Servizi di validazione elettronica temporale conformi al Regolamento eIDAS

TSA Practice Statement

DOCUMENTO DI POLICY

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima Emissione	15/09/2016
01	Revisione delle parti sotto indicate: 1. Par. 5.6: esplicitazione dei tempi di comunicazione degli incidenti, in coerenza con l'articolo 19 del Regolamento 910/2014; 2. Par. 7.8: esplicitazione del caso di negligenza nell'ambito delle esclusioni per limitazioni di responsabilità (introduzione del concetto di colpa, rispetto al limitativo colpa grave, che escludeva la negligenza), 3. Par. 7.9: collegamento del limite di responsabilità per danni causati a seguito di dolo o negligenza alla copertura assicurativa; 4. 0 7.11: esclusione dell'applicabilità del Codice del Consumo; 5. Par. 8.3: chiarimento sulla disponibilità delle informazioni afferenti i certificati revocati e sospesi.	06/12/2016
02	Revisione delle parti sotto indicate: 1. Modifica al titolo del documento 2. Par.1.2.1: Aggiornamento del nominativo dell'Amministratore Delegato 3. Par. 1.5: Aggiornamento dei riferimenti normativi	27/02/2019
03	Introduzione nuovo certificato CA di TSA	29/04/2021

Indice degli argomenti

1 Introduzione

Nel presente documento sono illustrate le modalità ed i processi operativi utilizzati da **Telecom Italia Trust Technologies S.r.l.** (in breve TI.TT) in qualità di Prestatore di Servizi Fiduciari Qualificati per l'erogazione di Servizi Fiduciari di Validazione Temporale Elettronica e Validazione Temporale Elettronica Qualificata (di qui in avanti i **SERVIZI**) come definiti dagli articoli 41 e 42 del Regolamento [eIDAS].

Il presente documento è redatto sulla base della specifica pubblica RFC3647:

- costituisce il **Manuale Operativo** e **Certification Practice Statement (**di qui in avanti solo **CPS)** con la descrizione di:
- modalità operative dei **SERVIZI**;
- ruoli, responsabilità e pratiche di tutti i soggetti coinvolti nel ciclo di vita, uso e gestione dei **SERVIZI**.
- è pubblicato a garanzia dell'affidabilità dei **SERVIZI** di TI.TT nei confronti degli utilizzatori finali ed è liberamente disponibile per la consultazione ed il download sul sito: https://www.trusttechnologies.it/download/documentazione/.

1.1 Identificazione del CPS

L'OID per TI.TT è {iso(1) identified-organization(3) uninfo(76) Telecom Italia Trust Technologies S.r.l. (33)}: 1.3.76.33

Questo CPS è indicato, nei certificati, col seguente Object Identifier (OID): 1.3.76.33.1.1.200.

TI.TT definisce ed organizza i suoi OID per i vari certificati e documenti di cui al presente CPS come segue:

TI.TT	*1.3.76.33*
Certification Service Provider	*1.3.76.33.1*
Certification Practice Statements	*1.3.76.33.1.1*
CPS TI.TT eIDAS TSA	*1.3.76.33.1.1.200*

1.2 Caratteristiche dei SERVIZI

Il servizio di Validazione Temporale Elettronica permette di attribuire ad uno o più documenti informatici un riferimento temporale opponibile ai terzi, costituito da una data ed un'ora certe asseverate mediante la generazione di una Marca Temporale (time-stamp token).

Ciascuna Marca generata ed apposta su un documento informatico è indissolubilmente legata al documento stesso grazie a riferimenti certi (impronta del documento, numero progressivo seriale, identificativo della CA).

Con l'associazione di un riferimento temporale ai propri documenti elettronici l'utente può dimostrare la loro esistenza ad un determinato istante e dare loro la validità legale corrispondente alla tipologia di firma utilizzata per la sottoscrizione.

1.2.1 Dati identificativi del Prestatore dei SERVIZI

Telecom Italia Trust Technologies S.r.l. è identificata come segue:

Denominazione sociale:	Telecom Italia Trust Technologies S.r.l.
Indirizzo della sede legale:	S. R.148 Pontina Km.29,100 – 00071 Pomezia
Legale rappresentante:	Salvatore Nappi (Amministratore Delegato)
P.IVA e Codice Fiscale:	04599340967
N° di telefono:	06911971
ISO Object Identifier (OID):	1.3.76.33

Sito web generale (informativo):	https://www.trusttechnologies.it/
Indirizzo servizio fiduciario:	https://tss.trusttechnologies.it
Indirizzo di posta elettronica:	CRPresidio_CA@telecomitalia.it

1.2.2 Time Stamping Policy

TI.TT eroga i **SERVIZI** in conformità alla "Best practices Time-Stamp Policy" (***BTSP***) definita nella norma [ETSI EN 319 421].

TI.TT dichiara la conformità a tale policy includendo il corrispondente object identifier nelle marche temporali.

L'OID è ***0.4.0.2023.1.1*** ed è così strutturato:

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

1.2.3 Time Stamping Authority (TSA)

TI.TT utilizza una CA dedicata (in seguito **CA di TSA** o semplicemente **TSA**) all'emissione dei certificati associati alle chiavi di marcatura temporale delle TSU.

Di seguito vengono riportate le informazioni necessarie ad identificare il certificato root della TSA:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=IT, O=Telecom Italia Trust Technologies S.r.l., OU=Servizi di certificazione, CN=TI Trust
Technologies eIDAS TSA
    Validity
      Not Before: Aug  2 08:53:38 2016 GMT
      Not After : Aug  2 08:53:38 2036 GMT
    Subject: C=IT, O=Telecom Italia Trust Technologies S.r.l., OU=Servizi di certificazione, CN=TI Trust
Technologies eIDAS TSA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
        Modulus:
        <omissis>
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:0
      X509v3 Certificate Policies:
        Policy: 1.3.76.33.1.1.200
          CPS: https://www.trusttechnologies.it/download/documentazione
      X509v3 CRL Distribution Points:
        Full Name:
          URI:http://ca.tipki.it/ETSA/CRL
      X509v3 Key Usage: critical
        Certificate Sign, CRL Sign
      X509v3 Subject Key Identifier:
        57:37:81:21:A6:C9:3C:F6:67:66:B7:2E:37:86:A4:DE:66:BB:22:84
  Signature Algorithm: sha256WithRSAEncryption
      <omissis>
```

Entro il primo semestre 2021 entrerà in esercizio il seguente certificato di TSA:

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=IT, O=Telecom Italia Trust Technologies S.r.l., OU=Qualified Trust Service Provider, CN=TI Trust Technologies QTSP TSA CA/2.5.4.97=VATIT-04599340967
Validity
Not Before: Apr 20 08:51:07 2021 GMT
Not After : Apr 20 08:51:07 2041 GMT
Subject: C=IT, O=Telecom Italia Trust Technologies S.r.l., OU=Qualified Trust Service Provider, CN=TI Trust Technologies QTSP TSA CA/2.5.4.97=VATIT-04599340967
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
<omissis>
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: https://www.trusttechnologies.it/download/documentazione

X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
23:83:68:C6:18:5A:AF:64:E2:03:01:86:31:89:43:65:C2:FF:BF:30
Signature Algorithm: sha256WithRSAEncryption
<omissis>

1.2.4 Soggetto richiedente (*Subscriber*)

I Soggetti richiedenti, ovvero i Subscriber, sono:

- Enti, aziende, istituti ed altri soggetti appartenenti alla Pubblica Amministrazione;
- Persone giuridiche che intendono far utilizzare i **SERVIZI** alle persone fisiche ad esse direttamente afferenti, ovvero ad esse collegate da uno specifico rapporto contrattuale (si veda in proposito il par. 3.2). Tali persone fisiche costituiscono i Titolari dei certificati, ovverosia gli utenti finali dei **SERVIZI**;
- Persone fisiche, a titolo privato.

Parte dei livelli di servizio garantiti per l'insieme delle attività inerenti l'emissione delle marche temporali e della gestione dei **SERVIZI** possono essere definiti nell'ambito degli specifici contratti stipulati con l'acquirente dei certificati.

1.2.5 Utilizzatori (*Relying Parties*)

Gli Utenti finali, utilizzatori dei **SERVIZI**, sono tutti i soggetti che fanno affidamento sulle informazioni contenute nelle marche temporali.

Un utilizzatore può anche essere Subscriber.

1.3 Amministrazione del CPS

Questo CPS è redatto, pubblicato ed aggiornato da TI.TT.

Richieste di informazioni o chiarimenti sul presente CPS possono essere inoltrate via posta elettronica all'indirizzo CRPresidio_CA@telecomitalia.it.

Questo CPS è approvato dal responsabile della sicurezza di TI.TT, di concerto con la Direzione, previo consulto con le funzioni aziendali coinvolte nell'erogazione dei **SERVIZI**.

1.4 Definizioni ed Acronimi

AgID	Agenzia per l'Italia Digitale	**LDAP**	Lightweight Directory Access Protocol
CA	Certification Authority	**OCSP**	On-line Certificate Status Protocol
CDP	CRL Distribution Point	**OID**	Object Identifier
CP	Certificate Policy	**PDF**	Portable Document Format
CPS	Certification Practice Statement	**PKI**	Public Key Infrastructure
CRL	Certificate Revocation List	**RA**	Registration Authority
CS	Centro Servizi	**SSL**	Secure Sockets Layer
CSR	Certificate Signing Request	**TLS**	Transport Layer Security
DN	Distinguished Name	**TSA**	Time Stamping Authority
FIPS	Federal Information Processing Standard	**TSR**	Time Stamp Request
HSM	Hardware Security Module	**TSS**	Time Stamping Server
HTTP	Hyper-Text Transfer Protocol	**TST**	Time Stamp Token
ISO	International Standards Organization	**TSU**	Time Stamping Unit

1.5 Riferimenti

# Rif.	Estremi
[ETSI EN 319 401]	ETSI EN 319 401 - "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
[ETSI EN 319 421]	ETSI EN 319 421 V1.1.1 - "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
[ETSI EN 319 422]	ETSI EN 319 422 - "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles"
[RFC 3161]	RFC 3161 - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)
[Normativa Privacy]	Regolamento Generale sulla Protezione dei Dati n. 2016/679/UE e s.m.i. Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n.123 della Gazzetta Ufficiale n. 174, 29 luglio 2003 e s.m.i.
[eIDAS]	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
[CAD]	Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (GU n.112 del 16-05-2005 - Suppl. Ordinario n. 93)
[FIPS 140-2]	FIPS PUB 140-2 - Federal Information Processing Standards Publication - Security Requirements for Cryptographic Modules

2 Pubblicazioni e Repository

Per "Repository" si intende un insieme di archivi o registri on-line contenenti informazioni di interesse pubblico relative ai certificati e al servizio di emissione e gestione degli stessi descritto in questo CPS.

2.1 Gestione del repository

Il "repository" di TI.TT è costituito dal sito web che gestisce in proprio e di cui è direttamente responsabile, disponibile all'indirizzo web:

https://www.trusttechnologies.it/download/documentazione/

2.2 Informazioni pubblicate

TI.TT pubblica sul proprio sito web la seguente documentazione:

- Certification Practice Statement (CPS)
- Certificate Policy (CP)
- Condizioni generali di utilizzo dei **SERVIZI**
- Modulistica
- Certificati e le CRL che concorrono all'erogazione dei **SERVIZI**.

Per la pubblicazione delle informazioni sui prezzi e sulle condizioni economiche per l'utilizzo dei **SERVIZI** si rimanda a quanto descritto nei paragrafi 7.1 (Soggetti e modello operativo) e 7.2 (Prezzo dei **SERVIZI**).

2.3 Tempi e frequenza delle pubblicazioni

TI.TT notifica con un preavviso di 30 giorni solari le modifiche che intende apportare al CPS, pubblicando nella sezione del sito in cui è disponibile una apposita nota informativa.

Allo scadere del preavviso il nuovo CPS e, se necessario anche la documentazione annessa, vengono pubblicati sul sito web di TI.TT.

I certificati utilizzati nell'erogazione dei **SERVIZI** vengono pubblicati al momento della loro emissione.

2.4 Controllo degli accessi

L'accesso al repository in sola lettura ("read-only") è completamente libero per chiunque.

L'accesso al repository per la pubblicazione di informazioni nuove o aggiornate è possibile solo da postazioni di lavoro di TI.TT attestate sulla medesima rete del repository, previa autenticazione.

3 Operatività dei SERVIZI

3.1 Richiesta di una marca temporale

L'accesso ai **SERVIZI** forniti dalla TSA e l'invio delle marche temporali in risposta al richiedente avvengono in conformità al protocollo ed ai formati definiti nella specifica [ETSI EN 319 422] ETSI EN 319 422 - "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles" e nella specifica [RFC 3161] RFC 3161 – "Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)" – e successive modificazioni.

La validazione elettronica temporale di un documento informatico può essere effettuata direttamente da un utente abilitato ai **SERVIZI** utilizzando l'applicativo fornito da TI.TT oppure un altro applicativo scelto direttamente dall'utilizzatore purché conforme al protocollo HTTPS come definito nella clausola 3.4 della [RFC 3161].

I **SERVIZI** sono raggiungibili sulla rete Internet agli indirizzi indicati da TI.TT e prevedono l'utilizzo dell'applicazione client fornita da TI.TT per richiedere la marca temporale ed associarla al documento previa autenticazione effettuata tramite UserID e Password.

A seconda dello strumento utilizzato, la richiesta di una Marca Temporale può pertanto essere effettuata nelle seguenti modalità:

- **client fornito da TI.TT:** (il software applicativo di TI.TT per firmare digitalmente qualsiasi documento elettronico e per verificare la firma di quelli ricevuti): l'utente seleziona un file da marcare temporalmente; il client si occupa dell'invio della richiesta a TI.TT e, dopo aver autenticato l'utente tramite **user name** e **password**, appone la marca temporale al documento.
- **applicativo scelto dal cliente**: l'utente dovrà preventivamente configurare il suo applicativo con i parametri propri dei **SERVIZI** TI.TT (url *https* di accesso, user name e Password e Policy OID della TSA) che saranno comunicati all'utente al momento dell'attivazione.

Per apporre la validazione elettronica temporale su **documenti in serie** (ad esempio, estratti conto inviati via web da una banca ai suoi clienti nell'ambito di applicazioni legacy), i clienti possono utilizzare una modalità alternativa all'applicazione desktop sopra descritta.

In questo caso si presuppone che il Cliente utilizzi una o più applicazioni server nelle quali siano state sviluppate le opportune interfacce per interagire con un servizio di validazione elettronica temporale, che risponda alle specifiche dello standard [RFC 3161].

Quando il Cliente richiede l'emissione di marche temporali utilizzando **applicativi integrati con i propri sistemi informativi**, TI.TT non assume, ovviamente, alcuna responsabilità sul loro funzionamento.

3.2 Emissione delle marche

In base alle diverse procedure e modalità previste dalla TSA, alla ricezione delle richieste inviate dagli utenti dei **SERVIZI**, il sistema elettronico TSU genera e firma in maniera automatica, dopo gli opportuni controlli, le marche temporali associate ai documenti informatici utilizzando un riferimento temporale preciso e sicuro (data ed ora) corrispondente al Tempo Universale Coordinato (UTC), assieme a tutte le altre informazioni contenute nella marca.

Attraverso un apposito algoritmo di Hash, l'utente calcola con il suo applicativo client l'impronta relativa all'evidenza informatica da sottoporre a validazione temporale ed invia la sua richiesta alla TSA che, successivamente, provvede alla generazione della marca temporale.

Il TSU effettua una serie di controlli automatici prima di procedere alla generazione delle marche.
I controlli automatici effettuati dal TSU prima di procedere alla generazione delle marche prevedono anche la verifica:

- delle credenziali di autenticazione fornite dal richiedente
- del formato della richiesta (TimeStampReq)
- del contenuto della richiesta, in particolare:
  - L'algoritmo utlizzato per il calcolo dell'hash del documento da marcare;

- L'O.I.D. della policy da utilizzare.

Se i controlli hanno esito positivo il TSU produce la marca temporale associando all'hash del documento ricevuto il riferimento temporale acquisito secondo quanto specificato in 5.5.
La marca temporale viene automaticamente inviata al richiedente in risposta al protocollo utilizzato per la richiesta.

3.3 Verifica delle marche temporali

La verifica di una marca temporale può essere effettuata utilizzando il client di firma fornito da TI.TT ai propri utenti o attraverso analoghi sw in possesso degli utenti finali.

3.4 Conservazione delle marche temporali

I **SERVIZI** di TI.TT garantiscono la conservazione di tutte le marche temporali emesse in un apposito archivio digitale non modificabile, per un periodo non inferiore a venti (20) anni.

Su richiesta dell'interessato, è possibile conservare le suddette marche per un periodo maggiore, secondo specifiche condizioni da concordare.

3.5 Servizi informativi sullo stato del certificato del TSU

TI.TT rende disponibile, a tutti gli interessati, i servizi di controllo dello stato dei certificati di marcatura temporale mediante pubblicazione della Certificate Revocation List (CRL). Lo stato dei certificati (attivo, sospeso, revocato) è visibile tramite la url contenuta nell'estensione CRL Distribution Point del certificato del TSU.

3.6 Obblighi dei soggetti esterni che supportano i SERVIZI

TI.TT utilizza soggetti esterni che effettuano su base contrattuale o delegata attività correlate all'erogazione dei **SERVIZI**. In modo particolare detti soggetti garantiscono:

- La piena operatività dei siti utilizzati per garantire l'erogazione in condizioni normali, la continuità operativa ed il disaster recovery dei **SERVIZI** (v. successivo capitolo 4);
- I servizi di connettività base per l'accesso ai predetti siti di erogazione dei **SERVIZI** (v. successivo capitolo 4);
- Gli interventi di manutenzione ordinaria ed evolutiva dell'applicativo di TSA (proprietario di TI.TT), secondo quando indicato dal sistema delle regole interne relativo alla realizzazione del prodotto/servizio (SGQSI - Sistema integrato di Gestione della Qualità e della Sicurezza delle Informazioni di TI.TT, certificato secondo la norma ISO 9001 e la norma ISO 27001).

Inoltre, per la gestione di alcuni processi di natura organizzativa e amministrativa, TI.TT utilizza risorse e servizi della Capo Gruppo TIM S.p.A. sulla base di specifici accordi o deleghe, in una cornice comune di policy, procedure e processi.

4 Misure di sicurezza fisica ed operativa

L'infrastruttura tecnologica, le procedure operative, le misure di sicurezza fisica e logica ed il personale preposto all'erogazione dei **SERVIZIO** sono gli stessi utilizzati nell'ambito del servizio TI.TT di emissione e gestione dei certificati qualificati per firma digitale a norma di legge.

4.1 Sicurezza fisica

Il Centro Servizi di TI.TT è ubicato presso il Data Center TIM di Pomezia 00071, con sede in S. R. 148 Pontina km 29,100.

Le misure di sicurezza implementate per la protezione fisica dei siti e dei locali che ospitano le piattaforme tecnologiche utilizzate per l'erogazione di tutti i servizi di certificazione digitale si articolano su 3 livelli.

4.1.1 I Livello (protezione fisica di confine)

Il primo livello di protezione è costituito dal confine di proprietà del sito che ospita il Data Center / Centro servizi ed impedisce l'accesso a soggetti e/o automezzi non autorizzati. La delimitazione fisica perimetrale sia che si riferisca a siti già esistenti sia che si tratti di nuove realizzazioni deve possedere idonei requisiti costruttivi quali altezza, spessore, materiali utilizzati, etc., ed essere integrata con sistemi attivi antintrusione, i cui principi di funzionamento offrano la massima affidabilità.

L'integrazione di protezioni attive e passive deve garantire la rilevazione attendibile degli eventi anomali (tentativi di intrusione, manomissioni, etc.) da parte del personale di Vigilanza. Tale funzione può essere soddisfatta da un sistema di videosorveglianza gestito dalla Vigilanza, che deve operare in un locale presso il quale saranno accentrati tutti i telecomandi di sicurezza e le segnalazioni di allarme.

Misure di sicurezza fisica per il primo livello di protezione sono:

- Protezione Perimetrale Esterna (mura, recinzioni, sistemi elettronici);
- Videosorveglianza analogica e digitale: un sistema di videosorveglianza a circuito chiuso (TVCC) con video registrazione, il controllo del perimetro è effettuato con impianti a raggi infrarossi;
- Sbarre / Cancelli esterni, la cui apertura è a cura del personale di Vigilanza;
- Controllo Accessi pedonali e carrai: un presidio di Vigilanza, che supervisiona i transiti, identifica i visitatori ed eventualmente autorizza l'accesso all'interno del sito;
- Illuminazione;
- Vigilanza h24x7;
- Edifici dedicati.

4.1.2 II Livello (protezione fisica di sito ambientale)

Il secondo livello di protezione implementato, coincidente con il perimetro che delimita l'area o le aree dedicate agli ambienti valutabili di considerevole rilevanza strategica e le aree uffici, tutela l'accesso ai siti stessi. Misure di sicurezza fisica per il secondo livello di protezione sono:

- Videosorveglianza analogica e digitale: un sistema di videosorveglianza a circuito chiuso (TVCC) con video registrazione;
- Controllo Accessi tramite badge (di prossimità) e/o con riconoscimento biometrico;
- Illuminazione, Bussole, Tornelli, Vetri antisfondamento, grate;
- Vigilanza h24x7;
- Frazionamento delle aree.

L'accesso ai siti è possibile solo attraverso un ingresso esterno regolamentato da sistemi di tornelli ad accesso singolo a lettura badge. Il controllo accessi riferito agli edifici che costituiscono le sedi di TI.TT avviene secondo quanto previsto dalle procedure di accesso ai siti di TIM.

4.1.3 III Livello (protezione fisica degli apparati)

Il terzo livello di protezione protegge le aree critiche che includono gli asset a maggior valore strategico e che costituiscono il core business aziendale. Sono considerate aree critiche, ad esempio:

- le Sale TLC, ambienti dedicati ad ospitare switch, router e firewall
- le Sale Sistemi, che ospitano i sistemi della CA
- le Cage, "spazi chiusi" completamente dedicati ai sistemi - realizzate all'interno di sale sistemi - compartimentate per mezzo di una gabbia metallica, al fine di offrire un alto livello di sicurezza dei sistemi.

Misure di sicurezza fisica per il terzo livello di protezione sono:

- Videosorveglianza analogica e digitale: un sistema di videosorveglianza a circuito chiuso (TVCC) con video registrazione;
- Controllo Accessi tramite badge (di prossimità) e/o con riconoscimento biometrico;
- Illuminazione;
- Bussole, Cage;
- Armadi blindati, Camere di sicurezza (Lamperz).

4.1.4 Descrizione dei Data Center TIM

I Data Center dove opera TI.TT sono conformi alle direttive del Gruppo TIM:

- hanno pareti esterne realizzate in cemento armato, con sale apparati delimitate da tramezzi realizzati con materiale da costruzione conforme alle norme antincendio;
- la Sala Sistemi di TI.TT a Pomezia, è dotata di un impianto di videocitofono utilizzato per mettere in comunicazione le persone che non fanno parte dell'organizzazione del Centro con il personale all'interno della sala stessa che è così in grado di vedere e riconoscere l'interlocutore esterno. È inoltre collegata mediante videocitofono con la Guardiola per le eventuali comunicazioni di servizio;
- tutti i supporti contenenti software di produzione e dei dati, audit, archivio o informazioni di backup vengono memorizzati all'interno di strutture con adeguati controlli di accesso fisici e logici volti a limitare l'accesso al personale autorizzato e proteggere tali supporti da danni accidentali (ad esempio, acqua, fuoco ed emissioni elettromagnetiche);
- i rilievi strumentali effettuati presso il Data Center, allo scopo di valutare i livelli di emissione del campo elettrico e magnetico prodotto dagli impianti ivi esistenti, permettono di evidenziare il rispetto dei limiti di esposizione, dei valori di attenzione e degli obiettivi di qualità previsti dal DPCM 8 luglio 2003. Si evidenzia che secondo quanto previsto dalla normativa sono presi come riferimento, per la valutazione dell'esposizione professionale del personale che opera nel Data Center, i limiti più cautelativi previsti per la popolazione;
- in tutti i locali protetti sono installati sensori volumetrici che rilevano i tentativi di passaggio nelle zone immediatamente sottostanti il sensore stesso e/o possibili mascheramenti. Questi sensori sono attivati dal personale della guardiania nell'orario di chiusura del Centro;
- l'energia elettrica è fornita da un sistema a doppia cabina di distribuzione, che implementa un meccanismo di ridondanza per garantire la continuità: i punti di allaccio alla rete sono serviti da una doppia alimentazione con possibilità di isolamento e manutenzione di tutti i componenti. Tutti i quadri che forniscono la corrente elettrica alle apparecchiature delle piattaforme di erogazione sono alimentati da gruppi di continuità;
- la continuità elettrica è garantita da gruppi statici di continuità, connessi in parallelo con modulo centrale di distribuzione e batterie con autonomia di molte ore. Tale impianto è asservito ad un sistema di gruppi elettrogeni di soccorso, di cui uno cabinato esterno, alimentati, all'occorrenza, tramite un deposito di combustibile costituito da serbatoi di gasolio di grande capacità;
- tutti gli ambienti sono dotati di rilevatori antifumo e sistemi antincendio con attivazione degli impianti di spegnimento automatico degli incendi a saturazione di ambiente. Tutte le segnalazioni dell'impianto antincendio sono tempestivamente riportate sia al presidio interno di manutenzione sia al presidio di

security, in modo che il personale addetto possa avvertire in tempi contenuti i soggetti individuati nello specifico piano di sfollamento della sede.

4.2 Sicurezza delle procedure

TI.TT definisce e mantiene un Piano della Sicurezza che analizza gli asset e descrive le misure tecniche ed organizzative atte a garantire un adeguato livello di sicurezza delle operazioni.

Tutte le procedure operative standard sono documentate e comprese nel Sistema integrato di Gestione della Qualità e della Sicurezza delle Informazioni di TI.TT, certificato secondo la norma ISO 9001 e la norma ISO 27001.

4.3 Sicurezza del personale

Il personale addetto al servizio ha una pluriennale esperienza nel campo della definizione, sviluppo e gestione di servizi di PKI ed ha ricevuto una adeguata formazione sulle procedure e gli strumenti da utilizzare nelle varie fasi operative.

4.4 Logging degli eventi

I dati degli eventi relativi al ciclo di vita delle chiavi e dei certificati, incluse le richieste di certificazione, sospensione o revoca, etc. sono registrati in forma cartacea o elettronica. Sono inoltre registrati anche altri eventi quali: gli accessi logici al sistema di gestione dei certificato, le operazioni svolte dal personale TI.TT, l'entrata e l'uscita di visitatori nei locali in cui si svolge l'attività di certificazione, etc.

Di ogni evento viene registrata la tipologia, la data e l'ora di occorrenza e, se disponibili, altre informazioni utili ad individuare gli attori coinvolti nell'evento e l'esito delle operazioni.

In nessun caso viene registrata nei log la chiave privata della CA in alcuna forma (in chiaro o cifrata).

L'insieme delle registrazioni costituisce l'Audit log (per la CA si parla anche di Giornale di Controllo): i file che lo compongono vengono trasferiti – con le modalità previste per ogni tipologia di log – tutti i giorni su supporto permanente, con garanzia di integrità ed inalterabilità del dato.

4.5 Archiviazione dei dati

TI.TT conserva e mantiene accessibili, per un periodo non inferiore a 20 anni, tutte le informazioni relative ai processi di emissione e gestione dei certificati, come le seguenti:

- le richieste di emissione,
- la documentazione fornita dai richiedenti,
- le CSR (Certificate Signing Request) fornite dai richiedenti,
- i dati anagrafici dei richiedenti e degli utilizzatori finali (ove siano soggetti diversi),
- i risultati delle verifiche svolte dalla CA (visure camerali, interrogazioni sui record WHOIS, ecc.),
- le richieste di revoca o sospensione,
- tutti i certificati emessi,
- gli audit log.

Una copia di sicurezza (backup) dei dati, delle applicazioni, del giornale di controllo e di ogni altro file necessario al completo ripristino del servizio viene effettuata quotidianamente.

4.6 Key Compromise e Disaster Recovery

Per "key compromise" s'intende la violazione di una o più condizioni vincolanti per l'erogazione del servizio di Certification Authority ed i servizi da esso dipendenti.

Per "disastro" s'intende un evento dannoso le cui conseguenze determinano l'indisponibilità del servizio in condizioni ordinarie.

A seguito di situazioni di compromissione della chiave privata della CA è prevista apposita procedura finalizzata al ripristino (recovery) dei servizi di certificazione, procedura che è indirizzata all'interno del Piano di Continuità Operativa (il Business Continuity Plan) di TI.TT.

Il ripristino da compromissione o disastro avviene in ogni caso nelle seguenti situazioni:

- guasti di una o più delle apparecchiature usate per erogare i servizi di certificazione;
- compromissione (es. rivelazione a terzi non autorizzati, perdita, ecc.) di una o più chiavi private di certificazione.

La procedura di ripristino a seguito di disastro prevede una distinzione dei Servizi in funzione del valore di RTO (Recovery Time Objective) da rispettare e dello SLA previsto. La distinzione è puramente basata sulla necessità di attivare per primi, e nel minor tempo possibile, i servizi "essenziali" che la normativa considera continuativi (ad esempio la Pubblicazione CRL) rispetto agli altri.

5 Misure di sicurezza tecnica

L'infrastruttura tecnologica, le procedure operative, le misure di sicurezza fisica e logica ed il personale preposto all'erogazione del servizio descritto in questo CPS sono gli stessi utilizzati nell'ambito del servizio TI.TT di emissione e gestione dei certificati qualificati di firma digitale come disciplinati dal [CAD].

5.1 Generazione e protezione delle chiavi

5.1.1 Chiavi della CA di TSA

La coppia di chiavi di certificazione usata dalla TSA per firmare i certificati dei TSU e le CRL è generata all'interno di un dispositivo crittografico che è almeno certificato [FIPS 140-2] Level 3 o superiore, in un ambiente fisicamente sicuro.

È previsto il ripristino della chiave (key recovery) di certificazione in caso di cancellazione involontaria o guasto o sostituzione del dispositivo HSM.

Al fine di consentire il key recovery, la CA mantiene una copia di backup della chiave di CA secondo le modalità previste dalla certificazione di sicurezza del dispositivo.

5.1.2 Chiavi dei TSU

La coppia di chiavi di marcatura temporale usata dai TSU per firmare le marche temporali sono generate all'interno dispositivi crittografici che sono conformi ai requisiti di sicurezza specifcati in [ETSI-319421], in un ambiente fisicamente sicuro.

Le chiavi dei TSU ed i corrispondenti certificati vengono sostituiti ogni sei mesi.

Per le chiavi di marcatura temporale non è previsto il key recovery.

5.2 Caratteristiche delle chiavi

5.2.1 Chiavi della CA di TSA

Per firmare i certificati dei clienti e le CRL la TSA TI.TT utilizza chiavi di certificazione con un modulo lungo 4096 bit, generate utilizzando l'algoritmo RSA.

5.2.2 Chiavi dei TSU

Le chiavi dei TSU hanno lunghezza di (almeno) 2048 bit e sono generate utilizzando l'algoritmo RSA.

5.3 Requisiti di sicurezza degli elaboratori

I sistemi operativi usati dalla CA per la gestione dei certificati e delle marche temporali sono dotati di livello di sicurezza adeguato e seguono le procedure di hardening definite a livello di Gruppo TIM.

I sistemi operativi sono configurati in modo tale da richiedere sempre l'identificazione dell'utente mediante username e password oppure, nel caso dei sistemi più critici, mediante smartcard e relativo PIN.

Gli eventi di accesso ai sistemi sono loggati, come descritto nella sezione 4.4.

5.4 Sicurezza di rete

L'accesso agli host on-line della TSA è protetto da firewall di alta qualità che garantiscono un adeguato filtraggio delle connessioni. Prima dei firewall, una batteria di router che implementano opportune ACL (Access Control List) costituisce un'ulteriore barriera di protezione.

Sui server del servizio di certificazione, tutte le porte di comunicazione non necessarie sono disattivate. Sono attivi esclusivamente quegli agenti che supportano i protocolli e le funzioni necessarie per il funzionamento del servizio.

Per irrobustire il filtraggio delle comunicazioni tutto il sistema di certificazione è suddiviso in un'area esterna, una interna ed una DMZ.

TI.TT svolge con cadenza almeno annuale un assessment di sicurezza per verificare l'eventuale presenza di vulnerabilità di rete (Vulnerability Assessment), avvalendosi di specialisti indipendenti (Security Operation Center di TIM).

5.5 Riferimento temporale

La sincronizzazione temporale dei sistemi di TI.TT rispetto alla scala di Tempo Universale Coordinato (UTC), è garantita dall'utilizzo di due orologi di qualità con NTP server incorporato che mantengono allineati i server della piattaforma.

In particolare vengono utilizzati sistemi[1] che permettono:

- la rilevazione satellitare GPS (Global Position System)
- la rilevazione del segnale DCF77, il trasmettitore di frequenza campione e di segnale orario situato in Germania, a Mainflingen.

Personale espressamente autorizzato da TI.TT, provvede a monitorare e garantire i buon funzionamento del sistema di sincronizzazione temporale.

Ulteriori meccanismi di controllo consentono il monitoraggio continuo delle fonti di riferimento temporale, verificando lo stato dei server della piattaforma della TSA. Mediante tali dispositivi di monitoraggio, infatti, è possibile richiedere, tramite protocollo SMNP, il riferimento temporale all'elemento di rete monitorato (server), confrontando i dati ricevuti con una terza parte esterna, lo IEN "Galileo Ferraris".

La rilevazione di qualsiasi anomalia che possa modificare la sincronizzazione dei sistemi, in modo da renderla incompatibile con i requisiti previsti dalla norma, viene registrata e successivamente risolta dal personale autorizzato da TI.TT.

5.6 Comunicazione degli incidenti

Al verificarsi di eventi di gravità tale da compromettere il funzionamento del servizio o nel caso di perdita di calibrazione degli orologi dei TSU, TI.TT rende disponibili ai clienti ed agli utilizzatori del servizio le informazioni che possono essere utilizzate per individuare eventuali marche temporali emesse in modo non conforme alla normativa.

In particolare vengono resi noti, attraverso apposita informativa sul sito web di TI.TT, gli identificativi dei TSU interessati e l'intervallo temporale nel quale si è verificato l'evento.

In caso di violazioni della sicurezza o perdite di integrità che abbiano impatto significativo sui servizi fiduciari o sui dati personali ivi custoditi, TI.TT ne dà comunicazione ai soggetti seguenti:

- AgID in qualità di organismo di vigilanza
- La Divisione III - Sicurezza delle informazioni, internet e qualità dei servizi ICT del Ministero dello Sviluppo Economico, in qualità di ente nazionale competente per la sicurezza delle informazioni;
- L'Autorità Garante per la protezione dei dai personali;
- Eventuali altri organismi interessati, in ragione dell'incidente occorso e delle sue ripercussioni.

TI.TT comunica la violazione tempestivamente e comunque entro le 24 ore dal momento in cui ne viene a conoscenza.

5.7 SLA, indicatori e misure di qualità

In questo paragrafo sono definiti gli indicatori atti a descrivere i livelli di qualità della fornitura.

[1] Time Server Meinberg©:

- "*LANTIME M300/PZF: DCF Time Server with integrated DCF77 radio clock*";
- "*LANTIME M300/GPS : NTP Time Server with integrated GPS radio clock*".

Gli SLA (Service Level Agreement) riportati nel seguito sono validi per il servizio erogato da TITT con piattaforma allocata e gestita presso il centro servizi di Pomezia.

Gli SLA vengono calcolati sulla base delle segnalazioni degli utenti tracciate su trouble ticket aperti dai tecnici dell'Help Desk. In particolare, ogni segnalazione di guasto che perviene al numero verde gestito dall'Help Desk dà luogo all'apertura di un ticket la cui registrazione consente di effettuare un monitoraggio periodico per la verifica del rispetto degli SLA.

Servizio	SLA
Disponibilità dei SERVIZI	99,5% su base 4 mesi
Disponibilità Certificate Revocation List (CRL)	99,8% su base 4 mesi
Supporto di Help Desk telefonico	H24 7x7

6 Profilo delle Marche temporali

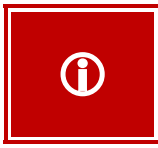
Le marche temporali prodotte sono conformi al profilo IETF RFC 3161 [RFC 3161] ed alle ulteriori specifiche richieste dallo standard ETSI EN 319 422 [ETSI EN 319 422].

In particolare sono valorizzati i seguenti attributi:

- numero di serie
- date e ora di generazione
- accuracy (valorizzata ad un secondo)
- impronta (hash) del documento marcato calcolata con l'algoritmo SHA256
- identificativo dell'algoritmo di hash utilizzato per il calcolo dell'impronta
- identificativo del certificato del TSU che ha prodotto la marca (attributo *signerInfo* all'interno dell'attributo *SigningCertificateV2*)

7 Condizioni di utilizzo dei SERVIZI

Le condizioni contrattuali che regolano i **SERVIZI** sono pubblicate sul già richiamato sito di TI.TT. Esse si compongono di una parte generale, valevole per tutti i servizi erogati da TI.TT e di una sezione specifica che regola i soli **SERVIZI** di validazione elettronica temporale (vedere il paragrafo 2.2).



I documenti pubblicati sul sito sono gli unici che valgono come riferimento.

Le condizioni contrattuali sono accettate dall'utente/cliente prima dell'attivazione dei **SERVIZI** cui fanno riferimento.

Di seguito la sintesi del contenuto delle condizioni per l'utilizzo dei **SERVIZI**.

7.1 Soggetti e modello operativo

Tranne casi eccezionali e offerte proposte in acquisto nel proprio market place on line, TI.TT non vende direttamente i propri **SERVIZI**, che sono invece proposti al mercato tramite le funzioni di vendita delle aziende appartenenti al Gruppo TIM. Pertanto, nelle schema generale del modello operativo di TI.TT, si distinguono i soggetti seguenti:

- Venditore, ovvero la legal entity del Gruppo TIM che stipula il contratto di vendita dei **SERVIZI** nei confronti del cliente finale e degli utilizzatori;
- TI.TT, che eroga i **SERVIZI**;
- cliente finale che acquisisce tramite il venditore i **SERVIZI** erogati da TI.TT
- utilizzatore che utilizza materialmente i **SERVIZI** erogati da TI.TT;
- soggetto che fa affidamento sui **SERVIZI** e sulle informazioni in essi contenute.

7.2 Prezzo dei SERVIZI

In caso di servizi offerti in vendita on line direttamente da TI.TT, i prezzi sono quelli esposti nel market place ed associati alle offerte.

Per quanto concerne le proposte commerciali gestite dal Gruppo TIM, le informazioni sui prezzi di acquisto possono essere richieste direttamente ai soggetti proponenti.

Condizioni diverse possono comunque essere negoziate caso per caso, in base ai volumi richiesti.

7.3 Copertura assicurativa

TI.TT ha stipulato un'apposita assicurazione a copertura dei rischi derivanti da tutte le sue attività, che prevede le seguenti coperture:

TIPO DI RISARCIMENTO	MASSIMALE ANNUO	MASSIMALE PER SINGOLO SINISTRO E SINISTRI IN SERIE
Risarcimento di danni patrimoniali cagionati a Terzi in conseguenza di fatto accidentale verificatosi in relazione allo svolgimento della propria attività, oppure per: • fatto colposo e/o doloso dei dipendenti addetti all'attività per la quale è prestata l'assicurazione e dei quali TI.TT debba rispondere ai sensi di legge; • atti dolosi di Terzi, commessi tramite intromissione nei sistemi informatici di TI.TT superando le misure di sicurezza logica e fisica predisposte; • Inadempimenti o ritardi a seguito di danno materiale e diretto alle apparecchiature utilizzate per lo svolgimento dell'attività per la quale è prestata l'assicurazione.	€ 5.000.000,00 (cinque milioni)	€ 5.000.000,00 (cinque milioni)

7.4 Tutela della riservatezza e trattamento dei dati personali

TI.TT è titolare del trattamento dei dati personali da essa raccolti ai fini della vendita e dell'erogazione dei propri servizi. I trattamenti avvengono in conformità a quanto disciplinato dal [Normativa Privacy] e in caso di attività demandate a soggetti terzi, TI.TT provvede alle necessarie nomine e a fornire adeguate istruzioni operative.

Gli archivi contenenti dati personali sono:

- il database di registrazione
- l'archivio della documentazione cartacea

Tali archivi sono gestiti da personale dotato di idonee esperienza e competenza e sono adeguatamente protetti da tentativi di accesso non autorizzato.

TI.TT, in particolare, attua misure di sicurezza rispondenti almeno ai requisiti del Capo II ("Misure minime di sicurezza") del [Normativa Privacy] ed in particolare:

- mantiene un aggiornato "Piano della Sicurezza" (PdS)
- adotta un opportuno sistema di controllo degli accessi agli archivi
- adotta opportune procedure di gestione delle credenziali di autenticazione
- mantiene un registro permanente (audit log) degli accessi agli archivi
- effettua periodicamente copie di sicurezza dei dati, al fine di garantirne il ripristino

Limitatamente al servizio erogato sulla base di questo CPS, TI.TT non raccoglie e non tratta "dati sensibili" né "dati giudiziari" ai sensi dell'articolo 4 del [Normativa Privacy].

7.5 Diritti di proprietà intellettuale

I documenti relativi ai servizi pubblicati da TI.TT sono di sua proprietà ed essa si riserva tutti i diritti loro relativi.

Il Cliente e l'Utilizzatore dei servizi mantengono gli eventuali diritti di cui sono titolari rispetto ai loro marchi commerciali (brand name) e ai propri nomi di dominio.

Relativamente alla proprietà di altri dati ed informazioni si applicano le specifiche leggi vigenti.

7.6 Obblighi e garanzie

7.6.1 Obblighi di TI.TT

TI.TT si impegna a:

- operare in conformità a quanto indicato nel CPS e nei documenti descrittivi dei **SERVIZI**;
- emettere e gestire i certificati eventualmente necessari per l'utilizzo dei **SERVIZI** come descritto nel presente CPS ed a garantire per essi un efficiente servizio di sospensione o revoca dei certificati;
- fornire informazioni chiare e complete sulle procedure e requisiti dei **SERVIZI**;
- rendere sempre disponibile questo CPS tramite il proprio sito web;
- garantire un trattamento dei dati personali conforme alle norme vigenti;
- fornire un servizio informativo efficiente ed affidabile sullo stato dei **SERVIZI**.

7.6.2 Obblighi del cliente e dell'utilizzatore

Il cliente e l'utilizzatore si impegnano:

- leggere, comprendere ed accettare integralmente tutta la documentazione attinente ai **SERVIZI** che TI.TT rende disponibile su proprio sito;
- utilizzare e far utilizzare nel proprio ambito i servizi conformemente a quanto indicato da TI.TT nella documentazione descrittiva dei **SERVIZI**;
- evitare ogni comportamento che determina un utilizzo improprio dei **SERVIZI** ed informare TI.TT di qualunque evento possa compromettere l'accesso o il loro utilizzo;
- informare immediatamente TI.TT in caso risulti compromessa la riservatezza dei codici di accesso per l'utilizzo dei **SERVIZI**.

7.7 Esclusione di garanzie

TI.TT non ha ulteriori obblighi e non garantisce nulla più di quanto espressamente indicato nel CPS e nelle condizioni di utilizzo dei **SERVIZI** (v. par. 7.6.1) o previsto dalle norme vigenti.

7.8 Limitazioni di responsabilità - Esclusioni

TI.TT dichiara in modo esplicito nelle condizioni generali e specifiche di utilizzo dei **SERVIZI** i casi in cui non assume responsabilità:

- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti se non nei casi di proprio dolo o colpa;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti per eventi derivanti da atti della Pubblica Autorità, caso fortuito, forza maggiore ovvero da altra causa non imputabile ad TI.TT, esclusi i casi di dolo o colpa;
- danni di qualsiasi natura, diretti e/o indiretti, o pregiudizi da chiunque patiti causati da comportamenti dell'utilizzatore o del cliente non conformi a quanto indicato da TI.TT nella documentazione descrittiva dei **SERVIZI** oppure alle norma vigenti, oppure da eventi fuori del controllo di TI.TT che influiscono sull'erogazione dei **SERVIZI**.

7.9 Risarcimenti

TI.TT non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelle scaturenti dalla fornitura dei **SERVIZI** e dalla normativa vigente che li regola.

Fermo restando quanto precede e ad eccezione dei casi previsti dalla legge applicabile, TI.TT risponderà dei soli danni diretti fino a concorrenza dei massimali della copertura assicurativa, indicati nel par. 7.3.

7.10 Reclami e contatti

I reclami relativi ai **SERVIZI**, corredati da un numero di telefono cellulare per pronto riferimento, devono essere indirizzati a TI.TT attraverso i canali di contatto seguenti:

Canale di contatto	Riferimento da contattare
FAX	0691253559
Posta ordinaria	TI Trust Technologies S.r.l. S.R. 148 Pontina km. 29,100 00071 Pomezia (RM)
Posta elettronica	CRPresidio_CA@telecomitalia.it
Posta elettronica certificata	reclami@ttpec.telecomitalia.it

Qualora TI.TT non fornisca riscontro entro 30 giorni solari dalla ricezione del reclamo, sarà comunque possibile ricorrere davanti al foro competente.

7.11 Clausole particolari e foro competente

Per controversie attinenti alla validità, efficacia, interpretazione, esecuzione e/o estinzione delle condizioni di utilizzo dei **SERVIZI**, è competente in via esclusiva il Foro di Roma.

8 Cessazione dei SERVIZI

In ogni caso in cui se ne dovesse presentare la necessità, si procede alla cessazione dei **SERVIZI** secondo quanto di seguito descritto

1. TI.TT comunica con un **anticipo di almeno 90 giorni** la propria determinazione a cessare i **SERVIZI** di ad AGID, ai clienti ed agli utilizzatori.
2. Ove TI.TT abbia individuato soggetti sostitutivi, nella sua comunicazione indicherà il prestatore di servizi fiduciari qualificato sostitutivo, il depositario delle validazioni temporali emesse, della relativa documentazione ed il periodo in cui tale soggetto manterrà evidenza delle operazioni [2], [3].
3. Ove TI.TT non indichi un prestatore di servizi fiduciari qualificato sostitutivo, procederà alla revoca di tutti i certificati attivi al momento della cessazione della propria attività, e provvederà a riversare nel proprio sistema di Conservazione a norma le validazioni temporali emesse, la documentazione e l'evidenza delle operazioni, dove provvederà a mantenerle disponibili (v. par. 4.5) a far data dalle cessazione, generando una CRL finale raggiungibile all'URL originale e mantenuta disponibile per i tempi disposti dalla normativa vigente.
4. In caso di cessazione dei **SERVIZI**, TI.TT assicura la definizione dei rapporti pendenti con altri eventuali soggetti coinvolti nell'ambito dei servizi.
5. TI.TT distrugge in modo da renderle irrecuperabili le chiavi private dei TSU e revoca i corrispondenti certificati.
6. TI.TT procede alla dismissione delle infrastrutture HW e SW dei servizi, conformemente alle proprie policy.

==== FINE DEL DOCUMENTO ====

[2] Il trasferimento si configurerà come cessione di contratto da parte di TI.TT verso l'operatore sostitutivo per assicurare la continuità dei **SERVIZI** verso clienti ed utilizzatori.

[3] In caso di eventuale avvio di procedure concursuali a carico di TI.TT ed in considerazione della loro lunga durata, nel caso in cui si verificassero circostanze tali da impedire a TI.TT di garantire tutti gli adempimenti connessi ai **SERVIZI**, TI.TT procederà alla loro cessazione con trasferimento dei contratti ad un operatore sostitutivo.