dell'estensione Policy Constraint

Non presente.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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 TSA può includere le seguenti estensioni:

- Version
Il valore del campo è "1".
- 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.
The list of the suspended or revoked Certificates with the serial number of the Certificate and with the suspension or revocation time.

Le estensioni obbligatorie che devono essere presenti nella CRL sono:

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- CRL number – non critica

Un numero serial progressivo identificante la singola CRL

LA seguente estensione può essere usata dalla TSA

- expiredCertsOnCRL – non critica

La TSA indica attraverso la presente estensione che i certificati scaduti non sono rimossi dalla CRL (si veda cap 4.10). La notazione è in accordo la la 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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			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 [28], 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 [28];
- DPCM 22 febbraio 2013 [24];
- 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) [3]; 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];
- ETSI EN 319 421-2 v1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [25].

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

Il Lottomatica Holding S.r.l., all'interno dei propri servizi fiduciari qualificati, utilizza componenti certificate. Per quanto concerne la protezione delle chiavi private, il QTSP dichiara che le componenti HSM HW sono idonee per l'implementazione dei servizi Qualificati, in quanto in possesso delle certificazioni di specificate nel cap. 6.2.1.

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

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 [28].

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

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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;
- Non ha relazioni di business con il 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;
- Conformità con il presente documento;
- Adeguatezza dei processi coperti;
- Documentazione;
- Sicurezza fisica;
- Adeguatezza del personale;
- Sicurezza IT;
- Conformità 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;
- Dereghe 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 TSA del QTSP viene pubblicato nelle liste dei Prestatori di Servizi Fiduciari Qualificati.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

9 ASPETTI ECONOMICO LEGALI

9.1 TARIFFE

Il servizio di Marcatura Temporale Qualificato 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") [27] 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 [27], 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-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			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

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 [27] e dall'applicabile normativa nazionale Italiana di coordinamento sulla tutela dei dati personali nonché nel rispetto dei provvedimenti emessi dal Garante per la protezione dei dati personali.

La terminologia utilizzata nel presente capitolo è conforme a quella adottata dal Regolamento [27]. 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 [27]. 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);

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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;
- 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 [27].

Definizione e identificazione di "Dati personali"

Ai sensi dell'Art. 4 n. 1) del Regolamento [27], 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 [27] 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 [27], in particolare:

- Agli interessati sono fornite le necessarie informazioni ai sensi dell'Art. 13 del Regolamento [27] (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 [27], 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 [27].

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

Applicazione del Regolamento

Adempimenti generali

Dal punto di vista generale, il QTSP:

- Predispone, 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, il cui accesso è consentito ad un ristretto numero di dipendenti Lottomatica Holding S.r.l. autorizzati a svolgere 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

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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 [27];
- 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

- 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 [27] 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;

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- 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 [27] e dall'applicabile normativa Italiana di coordinamento sulla tutela dei dati personali potranno essere previste a livello contrattuale tra il 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 [27], 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. Il titolare del certificato mantiene tutti gli eventuali diritti sui propri marchi commerciali (brand name) e sul proprio nome di dominio.

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 TSA

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.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

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, 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).

9.7 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

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-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			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 documento nella misura stabilita da quanto specificato nel cap. 9.2.1.

9.10 DURATA E CESSAZIONE DEL SERVIZIO

9.10.1 Durata

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. La durata del servizio è allineata al 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 presente documento 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

Il QTSP comunica con i propri sottoscrittori utilizzando il **Portale Del QTSP**.

9.12 MODIFICHE AL CPS

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

- Modifica di norme;
- Modifiche a requisiti di sicurezza;

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- Varie ed eventuali;

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 documento 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'AgID.

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

Il QTSP può accettare osservazioni connesse con quanto pubblicato, attraverso l'indirizzo email **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 relativo CP.

9.13 RISOLUZIONE DELLE CONTROVERSIE

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

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 documento 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 [28];
- DPCM 22 Febbraio 2013;
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [1];

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. (Replaces ETSI TS 102 023) [25];
- ETSI EN 319 422 V1.1.1 (2016-03) [26]; Electronic Signatures and Infrastructures (ESI); Timestamping protocol and time-stamp to ken profiles (Replaces ETSI TS 101 861) [26];
- Regolamento EU n.2016/679 [27].

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			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] MSZ/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 3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)
- [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.
- [22] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

	Tipologia	REGISTRAZIONE	Codice	LTIS-05-00002/18
	Titolo	QTSP SERVIZI QUALIFICATI DI MARCATURA TEMPORALE - CERTIFICATION PRACTICE STATEMENT E CERTIFICATE POLICY	Revisione	3.0
			Data	08/02/2021
Classificazione: Pubblico				

- [23] CEN CWA 14169: Secure signature-creation devices "EAL 4+", March 2004.
- [24] DPCM 22 febbraio 2013.
- [25] ETSI TS 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI);
Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- [26] ETSI TS 319 422 V1.1.1 (2016-03) [26]; Electronic Signatures and Infrastructures (ESI);
Time-stamping protocol and time-stamp token profiles.
- [27] Regolamento nazionale Applicabile e Regolamento EU n.2016/679
- [28] 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.