

Manuale Operativo

Servizio qualificato e non qualificato di validazione temporale

CODICE DOCUMENTO	ICERT-INDI-TSA
VERSIONE	2.7
DATA	16/09/2021

SOMMARIO

1	INTRODUZIONE	6
1.1	Quadro generale	6
1.2	Nome ed identificativo del documento	6
1.3	Partecipanti e responsabilità	7
1.3.1	Time Stamping Authority	7
1.3.2	Richiedente	7
1.3.3	Utente	8
1.3.4	Autorità	8
1.4	Uso del servizio di marca temporale	8
1.4.1	Usi consentiti	8
1.4.2	Usi non consentiti	8
1.5	Amministrazione del Manuale Operativo	8
1.5.1	Contatti	8
1.5.2	Soggetti responsabili dell'approvazione del Manuale Operativo	9
1.5.3	Procedure di approvazione	9
1.6	Definizioni e acronimi	9
1.6.1	Definizioni	9
1.6.2	Acronimi e abbreviazioni	11
2	PUBBLICAZIONE E CONSERVAZIONE	13
2.1	Conservazione della marca temporale	13
2.2	Pubblicazione delle informazioni sulla certificazione	13
2.2.1	Pubblicazione del manuale operativo	13
2.2.2	Pubblicazione della chiave pubblica per la verifica della marcatura temporale	13
2.2.3	Pubblicazione delle liste di revoca e sospensione	13
2.3	Periodo o frequenza di pubblicazione	13
2.3.1	Frequenza di pubblicazione del manuale operativo	13
2.4	Controllo degli accessi agli archivi pubblici	14
3	IDENTIFICAZIONE E AUTENTICAZIONE	15
3.1	Denominazione	15
3.1.1	Tipi di nomi	15
3.1.2	Necessità che il nome abbia un significato	15
3.1.3	Anonimato e pseudonimia dei richiedenti	15
3.1.4	Regole di interpretazione dei tipi di nomi	15
3.1.5	Univocità dei nomi	15
3.2	Convalida iniziale dell'identità	15
3.3	Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati	15
3.4	Identificazione e autenticazione per le richieste di revoca o sospensione	15
4	OPERATIVITÀ	16
4.1	Richiesta di emissione o di verifica di marca temporale	16
4.1.1	Chi può richiedere l'emissione o la verifica di una marca temporale	16
4.1.2	Processo di registrazione e responsabilità	16
4.2	Elaborazione della richiesta	16
4.3	Emissione della marca temporale	16
4.4	Accettazione del certificato	17
4.5	Uso della coppia di chiavi e del certificato	17
4.6	Rinnovo del certificato	17
4.7	Rimissione del certificato	17
4.8	Modifica del certificato	17
4.9	Revoca e sospensione del certificato	17
4.9.1	Motivi per la revoca	18
4.9.2	Chi può richiedere la revoca	18
4.9.3	Procedure per richiedere la revoca	18
4.9.4	Periodo di grazia della richiesta di revoca	18
4.9.5	Tempo massimo di elaborazione della richiesta di revoca	18
4.9.6	Requisiti per la verifica della revoca	18

4.9.7	Frequenza di pubblicazione della CRL.....	18
4.9.8	Latenza massima della CRL.....	19
4.9.9	Servizi online di verifica dello stato di revoca del certificato.....	19
4.10	Servizi riguardanti lo stato del certificato.....	19
4.10.1	Caratteristiche operative.....	19
4.10.2	Disponibilità del servizio.....	19
4.11	Disdetta dai servizi della TSA.....	19
4.12	Deposito presso terzi e recovery della chiave.....	19
5	MISURE DI SICUREZZA E CONTROLLI.....	20
5.1	Sicurezza fisica.....	20
5.1.1	Posizione e costruzione della struttura.....	20
5.1.2	Accesso fisico.....	21
5.1.3	Impianto elettrico e di climatizzazione.....	21
5.1.4	Prevenzione e protezione contro gli allagamenti.....	22
5.1.5	Prevenzione e protezione contro gli incendi.....	22
5.1.6	Supporti di memorizzazione.....	22
5.1.7	Smaltimento dei rifiuti.....	23
5.1.8	Off-site backup.....	23
5.2	Controlli procedurali.....	23
5.2.1	Ruoli chiave.....	23
5.3	Controllo del personale.....	23
5.3.1	Qualifiche, esperienze e autorizzazioni richieste.....	23
5.3.2	Procedure di controllo delle esperienze pregresse.....	23
5.3.3	Requisiti di formazione.....	23
5.3.4	Frequenza di aggiornamento della formazione.....	24
5.3.5	Frequenza nella rotazione dei turni di lavoro.....	24
5.3.6	Sanzioni per azioni non autorizzate.....	24
5.3.7	Controlli sul personale non dipendente.....	24
5.3.8	Documentazione che il personale deve fornire.....	24
5.4	Gestione del giornale di controllo.....	25
5.4.1	Tipi di eventi memorizzati.....	25
5.4.2	Frequenza di trattamento e di memorizzazione del giornale di controllo.....	25
5.4.3	Periodo di conservazione del giornale di controllo.....	25
5.4.4	Protezione del giornale di controllo.....	25
5.4.5	Procedure di backup del giornale di controllo.....	25
5.4.6	Sistema di memorizzazione del giornale di controllo.....	25
5.4.7	Notifica in caso di identificazione di vulnerabilità.....	25
5.4.8	Valutazioni di vulnerabilità.....	26
5.5	Archiviazione dei verbali.....	26
5.5.1	Tipi di verbali archiviati.....	26
5.5.2	Protezione dei verbali.....	26
5.5.3	Procedure di backup dei verbali.....	26
5.5.4	Requisiti per la marcatura temporale dei verbali.....	26
5.5.5	Sistema di memorizzazione degli archivi.....	26
5.5.6	Procedure per ottenere e verificare le informazioni contenute negli archivi.....	26
5.6	Sostituzione della chiave privata della TSU.....	26
5.7	Compromissione della chiave privata della TSA e disaster recovery.....	27
5.7.1	Procedure per la gestione degli incidenti.....	27
5.7.2	Corruzione delle macchine, del software o dei dati.....	27
5.7.3	Procedure in caso di compromissione della chiave privata della TSA.....	27
5.7.4	Erogazione dei servizi in caso di disastri.....	27
5.8	Cessazione del servizio di validazione temporale.....	27
6	CONTROLLI DI SICUREZZA TECNOLOGICA.....	29
6.1	Generazione della coppia di chiavi di marcatura temporale della TSU.....	29
6.1.1	Algoritmo e lunghezza delle chiavi.....	29
6.1.2	Controlli di qualità e generazione della chiave pubblica.....	29
6.2	Protezione della chiave privata e controlli ingegneristici del modulo crittografico.....	29
6.2.1	Controlli e standard del modulo crittografico.....	29
6.2.2	Controllo di più persone della chiave privata di TSA.....	29
6.2.3	Backup della chiave privata di TSA.....	30

6.2.4	Memorizzazione della chiave privata su modulo crittografico	30
6.2.5	Metodo di attivazione della chiave privata	30
6.2.6	Metodo per distruggere la chiave privata della TSA	30
6.3	Dati di attivazione della chiave privata	30
6.4	Controlli sulla sicurezza informatica	30
6.4.1	Requisiti di sicurezza specifici dei computer	30
6.5	Operatività sui sistemi di controllo	31
6.6	Controlli di sicurezza della rete	31
7	FORMATO	32
7.1	Formato del certificato della TSU	32
7.1.1	Numero di versione	32
7.1.2	Estensioni del certificato	32
7.1.3	OID dell'algoritmo di firma	32
7.1.4	Forme di nomi	32
7.1.5	Vincoli ai nomi	32
7.1.6	OID del certificato	32
7.1.7	Formato e contenuto della marca temporale	32
7.2	Formato della CRL del certificato di marcatura	33
7.2.1	Numero di versione	33
7.3	Formato dell'OCSP	33
7.3.1	Numero di versione	33
8	CONTROLLI E VALUTAZIONI DI CONFORMITÀ	34
8.1	Frequenza o circostanze per la valutazione di conformità	34
8.2	Identità e qualifiche di chi effettua il controllo	34
8.3	Rapporti tra InfoCert e CAB	34
8.4	Aspetti oggetto di valutazione	35
8.5	Azioni in caso di non conformità	35
9	ALTRI ASPETTI LEGALI E DI BUSINESS	36
9.1	Tariffe	36
9.1.1	Tariffe per il rilascio della marca temporale	36
9.1.2	Tariffe per la verifica della marca temporale	36
9.1.3	Tariffe per altri servizi	36
9.1.4	Politiche per il rimborso	36
9.2	Responsabilità finanziaria	36
9.2.1	Copertura assicurativa	36
9.2.2	Garanzia o copertura assicurativa per i soggetti finali	36
9.3	Confidenzialità delle informazioni di business	36
9.3.1	Ambito di applicazione delle informazioni confidenziali	36
9.4	Privacy	37
9.4.1	Programma sulla privacy	37
9.4.2	Dati che sono trattati come personali	37
9.4.3	Trattamento dei dati personali	37
9.4.4	Informativa privacy e consenso al trattamento dei dati personali	37
9.4.5	Divulgazione dei dati a seguito di richiesta da parte dell'autorità	37
9.4.6	Altri motivi di divulgazione	37
9.5	Proprietà intellettuale	38
9.6	Rappresentanza e garanzie	38
9.7	Limitazione di garanzia	38
9.8	Limitazione di responsabilità	38
9.9	Indennizzi	39
9.10	Termine e risoluzione	39
9.10.1	Termine	39
9.10.2	Risoluzione	39
9.10.3	Effetti della risoluzione	40
9.11	Canali di comunicazione ufficiali	40
9.12	Revisione del Manuale Operativo	40
9.12.1	Storia delle revisioni	41
9.12.2	Procedure di revisione	43
9.12.3	Periodo e meccanismo di notifica	43
9.13	Risoluzione delle controversie	43

9.14	Foro competente.....	43
9.15	Legge applicabile.....	43
9.16	Standard di riferimento	44
9.17	Disposizioni varie.....	44
9.18	Altre disposizioni.....	45
Appendice A.....		46
	Time stamp root "InfoCert Time Stamping Authority 2"	46
	Qualified time stamp root "Qualified InfoCert Time Stamping Authority 2"	48
	Time stamp root "InfoCert Time Stamping Authority 3"	52
Avvertenza		55

INDICE DELLE FIGURE

Figura 1 - ubicazione Data Center InfoCert e sito della Disaster Recovery	21
---	----

1 INTRODUZIONE

1.1 Quadro generale

Il presente manuale ha lo scopo di descrivere le regole e le procedure operative adottate dalla struttura di certificazione digitale di InfoCert per l'erogazione del servizio fiduciario qualificato e non qualificato di validazione temporale secondo la norma eIDAS.

InfoCert eroga il servizio di validazione temporale di documenti informatici, siano essi firmati digitalmente ovvero non firmati.

In generale, il servizio di marcatura temporale consente di stabilire l'esistenza di un documento informatico prima di un certo istante temporale, associando all'evidenza informatica ricavata dal documento, una data e ora proveniente da una fonte temporale certificata. Un'evidenza informatica è sottoposta a validazione temporale nel momento in cui si ha la generazione di una marca temporale ad essa associata: la marca temporale è una struttura di dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento di tempo (data e ora).

La marca temporale viene firmata ed emessa da un prestatore di servizi fiduciari che fornisce sistemi di marcatura temporale (Time Stamping Authority (TSA)) che certifica le chiavi di un sistema fidato (Time Stamp Unit (TSU)) al quale gli utenti indirizzano le loro richieste secondo necessità; chiunque abbia richiesto e conservato una marca temporale per un certo documento potrà, in seguito, dimostrare che tale documento effettivamente esisteva alla data/ora riportate nella marca firmata da quella catena di certificazione TSU/TSA.

In particolare, la validazione temporale di un documento firmato digitalmente consente di verificare e considerare valida la firma digitale apposta anche quando il certificato del sottoscrittore risulti scaduto o revocato, purché l'assegnazione della marca temporale al documento sia stata effettuata durante il periodo di validità del certificato medesimo.

Il servizio fornito da InfoCert è conforme alla policy BTSP come definita in ETSI319421 [2] identificata dall'OID.

itu-t(0)	identified-organization(4)	etsi(0)	time-stamp-	0.4.0.2023.1.1
policy(2023)	policy-identifiers(1)	best-practices-ts-policy	(1)	

1.2 Nome ed identificativo del documento

Questo documento è denominato "Servizio qualificato e non qualificato di validazione temporale – Manuale Operativo" ed è caratterizzato dal codice documento: **ICERT-INDI-TSA**. La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.

Al documento è associato l'*object identifier* (OID) **1.3.76.36.1.1.40**. Tale OID identifica:

InfoCert	1.3.76.36
Certification-service-provider	1.3.76.36.1

Certificate-policy	1.3.76.36.1.1
Manuale-operativo-servizio qualificato di validazione temporale	1.3.76.36.1.1.40
Manuale-operativo-servizio non qualificato di validazione temporale (certificati per TSU non InfoCert)	1.3.76.36.1.1.41
Manuale-operativo-servizio non qualificato di validazione temporale	1.3.76.36.1.1.42

Inoltre, tutti i certificati rispettano le raccomandazioni della della Determinazione AgID n. 121/2019, in vigore dal 5 luglio 2019 e contengono un ulteriore elemento PolicyIdentifier con valore agIDcert (OID 1.3.76.16.6) nel campo CertificatePolicies (OID 2.5.29.32)

1.3 Partecipanti e responsabilità

1.3.1 Time Stamping Authority

La **Time Stamping Authority** è il soggetto terzo e fidato che eroga il servizio di validazione temporale.

InfoCert è il prestatore di servizi fiduciari (**TSA**) che eroga il servizio qualificato e non qualificato di validazione temporale (TSU) operando in conformità al Regolamento eIDAS [1] e agli standard ETSI (European Telecommunication Standard Institute).

I dati completi dell'organizzazione che svolge la funzione di CA sono i seguenti:

Denominazione sociale	InfoCert – Società per azioni Società soggetta a direzione e coordinamento di Tinexta S.p.A.
Sede legale	Piazza Sallustio n.9, 00187, Roma (RM)
Sede operativa	Via Marco e Marcelliano n.45, 00147, Roma (RM)
Rappresentante legale	Danilo Cattaneo In qualità di Amministratore Delegato
N. di telefono	06 836691
N. Iscrizione Registro Imprese	Codice Fiscale 07945211006
N. partita IVA	07945211006
Sito web	https://www.infocert.it

1.3.2 Richiedente

Il **Richiedente** è la persona fisica o giuridica a cui viene erogata la marcatura temporale e che stipula il contratto con InfoCert.

1.3.3 Utente

È il soggetto che riceve un documento informatico cui è apposta marca temporale e che fa affidamento sulla validità della marca medesima per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

1.3.4 Autorità

1.3.4.1 Agenzia per l'Italia Digitale - AgID

L'Agenzia per l'Italia Digitale (**AgID**) è l'organismo di vigilanza sui prestatori di servizi fiduciari, ai sensi dell'articolo 17 del Regolamento eIDAS. In tale veste, AgID effettua la vigilanza sui prestatori di servizi fiduciari qualificati stabiliti nel territorio italiano al fine di garantirne la rispondenza ai requisiti stabiliti dal Regolamento.

1.3.4.2 Organismo di valutazione della conformità - Conformity Assessment Body

L'organismo di valutazione della conformità (**CAB**, acronimo di Conformity Assessment Body) è un organismo accreditato secondo quanto previsto dal Regolamento eIDAS, che è competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificati e dei servizi fiduciari qualificati da esso prestati alle normative e agli standard applicabili.

1.4 Uso del servizio di marca temporale

1.4.1 Usi consentiti

Le marche temporali emesse da InfoCert, secondo le modalità indicate dal presente manuale operativo, sono qualificate ai sensi del Regolamento eIDAS.

Il certificato emesso dalla TSA sarà usato per verificare la marca.

InfoCert mette a disposizione per la verifica delle marche il prodotto GoSign scaricabile dal sito InfoCert. Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.

1.4.2 Usi non consentiti

È vietato l'utilizzo fuori dai limiti e dai contesti specificati nel Manuale Operativo e nei contratti.

1.5 Amministrazione del Manuale Operativo

1.5.1 Contatti

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. Domande, reclami, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.

Responsabile del Servizio di Certificazione Digitale

Piazza Luigi da Porto n.3

35131 Padova

Telefono: 06 836691

Fax: 06 23328861

Call Center Firma Digitale: consultare il link <https://help.infocert.it/contatti/>

Web: <https://www.firma.infocert.it>

e-mail: firma.digitale@legalmail.it

1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

Questo Manuale Operativo viene verificato dal Responsabile della Sicurezza e delle policies, dal Responsabile della Privacy, dal Responsabile del Servizio di Certificazione, dall'Ufficio Legale e dall'Area di Consulenza e approvato dal management aziendale.

1.5.3 Procedure di approvazione

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2015.

Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

1.6 Definizioni e acronimi

1.6.1 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal Regolamento eIDAS [1] e dal CAD [ii.] si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Termine	Definizione
CAB - Conformity Assessment Body (Organismo di valutazione della conformità)	Organismo accreditato a norma del Regolamento eIDAS come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificati e dei servizi fiduciari qualificati da esso prestati. Redige il CAR.
Certificato di firma elettronica	Un attestato elettronico che collega i dati di convalida di una firma elettronica ad una TSU.
Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dalla TSU per firmare una marca temporale (cfr CAD [2])
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la marca temporale.
Convalida	Il processo di verifica e conferma della validità di una marca temporale.
Dati di convalida	Dati utilizzati per convalidare marca temporale.
Digest (impronta)	Impronta del messaggio dopo l'applicazione di un algoritmo di hash.
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (cfr eIDAS [1]).

Termine	Definizione
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dalla TSU per emettere una marca temporale.
Lista dei certificati revocati o sospesi [Certificate Revocation List - CRL]	È una lista di certificati che sono stati resi “non validi” prima della loro naturale scadenza. L’operazione è chiamata revoca se definitiva, sospensione se temporanea. Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla CRL, che viene quindi pubblicata nel registro pubblico.
Manuale operativo [certificate practice statement]	Il Manuale Operativo definisce le procedure che il TSP applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall’Autorità di vigilanza e quelle della letteratura internazionale.
Marca temporale (time-stamp)	Dati in forma elettronica che connettono altri dati elettronici con un’evidenza temporale dimostrando che questi dati esistevano in quel momento.
Online Certificate Status Protocol (OCSP)	Protocollo definito dallo IETF nella RFC 6960, consente alle applicazioni di verificare la validità del certificato in maniera più veloce e puntuale rispetto alla CRL, di cui condivide i dati.
PKCS#10	Acronimo di Public Key Cryptography Standards, è un insieme di standard per la crittografia a chiave pubblica sviluppati dai Laboratori RSA: definiscono la sintassi del certificato digitale e dei messaggi crittografati, in particolare il PKCS#10 definisce la struttura della richiesta per la certificazione della chiave pubblica di una coppia di chiavi asimmetriche.
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 (cfr eIDAS [1]).
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 (cfr eIDAS [1])
Revoca o sospensione di un certificato	È l’operazione con cui la CA annulla la validità del certificato prima della naturale scadenza.
Servizio fiduciario	Un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: <ul style="list-style-type: none"> 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 (cfr eIDAS [1]).
Servizio fiduciario qualificato	Un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento (cfr eIDAS [1]).
SHA-256	La sigla SHA sta per Secure Hash Algorithm, è una funzione crittografica utilizzate per calcolare l’hash o digest o impronta. 256 è il numero di bit del messaggio risultante.
Tempo Universale Coordinato [Coordinated Universal Time]	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.
Validazione temporale elettronica	Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento (cfr eIDAS [1]).
Validazione temporale elettronica qualificata	Una validazione temporale elettronica che soddisfa i requisiti di cui all’articolo 42 del Regolamento eIDAS (cfr eIDAS [1])

Termine	Definizione
X.509	Standard per la definizione della struttura del formato dei certificati digitali di chiave pubblica. Definisce, inoltre, le caratteristiche di un'Infrastruttura a Chiave Pubblica (PKI).

1.6.2 Acronimi e abbreviazioni

Acronimo	
AgID	Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari
BTSP	Best practices Time-Stamp Policy - cfr ETSI319421
CA	Certification Authority
CAB	Conformity Assessment Body – Organismo di valutazione della conformità
CAD	Codice dell'Amministrazione Digitale
CAR	Conformity Assessment Report – Relazione di valutazione della conformità
CC	Common Criteria
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
eIDAS	Electronic Identification and Signature Regulation
ETSI	European Telecommunications Standards Institute
HSM	Hardware Secure Module: è un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smartcard, ma con superiori caratteristiche di memoria e di performance
ISO	International Organization for Standardization: fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione
LDAP	Lightweight Directory Access Protocol: protocollo utilizzato per accedere al registro dei certificati
OID	Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia
PEC	Posta Elettronica Certificata
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica): insieme di risorse, processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un soggetto, nonché di associare una chiave pubblica a un soggetto
RFC	Request for Comment: documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico, posto in valutazione della comunità da parte degli estensori
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SSCD – QSSCD	Secure Signature Creation Device: dispositivo per la creazione di una

Acronimo	
	<p>firma elettronica.</p> <p>Qualified Secure Signature Creation Device: dispositivo qualificato per la creazione di una firma elettronica.</p>
TSA	Time-Stamping Authority: prestatore di servizi fiduciari che utilizza uno o più sistemi di emissione di marca temporale – cfr ETSI319421
TST	Time-Stamp Token: termine usato nella pubblicistica internazionale per la marca temporale
TSU	Time-Stamping Unit: insieme di hardware e software gestito come un unico sistema di marcatura temporale composto di una sola chiave attiva – cfr ETSI319421
TSP	Trust Service Provider vd. Prestatore di servizi fiduciari.
UTC	Coordinated Universal Time (Tempo coordinato universale) come definito in ITU-R TF.460-6 (2000) – cfr ETSI319421
X509	Standard ITU-T per le PKI

2 PUBBLICAZIONE E CONSERVAZIONE

2.1 Conservazione della marca temporale

Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per venti anni.

2.2 Pubblicazione delle informazioni sulla certificazione

2.2.1 Pubblicazione del manuale operativo

Il presente Manuale Operativo, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative alla TSA previste dalla legge sono pubblicate presso l'elenco dei certificatori (al link <https://eidas.agid.gov.it/TL/TSL-IT.xml>) e presso il sito web della Certification Authority (cfr. § 1.5.1).

2.2.2 Pubblicazione della chiave pubblica per la verifica della marcatura temporale

È garantita l'integrità e l'autenticità della chiave pubblica del server TSU in quanto distribuita tramite l'emissione di un certificato di chiave pubblica:

- Viene generata la richiesta di certificato da parte del personale autorizzato e inoltrata alla CA InfoCert dedicata alla certificazione di chiavi di marcatura temporale.
- La CA genera il certificato.

Il formato del certificato di marcatura temporale, contenente la chiave pubblica della TSU, è conforme a quanto specificato in ETSI319422 [iii]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa eIDAS e italiana.

La chiave pubblica utilizzata dalla TSU è distribuita tramite il certificato.

2.2.3 Pubblicazione delle liste di revoca e sospensione

Le liste di revoca e di sospensione sono pubblicate nel registro pubblico dei certificati accessibile con protocollo LDAP all'indirizzo: <ldap://ldap.infocert.it> o con protocollo http all'indirizzo <http://crl.infocert.it>. Tale accesso può essere effettuato tramite i software messi a disposizione da InfoCert e/o le funzionalità presenti nei prodotti disponibili sul mercato che interpretano il protocollo LDAP e/o HTTP.

2.3 Periodo o frequenza di pubblicazione

2.3.1 Frequenza di pubblicazione del manuale operativo

Il manuale operativo viene pubblicato con frequenza variabile se sono subentrati dei cambiamenti. Se i cambiamenti sono importanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare

il rapporto di certificazione (*CAR – Conformity Assessment Report*) e il manuale operativo all’Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

2.4 Controllo degli accessi agli archivi pubblici

Le informazioni relative ai certificati pubblicati e i manuali operativi sono pubbliche, la CA non ha messo restrizione all’accesso in lettura e ha attuato tutte le contromisure per scongiurare modifiche/cancellazioni non autorizzate.

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Denominazione

3.1.1 Tipi di nomi

La chiave utilizzata dalla TSU nel certificato è identificata con l'attributo Distinguished Name (DN) che, quindi, deve essere valorizzato e conforme allo standard X500. I certificati vengono emessi secondo gli standard ETSI per l'emissione dei certificati qualificati per validazione temporale.

3.1.2 Necessità che il nome abbia un significato

L'attributo del certificato Distinguished Name (DN) contiene un nome che identifica la TSU utilizzata, il mese e l'anno di emissione.

3.1.3 Anonimato e pseudonimia dei richiedenti

n/a

3.1.4 Regole di interpretazione dei tipi di nomi

InfoCert si attiene allo standard X500.

3.1.5 Univocità dei nomi

L'attributo del certificato Distinguished Name (DN) contiene un nome che identifica la TSU utilizzata, il mese e l'anno di emissione: ogni TSU utilizza un unico certificato.

3.2 Convalida iniziale dell'identità

n/a

3.3 Identificazione e autenticazione per il rinnovo delle chiavi e dei certificati

n/a

3.4 Identificazione e autenticazione per le richieste di revoca o sospensione

n/a

4 OPERATIVITÀ

4.1 Richiesta di emissione o di verifica di marca temporale

4.1.1 Chi può richiedere l'emissione o la verifica di una marca temporale

Il servizio di marcatura temporale prevede di indirizzare le richieste di emissione o di verifica delle marche temporali di documenti informatici al server TSU tramite moduli software opportunamente predisposti.

La richiesta di emissione o di verifica della marca temporale può essere effettuata dal **Richiedente/Utente** utilizzando il software di firma/verifica fornito da InfoCert, che consente di apporre la marca temporale a documenti firmati digitalmente e non, e consente di eseguirne un'immediata verifica.

Il Richiedente può utilizzare un proprio software attraverso protocollo definito in RFC 3161, RFC 5816 e profilato dallo standard ETSI 319 422 utilizzando URL e credenziali concordate con InfoCert.

Una volta accettata e registrata la richiesta ed effettuati gli opportuni controlli di correttezza, il server TSU la elabora, genera la marca temporale e la rinvia al Richiedente/Utente.

Nota: nel sito del certificatore InfoCert sono presenti i software per l'apposizione e la verifica della marca, sia essa associata ad un documento firmato che ad un non firmato.

4.1.2 Processo di registrazione e responsabilità

Nel processo, i diversi attori hanno responsabilità differenziate e concorrono congiuntamente al buon esito dell'emissione:

- Il Richiedente/Utente ha la responsabilità d'inoltrare la richiesta di emissione o di verifica di marca temporale attraverso i moduli software a tal fine predisposti dal prestatore fiduciario InfoCert.
- InfoCert è la responsabile ultima del buon esito del processo di generazione della marca temporale.

4.2 Elaborazione della richiesta

L'elaborazione della richiesta avviene nel modo seguente:

- il Richiedente, mediante le procedure predisposte dalla TSA, invia la richiesta di marcatura temporale del documento informatico, eventualmente prendendone precedente visione, al server TSU;
- la richiesta contiene l'impronta del documento informatico da marcare utilizzando l'algoritmo per l'impronta è SHA-256 (secure hash algorithm 256-bit).

4.3 Emissione della marca temporale

L'emissione della marca temporale viene effettuata in modo automatico da un sistema elettronico sicuro (server TSU), gestito dalla TSA, in grado di:

- calcolare con precisione la data e ora di generazione della marca temporale con riferimento al Tempo Universale Coordinato (UTC);
- generare la struttura di dati contenente le informazioni specificate[iii];
- sottoscrivere digitalmente (nel significato tecnico del termine) detta struttura di dati.

Alla ricezione della richiesta, l'emissione della marca temporale avviene nel modo seguente:

- La TSU, ricevuta la richiesta di marcatura temporale, provvede a generare la struttura prevista dallo standard [iii] che contiene, tra le varie informazioni, l'impronta medesima e la data/ora corrente;
- Il server TSU appone la firma alla struttura dati generata, ottenendo la marca temporale;
- Terminata correttamente la procedura di generazione della marca temporale, quest'ultima viene inviata al Soggetto.

4.4 Accettazione del certificato

n/a

4.5 Uso della coppia di chiavi e del certificato

n/a La coppia di chiavi e il certificato di marcatura sono usati esclusivamente per firmare l'associazione tra data-ora e impronta del documento.

4.6 Rinnovo del certificato

n/a Il certificato non prevede rinnovo.

4.7 Riemissione del certificato

Ogni 3 mesi viene riemesso un nuovo certificato per ogni TSU.

4.8 Modifica del certificato

n/a

4.9 Revoca e sospensione del certificato

La revoca o la sospensione di un certificato ne tolgono la validità prima della scadenza stabilita e rendono non valide le marche apposte successivamente al momento della pubblicazione della revoca. I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dalla TSA che li ha emessi, pubblicata nel registro dei certificati con periodicità prestabilita. La TSA può forzare un'emissione non programmata della CRL in circostanze particolari. L'efficacia della

revoca e della sospensione si ha dal momento di pubblicazione della lista, attestato dalla data apposta alla registrazione dell'evento nel Giornale di Controllo della TSA.

L'informazione sullo stato di revoca rimane disponibile presso la Certification Authority per 20 anni dopo la scadenza del certificato di root TSA tramite l'emissione e conservazione a norma dell'ultima CRL.

4.9.1 Motivi per la revoca

Le condizioni per cui il certificato di marcatura può essere revocato sono:

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
 - sia stato violato il dispositivo sicuro di firma che contiene la chiave;
 - sia venuta meno la segretezza della chiave o del suo codice d'attivazione (PIN);
 - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave.
2. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

4.9.2 Chi può richiedere la revoca

Il certificato può essere revocato o sospeso d'ufficio dalla TSA per i motivi indicati nel § 4.9.1.

4.9.3 Procedure per richiedere la revoca

n/a

4.9.4 Periodo di grazia della richiesta di revoca

Il periodo di grazia della CRL è il periodo di tempo che intercorre tra il momento della pubblicazione da parte della TSA della successiva CRL e il momento in cui scade la CRL corrente. Per non causare disservizi ad ogni parte coinvolta, questo periodo è più lungo del periodo di tempo di cui la TSA ha bisogno per generare e pubblicare una nuova CRL. In questo modo la CRL corrente rimane valida almeno fino a quando non viene sostituita dalla nuova CRL.

4.9.5 Tempo massimo di elaborazione della richiesta di revoca

La richiesta viene elaborata immediatamente appena la TSA ha verificato il motivo di revoca.

4.9.6 Requisiti per la verifica della revoca

n/a

4.9.7 Frequenza di pubblicazione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dalla TSA, e pubblicata nel Registro pubblico. La CRL viene pubblicata in modo programmato ogni ora (emissione ordinaria). La TSA può, in circostanze particolari, forzare un'emissione non programmata della CRL (emissione straordinaria immediata), ad esempio nel caso in cui la revoca o la sospensione di un certificato avvenga per la sospetta compromissione della segretezza della chiave privata (revoca o sospensione immediata). La CRL è emessa sempre integralmente. Il momento della

pubblicazione della CRL viene attestata utilizzando quale riferimento temporale la data fornita dal sistema di Time Stamping Authority InfoCert e tale registrazione viene riportata sul giornale di controllo. Ogni elemento della lista CRL contiene nell'apposita estensione la data e l'ora di revoca o sospensione. La CRL da consultare per lo specifico certificato è indicata nel certificato stesso secondo le norme vigenti.

4.9.8 Latenza massima della CRL

Il tempo di attesa tra la richiesta di revoca o di sospensione e la sua realizzazione tramite pubblicazione della CRL è al massimo di un'ora.

4.9.9 Servizi online di verifica dello stato di revoca del certificato

Oltre alla pubblicazione della CRL nei registri LDAP e http, InfoCert mette a disposizione anche un servizio OCSP per la verifica dello stato del certificato. L'URL del servizio è indicato nel certificato. Il servizio è disponibile 24 X 7.

4.10 Servizi riguardanti lo stato del certificato

4.10.1 Caratteristiche operative

Le informazioni sullo stato dei certificati sono disponibili tramite CRL e servizio OCSP. Il numero di serie di un certificato revocato rimane in CRL anche dopo la fine della validità del certificato ed almeno sino alla scadenza del certificato di TSA.

Le informazioni fornite dal servizio OCSP per i certificati sono aggiornate all'ultima CRL pubblicata.

4.10.2 Disponibilità del servizio

Il servizio OCSP e le CRL sono disponibili 24 ore per 7 giorni la settimana.

4.11 Disdetta dai servizi della TSA

n/a

4.12 Deposito presso terzi e recovery della chiave

n/a

5 MISURE DI SICUREZZA E CONTROLLI

Il TSP InfoCert ha realizzato un sistema di sicurezza del sistema informativo relativo al servizio di certificazione digitale. Il sistema di sicurezza implementato è articolato su tre livelli:

- un livello fisico che mira a garantire la sicurezza degli ambienti in cui il TSP gestisce il servizio,
- un livello procedurale, con aspetti prettamente organizzativi,
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio e con l'infrastruttura utilizzata.

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

Un estratto della politica di sicurezza InfoCert è disponibile facendone richiesta alla casella PEC infocert@legalmail.it.

5.1 Sicurezza fisica

Le misure adottate forniscono adeguate garanzie di sicurezza in merito a:

- Caratteristiche dell'edificio e della costruzione;
- Sistemi anti-intrusione attivi e passivi;
- Controllo degli accessi fisici;
- Alimentazione elettrica e condizionamento dell'aria;
- Protezione contro gli incendi;
- Protezione contro gli allagamenti;
- Modalità di archiviazione dei supporti magnetici;
- Siti di archiviazione dei supporti magnetici.

5.1.1 Posizione e costruzione della struttura

Il Data Center InfoCert si trova a Padova. Il sito di Disaster Recovery è ubicato a Modena ed è connesso al Data Center sopra citato tramite un collegamento dedicato e ridondato su due circuiti diversi MPLS a 40 Gbit/s ciascuno upgradabile fino a 100 Gbit/s.

All'interno di entrambi i siti sono stati ricavati dei locali protetti con dei più elevati livelli di sicurezza, sia fisici che logici, all'interno dei quali sono attestati gli apparati informatici che costituiscono il cuore dei servizi di certificazione digitale, marcatura temporale, firma remota e automatica.

Per i servizi in continuità operativa con valori di RTO/RPO prossimi allo zero, alcune componenti dei servizi di marcatura temporale relativi alla pubblicazione delle CRL, all'OCSP e ad alcuni servizi

di FrontEnd, sono ospitati su cloud AWS, rispettivamente, nelle Regioni Europa Francoforte, Europa Irlanda, Europa Milano.

AWS dispone di certificazioni di conformità ai sensi degli standard ISO/IEC 27001:2013, 27017:2015, 27018:2019 e ISO/IEC 9001:2015.



Figura 1 - ubicazione Data Center InfoCert e sito della Disaster Recovery

5.1.2 Accesso fisico

L'accesso al Data Center è regolato dalle procedure InfoCert di sicurezza. All'interno del Data Center c'è l'area bunker in cui sono i sistemi della CA, per il quale è richiesto un ulteriore fattore di sicurezza.

5.1.3 Impianto elettrico e di climatizzazione

Il sito che ospita il Data Center InfoCert su Padova, pur non essendo certificato, ha le caratteristiche di un Data Center di tier 3.

I locali tecnici sono provvisti di un sistema di alimentazione elettrica progettato al fine di prevenire guasti e soprattutto disservizi. L'alimentazione dei sistemi include le più moderne tecnologie al fine di incrementare l'affidabilità e assicurare la ridondanza delle funzionalità più critiche ai fini dei servizi erogati.

L'infrastruttura preposta all'alimentazione include:

- Gruppi di continuità, dotati di accumulatori, in corrente alternata (UPS);
- Disponibilità di tensione alternata (220-380V AC);
- Armadi alimentati in ridondanza con linee protette e dimensionate per l'assorbimento concordato;

- Servizio di generatori di emergenza;
- Sistema di commutazione automatico e sincronizzazione fra generatori, rete e batterie (STS).

Ogni armadio tecnologico installato presso il Data Center fruisce di due linee elettriche che assicurano l'HA in caso di interruzione di una delle due linee disponibili.

L'armadio tecnologico è monitorato remotamente; vengono effettuati controlli costanti sullo stato della linea elettrica (on/off) e le potenze elettriche assorbite (ogni linea non deve superare il 50% del carico).

L'area tecnica è normalmente mantenuta fra 20° e 27° con un tasso di umidità relativo compreso fra il 30% ed il 60%. Gli impianti sono dotati di batterie condensanti con sistema di raccolta e scarico condensa sigillato e controllato da sonde anti-allagamento. L'intero sistema di condizionamento è asservito ai generatori di emergenza in caso di assenza di energia elettrica. Si garantisce la capacità frigorifera per armadio con un carico massimo previsto di 10KW e massimo di 15 KW su due armadi affiancati.

5.1.4 Prevenzione e protezione contro gli allagamenti

La zona d'ubicazione dell'immobile non presenta rischi ambientali dovuti alla vicinanza ad installazioni "pericolose". Durante la progettazione dello stabile sono stati presi opportuni accorgimenti per isolare i locali potenzialmente pericolosi, quali quelli contenenti il gruppo elettrogeno e la centrale termica.

L'area che ospita gli apparati è al piano terreno in una posizione sopraelevata rispetto al livello della strada.

5.1.5 Prevenzione e protezione contro gli incendi

È presente nel Data Center un impianto di rilevazione fumi gestito da centrale analogica indirizzata NOTIFIER con sensori ottici posizionati in ambiente e nel controsoffitto e sensori a campionamento d'aria installati sottopavimento e nelle canalizzazioni dell'aria.

L'impianto di rilevazione automatica d'incendi è collegato ad impianti di spegnimento automatici a gas estinguenti ecologici NAFS125 e PF23 e, in alcune sale, con sistemi di spegnimento ad aerosol. Nel caso di intervento contemporaneo di due rivelatori nella stessa zona, è comandata la scarica di estinguento nella zona interessata.

Per ogni compartimento antincendio è previsto un impianto di estinzione dedicato.

Sono inoltre presenti mezzi estinguenti portatili in conformità alle leggi e normative vigenti.

Le canalizzazioni dell'aria primaria asservite alle sale apparati sono dotate, in corrispondenza degli attraversamenti dei compartimenti antincendio, di serrande tagliafuoco azionate dall'impianto automatico di rilevazione incendi.

5.1.6 Supporti di memorizzazione

Per quanto concerne la piattaforma storage, la soluzione in essere prevede per la parte NAS l'utilizzo di sistemi NetApp (FAS 8060). Per la parte SAN si è invece implementata un'infrastruttura per la parte data center basata su tecnologie Infinidat che comprendono n.2 enclosure InfiniBox di generazione F4000 e F6000; per la parte di CA l'infrastruttura si basa su tecnologia Pure Storage.

5.1.7 Smaltimento dei rifiuti

InfoCert è certificata ISO 14001 per la gestione ambientale sostenibile del proprio ciclo produttivo, compresa la raccolta differenziata e lo smaltimento sostenibile dei rifiuti. Per quel che riguarda il contenuto informativo dei rifiuti elettronici, tutti i media, prima della dismissione, vengono ripuliti secondo le procedure previste ovvero avvelandosi di società di sanitizzazione certificate.

5.1.8 Off-site backup

È realizzato nel sito di Disaster Recovery, con un dispositivo EMC Data Domain 4200, su cui, il Data Domain primario del sito di Padova, replica i dati di backup.

5.2 Controlli procedurali

5.2.1 Ruoli chiave

I ruoli chiave sono coperti da figure dotate dei necessari requisiti di esperienza, professionalità e competenza tecnica e giuridica, che vengono continuamente verificati mediante le valutazioni annuali.

La lista dei nomi e l'organigramma delle figure in ruolo chiave è stata depositata presso AgID in occasione del primo accreditamento e viene costantemente tenuta aggiornata per seguire la naturale evoluzione dell'organizzazione aziendale.

5.3 Controllo del personale

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

Effettuata la pianificazione annuale delle Risorse Umane, il Responsabile Funzione/Struttura Organizzativa identifica le caratteristiche e gli skill della risorsa da inserire (*job profile*). Successivamente, di concerto con il responsabile selezione, viene attivato il processo di ricerca e selezione.

5.3.2 Procedure di controllo delle esperienze pregresse

I candidati individuati partecipano al processo di selezione affrontando un primo colloquio conoscitivo-motivazionale con il responsabile della selezione e un successivo colloquio tecnico con il responsabile di Funzione/Struttura Organizzativa, volto a verificare le skill dichiarate dal candidato. Ulteriori strumenti di verifica sono esercitazioni e test.

5.3.3 Requisiti di formazione

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate, è previsto di affidare la gestione operativa del sistema a persone diverse, con compiti separati e ben definiti. Il personale addetto alla progettazione ed erogazione del servizio di certificazione è un dipendente InfoCert ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi

informatici, con caratteristiche di affidabilità e riservatezza. Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati.

5.3.4 Frequenza di aggiornamento della formazione

Ogni inizio anno viene svolta l'analisi delle esigenze formative propedeutica alla definizione delle attività formative da erogare nell'anno. L'analisi è strutturata nel modo seguente:

- Incontro con la Direzione per la raccolta dei dati relativi alle esigenze formative necessarie per raggiungere gli obiettivi aziendali;
- Intervista ai Responsabili per la rilevazione delle esigenze formative specifiche delle proprie aree;
- Restituzione dei dati raccolti alla Direzione Aziendale per chiusura ed approvazione del Piano Formativo.

Entro il mese di febbraio il Piano Formativo così definito viene condiviso e reso pubblico.

5.3.5 Frequenza nella rotazione dei turni di lavoro

La presenza in sede o in modalità di lavoro agile (smart working) si distribuisce su una fascia oraria dalle ore 08:00 alle ore 19:00 dal lunedì al venerdì.

Il presidio degli ambienti di produzione nella fascia notturna e nella fascia festiva viene garantito attraverso un piano di turnazione della reperibilità predisposto dal responsabile di unità organizzativa mensilmente con un anticipo di almeno 10 giorni. A seconda della necessità, gli interventi potranno essere condotti da remoto (teleintervento) o richiedere l'accesso alle sedi.

Fermo restando il possesso dei necessari requisiti tecnici e professionali, l'Azienda provvede ad avvicinare nella reperibilità il maggior numero possibile di lavoratori, dando priorità ai dipendenti che ne facciano richiesta.

5.3.6 Sanzioni per azioni non autorizzate

Si fa riferimento al "CCNL Metalmeccanici e installazione impianti industria privata" per la procedura di irrogazione delle sanzioni.

5.3.7 Controlli sul personale non dipendente

L'accesso al personale non dipendente è regolato da una specifica policy aziendale.

5.3.8 Documentazione che il personale deve fornire

Al momento dell'assunzione, il dipendente deve fornire copia di un documento d'identità valido, copia della tessera sanitaria valida e una foto in formato tessera per il badge di accesso ai locali. Dovrà in seguito compilare e firmare il consenso al trattamento dei dati personali e l'impegno a non divulgare notizie e/o documenti riservati. Dovrà infine prendere visione del Codice Etico e della Netiquette InfoCert.

5.4 Gestione del giornale di controllo

Gli eventi legati alla gestione della TSA , della vita del certificato e degli eventi relativi alla fonte del tempo sono raccolti nel giornale di controllo come previsto dal Regolamento e dalle regole tecniche [1.].

5.4.1 Tipi di eventi memorizzati

Vengono registrati eventi di sicurezza, avviamento e spegnimento, crash di sistema e guasti hardware, attività di firewall e router e tentativi di accesso sistema PKI.

Vengono registrati tutti gli eventi riguardanti le personalizzazioni dei dispositivi di firma.

Vengono registrati tutti gli accessi fisici ai locali ad alta sicurezza dove risiedono le macchine.

Vengono registrati gli eventi legati alle chiavi e certificati delle TSUs.

Vengono registrati tutti gli eventi riguardanti la sincronizzazione e ricalibrazione degli orologi delle TSU con il tempo universale coordinato UTC.

Ogni evento viene salvato con data e ora di sistema dell'evento.

5.4.2 Frequenza di trattamento e di memorizzazione del giornale di controllo

Il trattamento e raggruppamento dei dati nonché memorizzazione sul sistema di conservazione a norma InfoCert avviene mensilmente.

5.4.3 Periodo di conservazione del giornale di controllo

Il giornale di controllo viene conservato per 20 anni dalla CA.

5.4.4 Protezione del giornale di controllo

La protezione del giornale di controllo è garantita da Sistema di Conservazione dei documenti elettronici InfoCert, accreditato presso AgID secondo la normativa vigente.

5.4.5 Procedure di backup del giornale di controllo

Il Sistema di Conservazione dei documenti elettronici attua una politica e procedura di backup, come previsto dal manuale della sicurezza del suddetto sistema.

5.4.6 Sistema di memorizzazione del giornale di controllo

La raccolta dei log degli eventi avviene attraverso procedure automatiche ad hoc, la memorizzazione avviene nelle modalità previste dal sistema di conservazione a norma InfoCert e descritto nel manuale della sicurezza del suddetto sistema.

5.4.7 Notifica in caso di identificazione di vulnerabilità

n/a

5.4.8 Valutazioni di vulnerabilità

InfoCert svolge periodicamente delle valutazioni sulle vulnerabilità del Sistema (vulnerability assessment) e test antiintrusione (penetration test). A fronte dei risultati mette in atto tutte le contromisure per mettere in sicurezza le applicazioni.

5.5 Archiviazione dei verbali

5.5.1 Tipi di verbali archiviati

Vengono redatti e archiviati verbali relativi ai più importanti eventi di una Certification Authority. I verbali vengono conservati per 20 anni dalla Certification Authority nel Sistema di Conservazione dei documenti InfoCert.

5.5.2 Protezione dei verbali

La protezione è garantita dal Sistema di Conservazione dei documenti InfoCert, accreditato in AgID.

5.5.3 Procedure di backup dei verbali

Il sistema di conservazione a norma attua una politica e procedura di backup, come previsto dal manuale della sicurezza del suddetto sistema.

5.5.4 Requisiti per la marcatura temporale dei verbali

n/a

5.5.5 Sistema di memorizzazione degli archivi

La raccolta dei verbali avviene attraverso procedure automatiche ad hoc, la memorizzazione avviene nelle modalità previste dal sistema di conservazione a norma InfoCert e descritto nel manuale della sicurezza del suddetto sistema.

5.5.6 Procedure per ottenere e verificare le informazioni contenute negli archivi

Sono predisposte procedure e sistemi automatici per il controllo dello stato del sistema di certificazione e dell'intera infrastruttura tecnica della CA.

5.6 Sostituzione della chiave privata della TSU

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata al sistema che fornisce il servizio. Le chiavi di marcatura temporale (chiavi TSU) vengono sostituite ogni tre mesi prima della scadenza del certificato senza revocare il precedente.

5.7 Compromissione della chiave privata della TSA e disaster recovery

5.7.1 Procedure per la gestione degli incidenti

IL TSP ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO 27000. Ogni eventuale incidente, non appena rilevato, è soggetto a puntuale analisi, individuazione delle contromisure correttive e verbalizzazione da parte del responsabile del servizio. Il verbale è firmato digitalmente e inviato al Sistema di Conservazione InfoCert; una copia è inviata anche a AgID, unitamente alla dichiarazione delle azioni di intervento mirante a eliminare le cause che possono aver dato luogo all'incidente, se sotto il controllo di InfoCert come previsto dall'articolo 19 del Regolamento.

5.7.2 Corruzione delle macchine, del software o dei dati

In caso di guasto del dispositivo sicuro di firma HSM contenente le chiavi di certificazione si fa ricorso alla copia di riserva della chiave di certificazione, opportunamente salvata e custodita, e non vi è necessità di revocare il corrispondente certificato della TSA.

I software e i dati sono soggetti a regolare backup come previsto dalle procedure interne.

5.7.3 Procedure in caso di compromissione della chiave privata della TSA

La compromissione della chiave di certificazione è considerato un evento particolarmente critico, in quanto invaliderebbe i certificati emessi e le informazioni sullo stato di revoca firmati con tale chiave. Vi è quindi una particolare attenzione alla protezione della chiave di certificazione e a tutte le attività di sviluppo e manutenzione del sistema che possono avere impatto sulla stessa.

Nonostante sia un evento raro, InfoCert ha predisposto una procedura dettagliata da seguire nell'ambito del SGSI certificato ISO 27000, dandone evidenza al CAB.

Una volta accertata la compromissione della chiave privata di TSA, InfoCert procederà tempestivamente

- a informare il Supervisory Body italiano AgID per la rimozione della chiave dalla TSL e il CAB,
- ad avvisare i clienti tramite comunicazione diretta, ove possibile, e tramite comunicazione sul sito InfoCert,
- a spegnere il servizio con la chiave compromessa e a revocare i certificati impattati, a procedere eventualmente all'emissione e accreditamento di una nuova root TSA e a fornire in maniera affidabile le informazioni sullo stato di revoca dei certificati.

5.7.4 Erogazione dei servizi in caso di disastri

InfoCert ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità o di disastro.

5.8 Cessazione del servizio di validazione temporale

Nel caso di cessazione dell'attività di validazione temporale, InfoCert comunicherà questa intenzione all'Autorità di vigilanza (AgID) e all'ente di certificazione (CAB) con un anticipo di almeno 6 mesi, indicando, eventualmente, il depositario del registro dei certificati e della relativa

documentazione.

In caso di cessazione della TSA l'informazione sullo stato di revoca sarà fornita tramite l'emissione di un'ultima CRL.

Maggiori dettagli sono presenti nel documento TSP Termination Plan dei Servizi di Certificazione Digitale e di Validazione Temporale disponibile presso il certificatore.

6 CONTROLLI DI SICUREZZA TECNOLOGICA

6.1 Generazione della coppia di chiavi di marcatura temporale della TSU

La marca temporale viene firmata con algoritmo asimmetrico da una chiave privata memorizzata su un dispositivo hardware sicuro e la corrispondente chiave pubblica certificata da una Certification Authority InfoCert dedicata a questo servizio (TSA).

La coppia di chiavi asimmetriche è generata all'interno di un dispositivo crittografico hardware (HSM) conforme ai requisiti di sicurezza previsti da ETSI319421 [26].

I dispositivi per la generazione della coppia di chiavi asimmetriche delle TSU possono essere attivati solo da operatori autorizzati, che lavorano in coppia e che provvedono allo sblocco del dispositivo crittografico inserendo una coppia di smartcard accompagnate dal PIN.

Le chiavi private sono generate e memorizzate all'interno dei dispositivi crittografici in modo tale da impedirne l'esportazione.

6.1.1 Algoritmo e lunghezza delle chiavi

La coppia di chiavi asimmetriche di certificazione è generata all'interno di un dispositivo crittografico hardware di cui sopra. Viene usato l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiore a 2048 bit.

6.1.2 Controlli di qualità e generazione della chiave pubblica

I dispositivi utilizzati sono certificati secondo alti standard di sicurezza (si veda il § 6.2.1) e garantiscono che la chiave pubblica sia corretta e randomica. La CA, prima di emettere il certificato, verifica che la chiave pubblica non sia già stata utilizzata.

6.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico

6.2.1 Controlli e standard del modulo crittografico

I moduli crittografici utilizzati da InfoCert per le chiavi di certificazione (TSA) sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 in Europa.

6.2.2 Controllo di più persone della chiave privata di TSA

L'accesso ai dispositivi contenenti le chiavi di certificazione avviene solo con due persone autenticate contemporaneamente.

6.2.3 Backup della chiave privata di TSA

Il backup delle chiavi è contenuto in una cassaforte il cui accesso è dato solo al personale che non ha accesso ai dispositivi HSM. Un eventuale ripristino, richiede dunque la presenza sia del personale che ha accesso ai dispositivi sia di chi ha l'accesso alla cassaforte.

6.2.4 Memorizzazione della chiave privata su modulo crittografico

La chiave di certificazione viene generata e memorizzata in un'area protetta del dispositivo crittografico che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende bloccato o rende illeggibile il dispositivo stesso.

6.2.5 Metodo di attivazione della chiave privata

Il sistema per il servizio di marcatura temporale può essere attivato solo da operatori autorizzati tramite l'utilizzo di una serie di password e disponendo di un certo numero di dispositivi crittografici personali.

Una volta attivato, il sistema non necessita di ulteriori procedure interattive di login, tranne che per arrestarlo e riattivarlo a scopo di manutenzione.

6.2.6 Metodo per distruggere la chiave privata della TSA

Il personale InfoCert deputato a questo ruolo si occupa della distruzione della chiave privata quando il certificato è scaduto o revocato, secondo le procedure di sicurezza previste dalle politiche di sicurezza e le specifiche del produttore del dispositivo.

6.3 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 4.2.

6.4 Controlli sulla sicurezza informatica

6.4.1 Requisiti di sicurezza specifici dei computer

Il sistema operativo degli elaboratori utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati e la gestione del registro dei certificati, sono securizzati (hardening), sono cioè configurati in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione della CA.

L'accesso da parte degli Amministratori di sistema, all'uopo nominati in conformità con quanto prescritto dalla normativa vigente, avviene tramite un'applicazione di root on demand che permette l'utilizzo dei privilegi dell'utenza root solo previa autenticazione individuale. Gli accessi sono tracciati e loggati e conservati per 12 mesi.

6.5 Operatività sui sistemi di controllo

InfoCert attribuisce importanza strategica al trattamento sicuro delle informazioni e riconosce la necessità di sviluppare, mantenere, controllare e migliorare in modo costante un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in conformità alla norma ISO/IEC 27001.

InfoCert è certificata ISO/IEC 27001:2005 da marzo 2011 per le attività EA:33-35. Nel marzo 2015 è stata certificata per la nuova versione dello standard ISO/IEC 27001:2013.

Nel SGSI sono previsti procedure e controlli per:

- Gestione degli Asset;
- Controllo degli Accessi;
- Sicurezza Fisica ed Ambientale;
- Sicurezza delle Attività Operative;
- Sicurezza delle Comunicazioni;
- Acquisizione, Sviluppo e Manutenzione dei Sistemi;
- Gestione degli Incidenti;
- Continuità Operativa.

Tutte le procedure sono approvate dai relativi responsabili e condivisi internamente nel sistema di gestione documentale InfoCert.

6.6 Controlli di sicurezza della rete

InfoCert ha ideato, per il servizio di certificazione, un'infrastruttura di sicurezza della rete basata sull'uso di meccanismi di firewalling e del protocollo SSL in modo da realizzare un canale sicuro tra gli Uffici di Registrazione ed il sistema di certificazione, nonché tra questo e gli amministratori/operatori.

I sistemi e le reti di InfoCert sono connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (Demilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite. Le regole definite sui firewall vengono progettate in base ai principi di "default deny" (quanto non è espressamente permesso è vietato di default, ovvero, le regole consentiranno solo quanto è strettamente necessario al corretto funzionamento dell'applicazione) e "defense in depth" (vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere firewall, ed infine l'hardening a livello di sistema).

7 FORMATO

7.1 Formato del certificato della TSU

Nel certificato compaiono le informazioni indicate nella richiesta di certificazione.

Il formato del certificato prodotto è conforme al Regolamento eIDAS e alla Determinazione Agid 121/2019[12]; in questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.

InfoCert utilizza lo standard ITU X.509, version 3 per l'intera struttura PKI.

7.1.1 Numero di versione

Tutti i certificati emessi da InfoCert sono X.509 versione 3.

7.1.2 Estensioni del certificato

I certificati qualificati sono caratterizzati dalle estensioni presenti nei qcStatement clause 3.2.6 of IETF RFC 3739. Il loro utilizzo è regolato dalla norma ETSI 319 412-2 e ETSI 319 422.

7.1.3 OID dell'algoritmo di firma

L'algoritmo di sottoscrizione della marca temporale. Nella fattispecie l'algoritmo utilizzato è l'RSA. (sha256WithRSAEncryption OID:1.2.840.113549.1.1.11);

7.1.4 Forme di nomi

Ogni certificato contiene un numero di serie univoco all'interno della TSA che lo ha emesso.

7.1.5 Vincoli ai nomi

Si veda in merito il paragrafo 3.1.

7.1.6 OID del certificato

Si veda in merito il paragrafo 1.2.

7.1.7 Formato e contenuto della marca temporale

Il formato delle marche temporali ed il protocollo di colloquio con la TSA rispettano le specifiche tecniche richieste in ETSI319422 [27]. Ogni marca temporale emessa contiene tutte le informazioni richieste dalla normativa, ovvero:

- L'identificativo dell'emittente la marca temporale;
- Il numero di serie della marca temporale;
- L'identificativo del certificato relativo alla chiave pubblica della TSU;
- La data e l'ora di generazione della marca;
- L'accuratezza (accuracy) della fonte del tempo rispetto ad UTC. Nella fattispecie è di un secondo o migliore;

- L'identificativo dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale. Nella fattispecie l'algoritmo utilizzato è SHA-256 (secure hash algorithm 256-bit OID:2.16.840.1.101.3.4.2.1);
- Il valore dell'impronta dell'evidenza informatica.

7.2 Formato della CRL del certificato di marcatura

Per formare le liste di revoca CRLs, InfoCert utilizza il profilo RFC5280 "Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)" e aggiunge al formato di base le estensioni come definite da RFC 5280: "Authority Key Identifier", "CRL Number", "Issuing Distribution Point" e "expiredCertsOnCRL".

7.2.1 Numero di versione

Tutti le CRL emesse da InfoCert sono X.509 versione 2.

7.3 Formato dell'OCSP

Per consentire di determinare lo stato di revoca del certificato senza fare richiesta alla CRL, InfoCert rende disponibile servizi OCSP conformi al profilo RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP". Questo protocollo specifica i dati che devono essere scambiati da un'applicazione che vuole verificare lo stato del certificato e il servizio OCSP.

7.3.1 Numero di versione

Il protocollo OCSP utilizzato da InfoCert è conforme alla versione 1 del RFC6960.

8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ

Per ottenere la qualifica di prestatore di servizi fiduciari qualificati e non, in conformità al Regolamento eIDAS è necessario espletare l'iter previsto dall'articolo 21 del suddetto Regolamento. InfoCert ha presentato ad AgID l'apposita richiesta per ottenere il riconoscimento di "prestatore del servizio fiduciario qualificato" allegando un report della valutazione di conformità con il Regolamento (Conformity Assessment Report - CAR) rilasciato da un organismo di valutazione autorizzato dal preposto organismo nazionale (CAB), che in Italia è ACCREDIA.

InfoCert presta il Servizio quale prestatore di servizi fiduciari qualificati ai sensi del Regolamento (UE) N. 910/2014 del 23/07/2014, sulla base di una valutazione di conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento di cui sopra e della Norma ETSI EN 319 401, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319_403 e UNI CEI EN ISO/IEC 17065:2012.

8.1 Frequenza o circostanze per la valutazione di conformità

La valutazione di conformità viene ripetuta ogni due anni, ma ogni anno il CAB esegue un audit di sorveglianza.

8.2 Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da:

Denominazione sociale	CSQA Certification S.r.l.
Sede legale	Via S. Gaetano n. 74, 36016 Thiene (VI)
N. di telefono	+39 0445 313011
N. Iscrizione Registro Imprese	Codice Fiscale 02603680246 Registro Imprese VI n. 02603680246 / REA n. 258305
N. partita IVA	02603680246
Sito web	http://www.csqa.it

8.3 Rapporti tra InfoCert e CAB

InfoCert e CSQA non hanno interessi finanziari né relazioni di affari.

Non sono in corso rapporti commerciali o di partnership che possono creare pregiudizi a favore o contro InfoCert nella valutazione obiettiva di CSQA.

8.4 Aspetti oggetto di valutazione

Il CAB è chiamato a valutare la conformità rispetto al Manuale Operativo, al Regolamento e alla normativa applicabile delle procedure adottate, dell'organizzazione della CA, dell'organizzazione dei ruoli, della formazione del personale, della documentazione contrattuale.

8.5 Azioni in caso di non conformità

In caso di non conformità, il CAB deciderà se inviare comunque il rapporto ad AgID, o se riservarsi di rieseguire l'audit dopo che la non conformità sia stata sanata.

InfoCert si impegna a risolvere tutte le non conformità in maniera tempestiva, mettendo in atto tutte le azioni di miglioramento e adeguamento necessarie.

9 ALTRI ASPETTI LEGALI E DI BUSINESS

9.1 Tariffe

9.1.1 Tariffe per il rilascio della marca temporale

Le tariffe sono disponibili presso i siti <https://www.firma.infocert.it/> e <http://ecommerce.infocert.it>. La CA può stipulare accordi commerciali prevedendo tariffe specifiche.

9.1.2 Tariffe per la verifica della marca temporale

La verifica della marca temporale è libera e gratuita.

9.1.3 Tariffe per altri servizi

Le tariffe sono disponibili presso i siti <https://www.firma.infocert.it/> e <http://ecommerce.infocert.it>. La CA può stipulare accordi commerciali prevedendo tariffe specifiche.

9.1.4 Politiche per il rimborso

Qualora il servizio venga acquistato da un consumatore, il Soggetto ha il diritto di recedere dal contratto entro il termine di 14 giorni a decorrere dalla data di conclusione del contratto, ottenendo il rimborso del prezzo pagato. Le istruzioni per l'esercizio del diritto di recesso e la richiesta di rimborso sono disponibili presso il sito <https://help.infocert.it/>.

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

Il TSP InfoCert ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato trattato ed accettato da AgID, che ha come massimali:

- 10.000.000 euro per singolo sinistro;
- 10.000.000 euro per annualità.

9.2.2 Garanzia o copertura assicurativa per i soggetti finali

Si veda il paragrafo 9.2.1.

9.3 Confidenzialità delle informazioni di business

9.3.1 Ambito di applicazione delle informazioni confidenziali

Nell'ambito dell'attività oggetto del presente Manuale non è prevista la gestione di informazioni confidenziali.

9.4 Privacy

Le informazioni relative al Soggetto di cui la CA viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili.

In particolare i dati personali vengono trattati da InfoCert in conformità a quanto indicato nel Decreto Legislativo 30 giugno 2003, n. 196 e nel Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente vincolante dal 25 maggio 2018 [4].

9.4.1 Programma sulla privacy

InfoCert adotta un set di policy tramite le quali implementa e integra la protezione dei dati personali all'interno del suo Sistema di Gestione della Sicurezza delle Informazioni certificato ISO 27001, condividendo con quest'ultimo sistema il processo di miglioramento continuo.

9.4.2 Dati che sono trattati come personali

Sono trattati come dati personali i dati che ricadono nella corrispondente definizione di cui alla normativa vigente [4.]; per dato personale si intende quindi qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

9.4.3 Trattamento dei dati personali

InfoCert S.p.A.

Sede Operativa

Via Marco e Marcelliano 45

00147 Roma

richieste.privacy@legalmail.it

9.4.4 Informativa privacy e consenso al trattamento dei dati personali

L'informativa privacy è disponibile sul sito www.infocert.it.

Prima di eseguire ogni trattamento di dati personali, InfoCert procede a raccogliere il consenso al trattamento nei modi e nelle forme previsti dalla legge.

9.4.5 Divulgazione dei dati a seguito di richiesta da parte dell'autorità

La divulgazione di dati su richiesta delle Autorità è obbligatoria e viene svolta nelle modalità stabilite volta per volta dall'Autorità stessa.

9.4.6 Altri motivi di divulgazione

Non previsti.

9.5 Proprietà intellettuale

Il diritto d'autore sul presente documento è di InfoCert S.p.A. Tutti i diritti sono riservati.

9.6 Rappresentanza e garanzie

InfoCert mantiene la responsabilità per l'osservanza delle procedure prescritte nella propria policy sulla sicurezza delle informazioni, anche quando alcune funzioni vengono delegate ad un altro soggetto.

Il Cliente o Richiedente è responsabile della veridicità dei dati comunicati al Certificatore.

Il Cliente o Richiedente è altresì obbligato a rendere note e a fare accettare le condizioni Generali del Servizio di Validazione Temporale e il presente Manuale Operativo a tutti i soggetti che utilizzano il Servizio

9.7 Limitazione di garanzia

il Certificatore non presta alcuna garanzia i) sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dal Richiedente; ii) su usi della Marca Temporale che siano diversi rispetto a quelli previsti dalle norme vigenti e dal presente Manuale Operativo; iii) sul regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali; iv) sulla validità e rilevanza, anche probatoria, di qualsiasi messaggio, atto o documento associato alla Marca Temporale.

Il Certificatore garantisce unicamente il funzionamento del Servizio, secondo i livelli indicati al paragrafo 9.18 del presente Manuale Operativo.

9.8 Limitazione di responsabilità

Il Servizio è reso in base a quanto previsto nel Contratto per i Servizi di Marcatura Temporale (di seguito anche "Contratto"). Il Certificatore non esegue nessun controllo del documento per il quale si richiede la Marca Temporale, in quanto tali determinazioni e informazioni sono conosciute e trasmesse direttamente dal Richiedente sotto la propria ed esclusiva responsabilità. Il Certificatore non assume alcun obbligo di sorveglianza in merito al contenuto, alla tipologia o al formato elettronico dei documenti ed eventualmente degli hash trasmessi dalla procedura informatica indicata dal Richiedente o dal Titolare, non assumendo alcuna responsabilità, salvo il caso di dolo o colpa in merito alla validità e riconducibilità degli stessi all'effettiva volontà del Richiedente.

Fatto salvo il caso di dolo o colpa, il Certificatore non assume responsabilità per danni diretti e indiretti subiti dai Titolari e/o da terzi in conseguenza dell'utilizzo o del mancato utilizzo dei certificati di Marca Temporale rilasciati in base alle previsioni del presente Manuale e delle Condizioni Generali dei Servizi di Marcatura Temporale.

InfoCert non è responsabile di qualsiasi danno diretto e/o indiretto derivante in via anche alternativa i) dalla perdita, ii) dalla impropria conservazione, iii) da un improprio utilizzo, degli strumenti di Marcatura Temporale e/o dalla mancata osservanza di quanto sopra, da parte del Richiedente.

Il Certificatore, inoltre, fin dalla fase di formazione del Contratto per i servizi di Marcatura Temporale, e anche nel corso dell'esecuzione, non risponde per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informatico e della rete internet.

InfoCert, salvo il caso di dolo o colpa, non sarà gravata da oneri o responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero verificarsi al Richiedente e/o a terzi causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati da parte di terzi non autorizzati da InfoCert.

9.9 Indennizzi

InfoCert è responsabile degli eventuali danni direttamente determinati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica, in seguito a un mancato adempimento degli obblighi di cui al Regolamento Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e dal mancato utilizzo, da parte di InfoCert, di tutte le misure idonee ad evitare il danno stesso.

Nel caso di cui al paragrafo precedente, il Richiedente o il Titolare avranno diritto di ottenere, a titolo di risarcimento dei danni direttamente subiti in conseguenza del comportamento di cui al paragrafo precedente, un importo che non potrà in ogni caso essere superiore ai valori massimi previsti, per ciascun sinistro e per anno, dall'art. 3, c. 7, del Regolamento allegato alla Determinazione 185/2017.

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile all'utilizzo improprio del servizio di certificazione o al gestore della rete di telecomunicazioni ovvero derivante da caso fortuito, forza maggiore o cause comunque non imputabili ad InfoCert, quali, a titolo esemplificativo, scioperi, sommosse, terremoti, atti di terrorismo, tumulti popolari, sabotaggio organizzato, eventi chimici e/o batteriologici, guerra, alluvioni, provvedimenti delle competenti autorità in materia o inadeguatezza delle strutture, dei macchinari hardware e/o dei software utilizzati dal Richiedente

9.10 Termine e risoluzione

9.10.1 Termine

Gli effetti del Contratto si producono dalla sua conclusione e perdurano fino al momento in cui viene utilizzata l'ultima delle Marche temporali acquistate con un unico ordine d'acquisto.

La durata del Contratto del Servizio di Marca Temporale è pari alla durata della Marca Temporale. In caso di cessazione del Contratto, per qualsiasi causa essa avvenga, non sarà più possibile usufruire del Servizio.

9.10.2 Risoluzione

Il Contratto di risolverà di diritto con contestuale interruzione del Servizio e revoca delle credenziali di marcatura temporale, nel caso in cui il Richiedente sia inadempiente rispetto alle previsioni contenute nelle clausole del Contratto di cui all'art. 1 (Oggetto del Contratto, specifiche del Servizio e rapporti tra le Parti), all'art. 6 (Corrispettivi), all'art. 7 (Identificativi ed accessi al sistema); art. 11.1 (Obblighi del Richiedente), art. 11.2 (Responsabilità del Richiedente), nonché a quanto previsto nel presente Manuale Operativo, ovvero nel caso in cui le dichiarazioni rese dal Richiedente per la stipula del Contratto o l'emissione della Marca Temporale non siano corrispondenti al vero.

La risoluzione si verificherà di diritto quando la parte interessata dichiarerà all'altra a mezzo Posta Elettronica Certificata o raccomandata A/R, che intende valersi della presente clausola.

In tutti i casi in cui il Richiedente sia inadempiente rispetto alle obbligazioni assunte, InfoCert potrà sospendere l'erogazione del Servizio, attraverso la sospensione delle credenziali di marcatura temporale.

In caso di assoggettamento di una delle Parti a fallimento o ad altra procedura concorsuale, l'altra parte avrà diritto di recedere senza alcun preavviso e onere dal presente Contratto e da ogni altro rapporto in essere. In ogni caso di scioglimento, cessazione, recesso o di risoluzione per qualsiasi causa avvenga del Contratto il corrispettivo di cui al precedente art. 6 è comunque dovuto e se già versato non sarà restituito.

È comunque salva l'eventuale risarcibilità di ogni ulteriore danno subito da InfoCert in caso di inadempimento da parte del Richiedente.

Nel caso in cui il Titolare sia un consumatore, si applicano le disposizioni previste dalla Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori. Le controversie civili inerenti il Contratto concluso dal consumatore sono devolute alla competenza territoriale inderogabile del giudice del luogo di residenza o di domicilio di questo.

Seppure InfoCert non si sia impegnata a ricorrere ad alcun organismo di risoluzione alternativa delle controversie, si informa il consumatore che può servirsi, su base volontaria, dei metodi di risoluzione extragiudiziale delle controversie previsti dalle norme di legge applicabili in materia. Si informa altresì che, ai sensi e per gli effetti del Regolamento UE n. 524/2013, per la risoluzione delle controversie relative ai contratti online e ai servizi offerti online, vi è la possibilità di ricorrere al procedimento di Online Dispute Resolution (ODR), previsto dalla Commissione Europea e raggiungibile al seguente link: <https://webgate.ec.europa.eu/odr/>

9.10.3 .Effetti della risoluzione

La risoluzione comporta l'immediata impossibilità di usufruire del servizio di marcatura temporale.

9.11 Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel paragrafo 1.5.1.

9.12 Revisione del Manuale Operativo

La CA 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 Operativo annulla e sostituisce le precedenti versioni, che rimangono tuttavia applicabili ai certificati emessi durante la loro vigenza e fino alla prima scadenza degli stessi.

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste. Ogni modifica tecnica o procedurale a questo Manuale Operativo verrà prontamente comunicata alle RA.

Se i cambiamenti sono rilevanti la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (*CAR – Conformity Assessment Report*) e il manuale operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

9.12.1 Storia delle revisioni

Versione/Release n°:	2.7
Data Versione/Release:	16/09/2021
Descrizione modifiche:	§ 1.5.1 Aggiornamento dei contatti
Motivazioni:	Modifica contatti

Versione/Release n°:	2.6
Data Versione/Release:	15/06/2021
Descrizione modifiche:	Modifica al titolo del documento con l'aggiunta del servizio non qualificato di marca temporale § 1.1: Aggiunta del servizio non qualificato § 1.2: Aggiunta policy non qualificate e revisione della descrizione § 1.4.1: Cambio denominazione software di verifica § 5.3.5: Aggiornamento descrizione turni di lavoro § 5.8: Revisione descrizione § 4.9: Chiarimento relativo alle informazioni sullo stato di revoca § 5.1.1: Aggiornamento tecnologico § 5.7.3: Aggiornamento descrizione § Appendice A: Aggiunta appendice con certificati di root TSA Correzioni ortografiche
Motivazioni:	Nuove root Revisione periodica

Versione/Release n°:	2.5
Data Versione/Release:	22/05/2020
Descrizione modifiche:	§ 5.1.1 Aggiornamento tecnologico § 5.1.6 Aggiornamento tecnologico dei supporti di memorizzazione Correzioni ortografiche ai paragrafi § 1.3.2, § 5.3.7
Motivazioni:	Aggiornamento tecnologico Correzioni ortografiche

Versione/Release n°:	2.4
Data Versione/Release:	14/06/2019

Descrizione modifiche:	<p>§ 1.2 introduzione OID agIDcert</p> <p>§5.1.1 Chiarimento sulla sede del Data Center</p> <p>§ 5.3.7 Compilata descrizione accessi fisici</p> <p>§ 5.4.1 Aggiunti descrizione log accessi fisici e logici</p>
Motivazioni:	<p>Entrate in vigore determinazione AgID 121/2019</p> <p>Correzione refusi e precisazioni</p>

Versione/Release n°:	2.3
Data Versione/Release:	30/11/2018
Descrizione modifiche:	§ 1.3 aggiornamento denominazione gruppo Tinexta
Motivazioni:	Cambio denominazione gruppo TecnoInvestimenti

Versione/Release n°:	2.2
Data Versione/Release:	19/06/2018
Descrizione modifiche:	<p>§ 1.5, § 9.2, § 9.4, § 9.15</p> <p>Nuovi contatti telefonici, adeguamenti massimali polizza assicurativa, riferimenti privacy, refusi vari.</p>
Motivazioni:	

Versione/Release n°:	2.1
Data Versione/Release:	09/04/2018
Descrizione modifiche:	<p>Correzione refusi</p> <p>§ 9.6, § 9.7, § 9.8, § 9.9, § 9.10 riscrittura paragrafi per migliore contestualizzazione</p>
Motivazioni:	

Versione/Release n°:	2.0.1
Data Versione/Release:	28/07/2017
Descrizione modifiche:	<p>Correzione refusi</p> <p>Aggiornamento mesi utilizzo della chiave TSU</p>
Motivazioni:	-

Versione/Release n°:	2.0
-----------------------------	-----

Data Versione/Release:	02/05/2017
Descrizione modifiche:	Riposizionati i contenuti su indice RFC 3647
Motivazioni:	-

Versione/Release n°:	1.0
Data Versione/Release:	01/07/2016
Descrizione modifiche:	Prima emissione
Motivazioni:	-

9.12.2 Procedure di revisione

Le procedure di revisione del Manuale Operativo sono analoghe alle procedure di redazione. Le revisioni sono apportate di concerto con il Responsabile del Servizio di Certificazione, il Responsabile della Sicurezza, il Responsabile della Privacy, l'Ufficio Legale e l'Area di Consulenza e approvate dal management.

9.12.3 Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del TSP (indirizzo: <http://www.firma.infocert.it/doc/manuali.htm>);
- in formato elettronico nell'elenco pubblico dei certificatori tenuto da AgID.

9.13 Risoluzione delle controversie

Si rimanda alla contrattualistica che regola il servizio per il dettaglio delle modalità di risoluzione delle controversie.

9.14 Foro competente

Per i consumatori il foro competente è il tribunale della città dove il consumatore ha il domicilio. Per i soggetti diversi dai consumatori, il foro competente è quello di Roma. Negli accordi tra CA e Soggetto può essere definito un diverso foro competente.

9.15 Legge applicabile

La legge applicabile al presente Manuale Operativo è la legge italiana.

Di seguito un elenco non esaustivo dei principali riferimenti normativi applicabili:

- [1] Regolamento UE N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel

mercato interno e che abroga la direttiva 1999/93/CE (referenziato anche come *Regolamento eIDAS*).

- [2] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (referenziato anche come *CAD*) e ss.m.ii.
- [3] *non utilizzato*
- [4] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii e Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (vigente dal 25 maggio 2018).
- [5] *non utilizzato*.
- [6] *non utilizzato*
- [7] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori e relative normative nazionali di recepimento.
- [8] Verifica preliminare - 24 settembre 2015 [4367555] Trattamento di dati personali nell'ambito del "Processo di rilascio con riconoscimento a mezzo webcam" per firma elettronica qualificata o digitale.
- [9] Deliberazione CNIPA n. 45 del 21 maggio 2009, come modificata dalle determinazioni successive (dal 5 luglio 2019 sostituita da [12])..
- [10] Determinazione AgID n°189/2017
- [11] Si applicano inoltre tutte le circolari e le deliberazioni dell'Autorità di Vigilanza¹, nonché gli atti di esecuzione previsti dal Regolamento eIDAS [1].
- [12] Determinazione AgID n°121/2019 ver 1.1 (sostituisce deliberazione CNIPA 45/2009).

9.16 Standard di riferimento

Di seguito un elenco non esaustivo degli standard di riferimento applicabili al servizio:

- i. ETSI EN 319 401 V2.1.1 - ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); GENERAL POLICY REQUIREMENTS FOR TRUST SERVICE PROVIDERS;
- ii. ETSI EN 319 421 V1.1.1 -ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); POLICY AND SECURITY REQUIREMENTS FOR TRUST SERVICE PROVIDERS ISSUING TIME-STAMPS, di seguito ETSI319421;
- iii. ETSI EN 319 422 V1.1.1 (2016-03) ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); TIME-STAMPING PROTOCOL AND TIME-STAMP TOKEN PROFILES, di seguito ETSI319422.

9.17 Disposizioni varie

Si rimanda alla contrattualistica che regola il servizio per ogni altra disposizione non compresa nel presente Manuale.

¹ Disponibili sul sito <http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche>.

9.18 Altre disposizioni

Gli orari di erogazione del servizio sono (salvo accordi contrattuali differenti):

Servizio	Orario
Richiesta di marca temporale	Dalle 0:00 alle 24:00 7 giorni su 7
Verifica di marca temporale	Dalle 0:00 alle 24:00 7 giorni su 7


```

234 20:      SET {
236 18:      SEQUENCE {
238 3:      OBJECT IDENTIFIER serialNumber (2 5 4 5)
243 11:      PrintableString '07945211006'
      :      }
      :      }
256 43:      SET {
258 41:      SEQUENCE {
260 3:      OBJECT IDENTIFIER commonName (2 5 4 3)
265 34:      UTF8String 'InfoCert Time Stamping Authority 2'
      :      }
      :      }
301 290:     SEQUENCE {
305 13:     SEQUENCE {
307 9:     OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
318 0:     NULL
      :     }
320 271:     BIT STRING, encapsulates {
325 266:     SEQUENCE {
329 257:     INTEGER
      :     00 C1 82 81 37 2D 2F 2A A4 48 26 15 AE 06 D6 87
      :     E2 45 EA 4C 39 0C 4B 6C 35 DE AB 35 8C B8 74 3C
      :     67 BE 75 28 7F 94 1A 48 20 A0 1F 33 14 88 FA D3
      :     8A 65 9A 8B CC 53 A2 AC F3 E3 69 D4 AC 7F 67 D6
      :     77 33 90 36 5E F9 87 30 4D 6E 5C F9 A9 F0 AB 8D
      :     86 91 17 B7 82 0B 34 EE E7 8C CD 6F CB FF 84 DC
      :     CF 74 EA B0 E1 1C 60 86 CF 51 15 9C 87 96 45 FB
      :     54 28 14 C6 8E F3 B1 CE C4 2C BD 0B 81 A0 D9 64
      :     2A 11 79 0A FE 81 89 ED 0C 9C 7E 4C ED EE BA 8B
      :     C5 07 FC CE B2 C6 B0 C6 13 67 C3 EE 08 87 F8 99
      :     F9 80 3A 54 14 A1 18 D8 C9 3F 9A 1B 7F 82 C7 F0
      :     7D 33 3B F9 25 54 FB 36 14 40 0B C2 B2 0E BE 7D
      :     55 82 96 AE 71 D5 8B 88 E4 F6 3D 5C 2B 87 EC 6E
      :     72 4D BD F4 7D 57 BC C1 6A EF D1 E6 95 05 F3 CA
      :     4A CF 17 64 2C 0B 5C AD AF 26 F3 46 D2 C8 1F 20
      :     5B 9C 48 96 80 F2 2C FB A1 8E 8B 56 C7 DF 62 99
      :     3F
590 3:     INTEGER 65537
      :     }
      :     }
595 395:     [3] {
599 391:     SEQUENCE {
603 15:     SEQUENCE {
605 3:     OBJECT IDENTIFIER basicConstraints (2 5 29 19)
610 1:     BOOLEAN TRUE
613 5:     OCTET STRING, encapsulates {
615 3:     SEQUENCE {
617 1:     BOOLEAN TRUE
      :     }
      :     }
620 88:     SEQUENCE {
622 3:     OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
627 81:     OCTET STRING, encapsulates {
629 79:     SEQUENCE {
631 77:     SEQUENCE {
633 4:     OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
639 69:     SEQUENCE {
641 67:     SEQUENCE {
643 8:     OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
653 55:     IA5String
      :     'http://www.firma.infocert.it/documentazione/manu'
      :     'ali.php'
      :     }
      :     }
      :     }
      :     }
710 37:     SEQUENCE {
712 3:     OBJECT IDENTIFIER issuerAltName (2 5 29 18)
717 30:     OCTET STRING, encapsulates {
719 28:     SEQUENCE {
721 26:     [1] 'firma.digitale@infocert.it'
      :     }

```

```

:
:
749 195: SEQUENCE {
752 3:   OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
757 187:   OCTET STRING, encapsulates {
760 184:     SEQUENCE {
763 181:       SEQUENCE {
766 178:         [0] {
769 175:           [0] {
772 40:             [6] 'http://crl.infocert.it/crls/tss2/ARL.crl'
814 130:             [6]
:             'ldap://ldap.infocert.it/cn%3DInfoCert%20Time%20S'
:             'tamping%20Authority%202,ou%3DTSA,o%3DINFOCERT%20'
:             'SPA,C%3DIT?authorityRevocationList'
:           }
:         }
:       }
:     }
:   }
:
947 14: SEQUENCE {
949 3:   OBJECT IDENTIFIER keyUsage (2 5 29 15)
954 1:   BOOLEAN TRUE
957 4:   OCTET STRING, encapsulates {
959 2:     BIT STRING 1 unused bit
:     '1100000'B
:   }
:
963 29: SEQUENCE {
965 3:   OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
970 22:   OCTET STRING, encapsulates {
972 20:     OCTET STRING
:     07 36 16 18 B5 0E FD 77 8F 5D 68 25 F2 38 FD 6F
:     34 26 F5 F7
:   }
:
: }
:
994 13: SEQUENCE {
996 9:   OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1007 0:   NULL
: }
1009 257: BIT STRING
: 4E CB 99 48 10 A8 8F 80 68 80 D4 C5 FE EE F7 E0
: 42 3E 65 AB B8 A7 84 18 F5 B1 7B 2B 66 C7 E7 6C
: 60 0F E1 91 3D D4 7D 25 02 80 5F 1E 36 A6 F0 1E
: 91 54 D9 C2 7F 32 01 80 5B D4 29 57 58 5E 1B BE
: F3 C9 98 B2 55 87 DB 17 CB 4D B9 F0 8F 7C F3 D9
: 34 FF 73 EB EA 14 3D 9E E1 7E 7E 7C 42 08 05 C3
: B0 A8 11 D2 D6 C9 1D 80 59 74 24 A9 0B FC 5B 45
: 4D 1B 4E 6D 27 61 3C E4 42 45 D9 BE FF 28 7E 25
: 0C 65 D4 D8 45 9D 76 5F 09 D5 22 8F 50 5C 84 B3
: A7 3D 78 20 DD 98 1E F1 79 59 A0 A4 C7 36 F2 A9
: B2 F0 3B 2D 9D 4D E1 EB F8 21 7B 9D 60 B0 CF 64
: 21 A2 C7 C3 FA 05 1F AA 7B 08 DA DA 7C 2C 75 63
: 9A 16 83 F1 77 7D 8B B5 E0 85 DB 33 CA B0 22 54
: 46 42 2C E1 86 F2 28 A2 53 3A 99 13 65 66 CA D5
: 47 47 34 88 F8 1C 75 68 EE 65 68 F9 57 38 B2 A1
: 76 BC FD 87 15 37 B4 EB B8 56 A5 BF AF 53 46 48
: }

```

Qualified time stamp root "Qualified InfoCert Time Stamping Authority 2"

```

0 1810: SEQUENCE {
4 1274:   SEQUENCE {
8 3:     [0] {
10 1:       INTEGER 2
:     }
13 1:     INTEGER 1
16 13:    SEQUENCE {
18 9:     OBJECT IDENTIFIER
:       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
29 0:     NULL
:   }

```

```

31 127: SEQUENCE {
33 11:   SET {
35 9:     SEQUENCE {
37 3:       OBJECT IDENTIFIER countryName (2 5 4 6)
42 2:       PrintableString 'IT'
      :     }
      :   }
46 21:   SET {
48 19:     SEQUENCE {
50 3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
55 12:      UTF8String 'INFOCERT SPA'
      :     }
      :   }
69 12:   SET {
71 10:     SEQUENCE {
73 3:       OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
78 3:       UTF8String 'TSA'
      :     }
      :   }
83 20:   SET {
85 18:     SEQUENCE {
87 3:       OBJECT IDENTIFIER serialNumber (2 5 4 5)
92 11:      PrintableString '07945211006'
      :     }
      :   }
105 53:   SET {
107 51:     SEQUENCE {
109 3:       OBJECT IDENTIFIER commonName (2 5 4 3)
114 44:      UTF8String
      :       'InfoCert Qualified Time Stamping Authority 2'
      :     }
      :   }
160 30: SEQUENCE {
162 13:   UTCTime 28/06/2016 14:18:40 GMT
177 13:   UTCTime 28/06/2026 15:18:40 GMT
      :   }
192 127: SEQUENCE {
194 11:   SET {
196 9:     SEQUENCE {
198 3:       OBJECT IDENTIFIER countryName (2 5 4 6)
203 2:       PrintableString 'IT'
      :     }
      :   }
207 21:   SET {
209 19:     SEQUENCE {
211 3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
216 12:      UTF8String 'INFOCERT SPA'
      :     }
      :   }
230 12:   SET {
232 10:     SEQUENCE {
234 3:       OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
239 3:       UTF8String 'TSA'
      :     }
      :   }
244 20:   SET {
246 18:     SEQUENCE {
248 3:       OBJECT IDENTIFIER serialNumber (2 5 4 5)
253 11:      PrintableString '07945211006'
      :     }
      :   }
266 53:   SET {
268 51:     SEQUENCE {
270 3:       OBJECT IDENTIFIER commonName (2 5 4 3)
275 44:      UTF8String
      :       'InfoCert Qualified Time Stamping Authority 2'
      :     }
      :   }
321 546: SEQUENCE {
325 13:   SEQUENCE {
327 9:     OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
338 0:     NULL
      :   }
340 527: BIT STRING, encapsulates {
345 522:   SEQUENCE {

```

```

349 513:      INTEGER
      :      00 9F AB C7 3F 53 A6 89 34 EF 57 D7 FA 95 51 7A
      :      13 40 B9 99 25 1C BA 39 6E 8C 70 CD 49 5E 66 D4
      :      5D EC 6C 82 2F F7 B2 16 87 D3 ED BF 07 CF 58 5B
      :      0C A8 EC 5C 8C CE E9 D6 14 7A 52 F9 72 5F 4B C8
      :      16 7E 5C CE 78 06 10 88 0A C8 8C 24 B4 60 A8 2D
      :      7D 3D 0A AA 83 50 FA F5 CA 9A 91 C9 56 A6 D8 66
      :      61 C9 46 46 89 50 07 2F 52 73 70 8C 54 F8 84 6B
      :      C5 19 DC 7B B4 69 3B 6B 37 52 2F E0 F3 5C 8D 06
      :      CB F8 E7 7E A6 36 69 27 8C 04 EA 3C CD 2E A7 2D
      :      31 7B 6D E8 9D 41 2B DA F4 F9 07 98 31 FB BA B1
      :      88 20 17 B7 3F 9A 57 09 3F F6 AD 6C CC 7F 3A 41
      :      EE 72 E1 AF E0 8D 74 5F 0F 66 29 21 9C 4F C9 43
      :      19 2B 77 4F A7 F7 61 3D 9B 25 B5 E9 33 81 F7 A8
      :      1F AD 11 7E 3D E4 E9 44 99 05 13 57 34 B0 A2 45
      :      58 FD 8D 0F 37 70 7D C4 BD F3 D7 B6 E5 7C 1C 8F
      :      AE 26 2A AF E8 17 CC 46 EC 50 A5 DC 62 59 BA 54
      :      2F D9 B3 E1 9F A3 5C D5 CE 80 DE 5D 37 F6 7E BD
      :      80 8D 2D 9C 3F C0 1E 0F DA B0 23 EE 5D B7 71 11
      :      0C EB 87 E7 2E 48 61 71 FF B5 FE 83 69 DB 4F E2
      :      7D 86 B3 46 A3 11 FD 1E 38 BC 1B 03 70 E1 2A E0
      :      73 BD 05 45 C7 7E 87 BC 46 0F AE BA C7 5E B1 76
      :      08 32 62 1A 7E 8F 6D EE 71 82 CB 3E B6 FA 61 E8
      :      56 21 32 0F 86 58 96 F2 C7 DC 83 6B C7 81 E5 CE
      :      29 CE AA A6 20 63 8F C3 78 A3 F6 5E 8B 41 62 B0
      :      A4 CF 49 5B D3 ED EA A0 97 3B D5 D0 82 99 F2 48
      :      39 CE 8B 82 22 B8 DC 78 27 E1 A2 74 14 8E 18 B2
      :      E4 F0 CE FA 19 AA 40 A8 0A 44 AC E3 79 F4 99 53
      :      0E C8 23 29 BB 80 71 7D 8B 0E AF B7 B5 A7 17 F7
      :      8A E2 53 19 AC 71 86 0A BE 46 26 FC 22 62 8A A7
      :      4E 08 25 3F D5 19 20 39 1E ED 0B D2 4D 38 8E 1A
      :      15 5B F5 D1 C7 AC BE DE 04 7D D5 8E EE 89 63 51
      :      B6 33 FA ED 6A 57 CB 7B B9 F1 38 B2 39 B4 8D CD
      :      FF
866 3:      INTEGER 65537
      :      }
      :      }
871 407:    [3] {
875 403:    SEQUENCE {
879 15:    SEQUENCE {
881 3:      OBJECT IDENTIFIER basicConstraints (2 5 29 19)
886 1:      BOOLEAN TRUE
889 5:      OCTET STRING, encapsulates {
891 3:        SEQUENCE {
893 1:          BOOLEAN TRUE
      :        }
      :      }
896 88:    SEQUENCE {
898 3:      OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
903 81:      OCTET STRING, encapsulates {
905 79:        SEQUENCE {
907 77:          SEQUENCE {
909 4:            OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
915 69:            SEQUENCE {
917 67:              SEQUENCE {
919 8:                OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
929 55:                IA5String
      :                'http://www.firma.infocert.it/documentazione/manu'
      :                'ali.php'
      :              }
      :            }
      :          }
      :        }
896 37:    SEQUENCE {
988 3:      OBJECT IDENTIFIER issuerAltName (2 5 29 18)
993 30:      OCTET STRING, encapsulates {
995 28:        SEQUENCE {
997 26:          [1] 'firma.digitale@infocert.it'
      :        }
      :      }
1025 207:    SEQUENCE {
1028 3:      OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)

```

```

1033 199:         OCTET STRING, encapsulates {
1036 196:             SEQUENCE {
1039 193:                 SEQUENCE {
1042 190:                     [0] {
1045 187:                         [0] {
1048 40:                             [6] 'http://crl.infocert.it/crls/qtss/ARL.crl'
1090 142:                             [6]
                                'ldap://ldap.infocert.it/cn%3DInfoCert%20Qualifie'
                                'd%20Time%20Stamping%20Authority%202,ou%3D TSA,o%3'
                                'DINFOCERT%20SPA,c%3DIT?authorityRevocationList'
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}

1235 14: SEQUENCE {
1237 3:     OBJECT IDENTIFIER keyUsage (2 5 29 15)
1242 1:     BOOLEAN TRUE
1245 4:     OCTET STRING, encapsulates {
1247 2:         BIT STRING 1 unused bit
        :         '1100000'B
        :     }
    }

1251 29: SEQUENCE {
1253 3:     OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1258 22:    OCTET STRING, encapsulates {
1260 20:    OCTET STRING
        :        AE 92 81 E5 30 55 6D C8 4A 74 78 A1 71 6D 3F 39
        :        02 FE 58 87
        :    }
    }

1282 13: SEQUENCE {
1284 9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1295 0:     NULL
    }

1297 513: BIT STRING
        : 39 46 9B E9 7A 02 72 D5 F8 11 D4 94 42 80 26 CE
        : 2F DD 56 82 92 D5 68 05 14 D2 F0 C8 0C 5B 11 CF
        : 88 F0 94 3D 66 B9 B8 52 35 B1 E5 A1 9C 83 2C F3
        : 5B 4E AA 2E D8 B1 75 61 E0 FB 96 86 0C EC AB F6
        : 2A A8 5B 61 C7 20 46 32 48 75 01 52 23 09 7E 7D
        : 88 41 B5 80 0D 0B 0F 8F 63 7F D5 4B 25 58 7A D3
        : 4A 5C 1C DA B2 83 5F BF B5 CB 9F 73 08 BD 17 84
        : 57 5F 8E 6D 9B 15 6F 21 03 8A 9C 3E 94 03 34 D9
        : A4 08 62 08 03 39 38 9B F6 1B C6 D3 FB 1D BD DE
        : 23 E9 FA F5 62 73 2E EC 1E 9B 18 40 24 BE 45 8B
        : E8 A6 F6 79 FC EB 98 60 C7 9D 85 E6 C8 4C CC AB
        : 14 10 2A 50 AD 96 90 76 A9 82 BB D1 F9 91 48 1B
        : B5 5B A5 E7 6B D3 C8 E6 D4 C8 9A 44 30 9F E1 DF
        : C2 B5 6F ED 7D E7 E6 3C 01 07 BA 28 DA E4 06 E0
        : 04 22 6F 50 0F 58 74 A3 F1 71 B2 CD 74 68 27 73
        : CF 14 31 91 F8 14 F5 13 E0 6A ED 00 7D D6 10 D8
        : 69 94 99 37 DD A4 B1 83 41 46 75 9C BC 7D 7F 2C
        : A5 E3 46 6E AC C9 AE 75 87 F0 FD AC C5 52 12 EC
        : F3 FB 89 78 00 E7 C7 40 C6 59 98 F5 FA 15 6D 79
        : 8D AE 88 4A 60 F9 E3 61 6C 20 0A 48 61 7D D0 69
        : 4B 9E 27 A7 0E 81 2D 12 FB 12 78 11 4A EF 96 B5
        : 6D D4 E1 D1 4C 46 15 25 70 E6 BA 07 45 62 0C 8C
        : 77 D0 67 5D 07 6C 1C A3 59 4F E5 FE A3 F0 DF 8C
        : D5 9A BA 30 B5 35 8E 36 10 DA 20 7C E4 69 EA 17
        : 2C A4 72 32 E0 D4 30 92 DF B3 79 41 F1 C9 83 DC
        : 90 DF 69 4A 14 39 2F CE 7D CE 1A 03 62 7A 82 0D
        : 79 A5 BD FC 69 25 9D 05 71 97 1D A3 C3 BF 06 EF
        : EE 1D E5 2F BE CB 26 AC 7A 84 2F 1F AF D1 5A D9
        : 4A CC 97 11 70 27 4F 35 78 1E 74 10 8C AD 58 A9
        : 54 8D 6A 05 B0 5C 51 A6 6E 5F 5D 40 5A 25 53 CD
        : 7A EF 82 F4 FC 89 06 5C 0E CE BA 2C 18 B2 7F 90
        : D3 0C AF 56 B1 17 15 47 6A DA 40 3D 3E 32 EA D4
        : }

```

Time stamp root "InfoCert Time Stamping Authority 3"

```

0 1755: SEQUENCE {
4 1219: SEQUENCE {
8 3: [0] {
10 1: INTEGER 2
:
13 1: INTEGER 1
16 13: SEQUENCE {
18 9: OBJECT IDENTIFIER
: sha256WithRSAEncryption (1 2 840 113549 1 1 11)
29 0: NULL
:
31 126: SEQUENCE {
33 11: SET {
35 9: SEQUENCE {
37 3: OBJECT IDENTIFIER countryName (2 5 4 6)
42 2: PrintableString 'IT'
:
:
46 24: SET {
48 22: SEQUENCE {
50 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
55 15: UTF8String 'InfoCert S.p.A.'
:
:
72 12: SET {
74 10: SEQUENCE {
76 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
81 3: UTF8String 'TSA'
:
:
86 26: SET {
88 24: SEQUENCE {
90 3: OBJECT IDENTIFIER '2 5 4 97'
95 17: UTF8String 'VATIT-07945211006'
:
:
114 43: SET {
116 41: SEQUENCE {
118 3: OBJECT IDENTIFIER commonName (2 5 4 3)
123 34: UTF8String 'InfoCert Time Stamping Authority 3'
:
:
159 30: SEQUENCE {
161 13: UTCTime 07/06/2021 08:19:06 GMT
176 13: UTCTime 07/06/2033 09:19:06 GMT
:
191 126: SEQUENCE {
193 11: SET {
195 9: SEQUENCE {
197 3: OBJECT IDENTIFIER countryName (2 5 4 6)
202 2: PrintableString 'IT'
:
:
206 24: SET {
208 22: SEQUENCE {
210 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
215 15: UTF8String 'InfoCert S.p.A.'
:
:
232 12: SET {
234 10: SEQUENCE {
236 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
241 3: UTF8String 'TSA'
:
:
246 26: SET {
248 24: SEQUENCE {
250 3: OBJECT IDENTIFIER '2 5 4 97'
255 17: UTF8String 'VATIT-07945211006'
:
:
274 43: SET {
276 41: SEQUENCE {

```

```

278 3:          OBJECT IDENTIFIER commonName (2 5 4 3)
283 34:         UTF8String 'InfoCert Time Stamping Authority 3'
      :         }
      :       }
319 546:      SEQUENCE {
323 13:        SEQUENCE {
325 9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
336 0:         NULL
      :       }
338 527:      BIT STRING, encapsulates {
343 522:        SEQUENCE {
347 513:         INTEGER
      :         00 E2 74 6C AF FB 6F 8E 1C AF C0 BF 47 F6 6B F9
      :         0A B2 58 C9 13 38 EC 92 5C B1 5C 48 2C 45 47 5E
      :         8A 2C 52 D7 E0 19 D7 BC F8 C6 F2 97 C8 2A B6 76
      :         8C 22 3C CD 75 9D E7 2E D2 8B E7 61 8C 63 71 A2
      :         2C DE B3 0C B7 ED 0D 3B C1 8A 87 CC 64 9B 05 07
      :         BA 06 1A 17 19 AC C6 DD 8E D0 B3 2B B5 CD 0A C7
      :         18 89 AA 3C 21 4F AB 84 92 CF E0 FA 05 D3 DD EC
      :         F6 8C EB E8 0D 0A 96 1E 3D 43 E0 6D 10 38 F4 80
      :         74 4E 7A FA EF D9 3E A5 DF BE A8 9A 13 1F 1F 20
      :         1B B4 E9 A7 65 E9 3E 11 6C 2F 04 33 00 CC 92 8F
      :         49 34 83 31 F8 A2 19 34 F3 C0 31 70 1A C2 A3 81
      :         03 8D C8 6E 25 3C DE 8A C8 7F 16 9B A7 B9 CD D4
      :         7D 8D 8F F2 8D 33 1F 79 4C 3C 71 75 BE 1C C2 7E
      :         BF 9F 76 72 D9 99 C2 C5 6D 01 69 EF 4C 14 7A 54
      :         A8 89 6A 9C 8F 19 1F FA 03 15 A6 F2 6B 69 4C 04
      :         F5 6A 40 ED 11 02 2D DC 70 58 62 25 45 DA E9 68
      :         91 2F C4 8C 60 D3 7F 56 A2 40 D3 6D 2A 03 3D D2
      :         2A B8 15 49 7D AB A8 19 FF DB 98 78 37 98 54 CB
      :         F9 BA 7A F2 57 FF B7 D8 54 34 97 63 18 A4 01 9B
      :         7F E0 3C C5 ED E7 1C 14 BF 4E 8F CB A2 B2 24 0F
      :         8B CD 97 AD 80 A7 42 12 5E DF 2E C5 D6 61 86 83
      :         72 6B 02 C5 45 E7 69 C6 49 64 D7 B3 43 59 29 DC
      :         6E 91 8D 80 DD 11 2B A0 7B EF F9 08 AF B3 A3 97
      :         18 87 04 AA FB 08 6D 1C C9 AE FD 77 64 D4 CA 2D
      :         06 A9 D2 29 43 25 D0 E4 00 DD D7 3A 51 BA 6A 36
      :         9B A2 98 E3 72 BE 42 FB 8D 4A DD C6 35 95 05 BD
      :         3F E6 21 0A 70 20 19 E9 1F FC 19 40 A5 45 0A 2D
      :         CE F7 01 EF 58 7F D7 56 3D 79 87 98 56 E6 D7 5F
      :         88 63 9E 9F DE 6D D9 67 19 EF 28 66 11 84 AE 31
      :         A1 43 C1 24 C7 15 42 56 42 33 AE 4E 3E 43 F5 EC
      :         98 79 7E CD 20 71 04 74 17 8D 26 37 1C 5A DC DA
      :         A9 09 6D 44 C8 F6 BB B9 B4 3D 63 5B 33 66 7F 05
      :         55
864 3:         INTEGER 65537
      :       }
      :     }
869 354:    [3] {
873 350:      SEQUENCE {
877 15:        SEQUENCE {
879 3:         OBJECT IDENTIFIER basicConstraints (2 5 29 19)
884 1:         BOOLEAN TRUE
887 5:         OCTET STRING, encapsulates {
889 3:           SEQUENCE {
891 1:             BOOLEAN TRUE
      :           }
      :         }
894 88:      SEQUENCE {
896 3:        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
901 81:        OCTET STRING, encapsulates {
903 79:          SEQUENCE {
905 77:            SEQUENCE {
907 4:              OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
913 69:              SEQUENCE {
915 67:                SEQUENCE {
917 8:                  OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
927 55:                  IA5String
      :                  'http://www.firma.infocert.it/documentazione/manu'
      :                  'ali.php'
      :                }
      :              }
      :            }
      :          }
      :        }
      :      }
      :    }

```

```

:      }
:      }
984 193: SEQUENCE {
987   3:   OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
992 185:   OCTET STRING, encapsulates {
995 182:     SEQUENCE {
998 179:       SEQUENCE {
1001 176:         [0] {
1004 173:           [0] {
1007 38:             [6] 'http://crl.infocert.it/ca3/tsa/ARL.crl'
1047 130:             [6]
:               'ldap://ldap.infocert.it/cn%3DInfoCert%20Time%20S'
:               'tamping%20Authority%203,ou%3DTSA,o%3DINFOCERT%20'
:               'SPA,c%3DIT?authorityRevocationList'
:             }
:           }
:         }
:       }
:     }
:   }
: }
1180 14: SEQUENCE {
1182   3:   OBJECT IDENTIFIER keyUsage (2 5 29 15)
1187   1:   BOOLEAN TRUE
1190   4:   OCTET STRING, encapsulates {
1192   2:     BIT STRING 1 unused bit
:       '1100000'B
:     }
:   }
1196 29: SEQUENCE {
1198   3:   OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1203 22:   OCTET STRING, encapsulates {
1205 20:     OCTET STRING
:         2D 92 36 1F 33 B5 37 08 A8 4A 76 1C 1B 21 F1 77
:         C2 9F FA 44
:     }
:   }
: }
1227 13: SEQUENCE {
1229   9:   OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1240   0:   NULL
:   }
1242 513: BIT STRING
:   BC 1B 66 5F 2F 0B AA 17 DA 1D 82 62 F9 64 C8 9D
:   61 01 48 06 27 F2 2E 38 64 67 11 7B D5 4B 87 4A
:   91 03 E9 FB 75 26 47 8D 18 9D D1 B5 BB 40 93 7B
:   23 56 C7 AF 21 CA 45 DF AD EB 01 86 86 AD 16 D8
:   63 7F DE 3E C4 83 29 3B 65 B3 35 1A 77 CA 7A B7
:   53 DB DF 9C EB DD A1 45 24 05 CB D7 BE BE DE 2B
:   E6 D1 9D 21 5F 10 D1 33 17 EB 1E DD 55 5D 21 25
:   0E 9D 6E 65 35 D6 AA A4 81 AF F5 57 FD E5 72 73
:   22 0F 28 03 FE 1E 89 90 56 13 61 FA 97 08 95 3D
:   DE EB CA 6A 22 6C 86 4B 9F 0E 30 D1 97 C8 37 12
:   AF 83 EC 2C 77 82 F0 48 F2 EC 77 61 63 0F 59 86
:   94 D9 00 48 59 3D E7 C2 3C 34 5E 4C 37 30 A2 54
:   9D D7 6D C7 35 6B ED F3 F2 43 BA 7B 9C 6C 75 32
:   F6 9C 7A 20 79 60 55 64 B3 92 AA 82 68 4D 02 BC
:   4B 60 A6 DB E6 B6 DB 06 2E 96 A2 4B BE 1B 89 0D
:   3B A1 5D 39 0C E0 24 52 2A C2 B9 E8 75 68 64 A5
:   3F 44 DB B8 4F D7 48 31 32 39 F2 4F B6 94 B6 21
:   B5 1F 78 C7 47 65 6E BF 85 54 E5 B0 82 15 92 36
:   1B 74 65 0C 8E 43 9B 4E 05 B1 C3 A7 CE 1B 8F 64
:   F4 1E 89 76 32 04 89 F7 17 02 1D A4 1A B2 9B 90
:   E2 29 EA D0 DA 72 A9 2C EB 87 AA 7C 12 B2 EA B6
:   8A 7F F2 39 0F 71 E2 62 EC FE 99 55 95 BF 61 F7
:   33 D3 BF F1 C3 5E 77 D0 EB 3D AC BE 73 22 7A 6B
:   1B B9 F8 FE 44 C0 3D 4F F0 E7 6E 97 89 74 F1 F4
:   56 58 8E 4B 05 A9 BE 6B D8 B5 35 64 A6 75 97 69
:   E3 C5 70 67 BE DD 5B 4B B6 6E F1 27 E9 E0 E2 06
:   D8 FE CF 7E 1D C5 54 3F CC 90 3C 04 79 22 F8 5D
:   CC 06 BC 3A 99 ED 95 44 9E C3 34 4F 31 8B DE 2F
:   E0 D9 66 3E 71 7E 82 72 82 0B E1 D7 D4 41 2D 04
:   AE 82 2D C8 85 6B 1B 8D 23 3D 4A 99 CD D5 07 A5
:   3C 98 B6 D2 08 22 9C 35 0A 34 03 4A 85 3F 89 3B
:   D2 38 A3 F3 E0 76 68 9F DA 23 0B 5F EE 1D C7 4C
: }

```

Avvertenza

Alcuni formati permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. I file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 25 comma 2 del Regolamento [1], ossia non può considerarsi equivalente rispetto a una firma autografa. È cura del Titolare assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tale codice eseguibile.