TeamSystem®

Manuale Operativo

Certification Practice Statement /
Certificate Policy

INDICE

INFORMAZIONI GENERALI

1.1.1. Controllo documentale

Livello di sicurezza:	Pubblico
Ente di Emissione:	TeamSystem S.p.A.
Versione:	1.3
Data ultima edizione:	31/07/2026
Codice Documento:	TS_Manuale_Operativo_QTSP_v.1.3_IT

1.1.2. Controllo formale

Versione:	Redatto da:	Revisionato da:	Approvato da:
1,0	Legal & Compliance (Uanataca)	PM servizio	Responsabile del servizio di certificazione e validazione temporale
1.1	Tutti i ruoli fiduciari	Compliance	Responsabile del servizio di certificazione e validazione temporale
1.2	Compliance	Responsabile della conduzione tecnica dei sistemi	Responsabile del servizio di certificazione e validazione temporale
1.3	Compliance	Responsabile della sicurezza	Responsabile del servizio di certificazione e validazione temporale

1.1.3. Controllo delle versioni

Versione	Parti modificate	Descrizione delle modifiche	Data
1.0	Originale	Prima versione del documento	23/03/2023

1.1	Intero documento	a) Uniformata descrizione dei ruoli b) Aggiunti riferimenti normativi	05/11/2025
1.2	Cap. 2.5, 4.2 e 5.5	Aggiornamento in ossequio alle novità normative del Regolamento eIDAS	20/05/2026
1.3	Cap. 2.6, 4.2, 5.3, 5.5 e 7.1	- Introduzione della videoidentificazione da remoto (attended) tra le modalità di identificazione e dell'emissione del certificato qualificato di sottoscrizione di persona fisica su dispositivo fisico (smart card o token); - precisazione della non applicabilità del limite d'uso relativo al dominio applicativo TeamSystem ai certificati su dispositivo fisico; - introduzione dell'identificazione mediante Carta d'Identità Elettronica (CIE livello 3). - Introdotte chiavi crittograffiche compliant con Guidelines ENISA	31/07/2026

2. INTRODUZIONE

2.1.1. Scopo

Il presente documento pubblico, "*Manuale Operativo*" o anche "*Certification Practice Statement*" (CPS), descrive le procedure operative seguite da TeamSystem nell'erogazione dei seguenti Servizi Fiduciari:

- emissione di certificati di firma elettronica qualificata a persone fisiche;
- emissione di certificati di sigilli elettronici qualificati a persone giuridiche;
- emissione certificati di validazione temporale qualificata;

TeamSystem S.p.A. (di seguito anche solo "TeamSystem") è una società per azioni costituita in Italia.

2.2. Definizioni e acronimi

Le seguenti definizioni e acronimi sono in linea con quanto indicato all'interno dei seguenti riferimenti:

a. **Codice dell'Amministrazione Digitale** di cui al D.Lgs. 7 marzo 2005 n. 82 e s.m.i.;
b. **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 (di seguito anche solo "*Regolamento eIDAS*");
c. **DPCM 22 febbraio 2013** recante Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 (di seguito anche solo "*Regole Tecniche*").

Per i termini definiti dalle suddette disposizioni, si rimanda alle definizioni in esse stabilite.

Qualora, all'interno del documento, venga riscontrata la presenza di termini o acronimi non ricompresi nelle seguenti definizioni, dovrà attribuirsi alle stesse il significato proprio secondo la normativa applicabile

AgID (o anche "Agenzia")

Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Prestatori di Servizi Fiduciari Qualificati

Analisi dei rischi

Processo di comprensione della natura del rischio e di determinazione del livello di rischio.

Autorizzazione

Disposizione di garanzia sull'identità dell'entità (ISO/IEC 18014-2)

CAB

Conformity Assessment Body (o Organismo di valutazione della Conformità) è un organismo accreditato, secondo quanto previsto dal Regolamento eIDAS, competente ad 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.

Certificato qualificato

Quando non indicato diversamente, si intende indistintamente Certificato qualificato di firma elettronica e di Sigillo elettronico.

Certificato di firma elettronica

Un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona.

Certificato qualificato di firma elettronica

Un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I di cui al Regolamento eIDAS;

Certificatore

È il Prestatore di Servizi Fiduciari Qualificati (o *Certification Authority* – CA, o Qualified Trust Service Provider - QTSP), iscritto nell'elenco pubblico dei certificatori accreditati tenuto dall'AgID ai sensi dell'art. 29 co. 6 del CAD identificabile, ai sensi del presente Manuale Operativo, nella società TeamSystem S.p.A.; è un soggetto che rilascia al pubblico certificati qualificati, firmandoli con la propria chiave provata, detta chiave di CA o chiave di root, e che provvede anche alla pubblicazione e revoca dei certificati stessi.

CIE

Carta d'Identità Elettronica

Cliente

Persona física o giuridica che sostiene i costi di emissione di un Certificato in favore di un Richiedente.

CNS

Carta Nazionale dei Servizi.

Confidenzialità

Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati.

Criteri di rischio

Valori di riferimento rispetto ai quali è ponderato il rischio.

CRL

Certificate Revocation List, è un elenco dei certificati digitali che sono stati revocati dal Certificatore prima della data di scadenza pianificata e, dunque, da non considerare più come attendibili.

D. Lgs

Decreto Legislativo.

Dato personale

Si intende "qualunque informazione relativa a persona fisica identificata o identificabile" (art. 4 n. 1 del Regolamento UE n. 679/2016).

Dati particolari

Sono quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 9 del Regolamento UE n. 679/2016).

Dati giudiziari

Sono i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza di cui all'art. 10 del Regolamento UE n. 679/2016.

Disponibilità

Accertarsi che gli utenti autorizzati abbiano accesso all'informazione e alle attività associate quando richiesto.

Definizione del rischio

Processo di individuazione, riconoscimento e descrizione del rischio.

Entità

Può essere una persona fisica o un soggetto giuridico.

ETSI

Istituto Europeo per le Norme di Telecomunicazioni (in inglese *European Telecommunications Standards Institute*). È un organismo di standardizzazione europeo riconosciuto dalla Commissione Europea per lo sviluppo di norme armonizzate.

Evidenza informatica

Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

Gestione del rischio

Attività coordinate per dirigere e controllare una organizzazione in merito al rischio o ai rischi esistenti.

Hardware Security Module [HSM]

È un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.

Identificazione informatica

L'identificazione di cui all'art. 1 co. 1 lett. u-ter) del Decreti legislativo 7 marzo 2005 n. 82 (CAD).

IETF - Internet Engineering Task Force

Una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

Integrità

Salvaguardia dell'esattezza e della completezza dei dati e delle modalità di processo.

Intermediario Finanziario

Entità soggetta alla vigilanza di Banca d'Italia che ha l'obbligo di identificare i propri clienti ai sensi della normativa antiriciclaggio in ossequio a quanto previsto dal D.Lgs 231/2007 e ss.mm..

Intestatario della fattura

Persona fisica o giuridica cui è emessa la fattura relativa al servizio di emissione dei certificati qualificati disciplinati dal presente Manuale Operativo attribuiti al Titolare. Può coincidere con l'Utente Titolare e/o con il Richiedente.

ISO - International Organization for Standardization

Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union

Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

Manuale Operativo o Certification Practice Statement (CPS)

Il Manuale Operativo, ai sensi dell'art. 40 co. 1 delle Regole Tecniche, definisce le procedure applicate dal Certificatore che rilascia certificati qualificati nello svolgimento della sua attività. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Autorità di vigilanza e quelle della letteratura internazionale.

OCSP

On-line Certificate Status Protocol è un protocollo che permette di verificare la validità di un certificato senza ricorrere alle liste di revoca dei certificati.

One-Time Password - OTP

Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. Può essere basata su dispositivi hardware o su procedure software.

OTP

Vedi One-Time Password.

Parte interessata

Persona o organizzazione che può influenzare o essere influenzata da una decisione o un'attività.

Persona Fisica

Soggetto dotato di capacità giuridica.

Persona Giuridica

Organismo unitario, caratterizzato da una pluralità di individui o da un complesso di beni, al quale viene riconosciuta dal diritto capacità di agire in vista di scopi leciti e determinati.

PKI

Public Key Infrastructure o anche Infrastruttura a Chiave Pubblica, utilizzata dal Certificatore per la fornitura dei servizi fiduciari qualificati.

PIN - Personal Identification Number

Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso.

Ponderazione del rischio

Processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.

Pubblico ufficiale

Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

QSCD

Si intende "*Qualified Signature/Seal Creation Device*" o dispositivi sicuro per la generazione della firma o del sigillo qualificato.

Registrazione

L'insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione è rilasciato un certificato digitale a un utente, previa identificazione certa di quest'ultimo.

Richiedente [Subscriber]

Persona fisica o giuridica, in persona del legale rappresentante della stessa, che richiede l'emissione di un certificato qualificato. Può coincidere con l'Utente Titolare e con l'Intestatario della Fattura.

Riservatezza

Garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate.

SAML

Security Assertion Markup Language.

Sicurezza delle informazioni

Conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni; inoltre, possono essere coinvolte altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità.

Sigillo elettronico

Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi.

Sigillo elettronico qualificato

Un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici.

Sistema

Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione.

Tempo Universale Coordinato [UTC]

Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5.

Titolare o Utente Titolare

È il soggetto (persona fisica o giuridica) a cui è rilasciato un certificato digitale. È il soggetto che deve essere identificato dal Certificatore, può coincidere con il Richiedente e/o con l'Intestatario della Fattura.

Trattamento del rischio

Processi di selezione e implementazione di attività volte a diminuire o comunque modificare il rischio presente.

TSL

Trust-service Status List: si intende la lista dei Certificatori accreditati ai sensi del Regolamento eIDAS, disponibile on-line nella piattaforma della Commissione Europea.

Valutazione del rischio

Processo complessivo di identificazione, analisi e ponderazione del rischio.

2.3. Normativa applicabile

I certificati emessi in conformità al presente Manuale sono i seguenti:

- **Certificato qualificato di sottoscrizione:**
  - Certificato qualificato di sottoscrizione in QSCD;
- **Certificato qualificato di sigillo elettronico:**
  - Certificato qualificato di sigillo elettronico in QSCD;
- **Certificato di Time Stamping Unit:**
  - Certificato di Time Stamping Unit per l'emissione di marche temporali qualificate;

I Servizi Fiduciari qualificati erogati da TeamSystem soddisfano i requisiti del Regolamento EU N°910/2014 (eIDAS) e sono conformi agli standard:

- **ETSI EN 319 401**: *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*.
- **ETSI EN 319 411**: *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates*.
- **ETSI EN 319 412 (1,2,3,4 e 5)**: *Electronic Signatures and Infrastructures (ESI); Certificate Profiles*.
- **ETSI EN 319 421**: *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*.
- ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI TS 119 461: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Components providing Identity Proofing of Trust Service Subjects.

Inoltre, TeamSystem si conforma alle Linee Guida in materia di "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche

qualificate" di cui alla Determina n. 147 del 4 giugno 2019 emessa dall'Agenzia per l'Italia Digitale (AgID) che ha confermato il contenuto della sua precedente Determinazione n. 121/2019.

Con riferimento al trattamento dei dati personali, TeamSystem si conforma 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 e che abroga la direttiva 95/46/CE (di seguito anche solo "GDPR").

Il contenuto del presente Manuale segue le indicazioni fornite dall'RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*".

2.4. OID (Object Identifier)

Di seguito sono elencati gli OID ("*Object Identifier*") delle policy supportate da questo Manuale Operativo. Le Policy OID contraddistinguono ciascun profilo di certificato emesso da TeamSystem e sono specificate all'interno di ciascun certificato.

L'*Object Identifier* (OID) che identifica la CA TeamSystem è il seguente:

OID	Tipo di certificato
	Servizio di firma e sigillo
1.3.6.1.4.1.59699.1	Certificato qualificato di sottoscrizione su dispositivo QSCD
1.3.6.1.4.1.59699.2	Certificato qualificato di sottoscrizione su dispositivo remoto QSCD
1.3.6.1.4.1.59699.3	Certificato qualificato di sottoscrizione di tipo "*One-Shot*" su dispositivo remoto QSCD
1.3.6.1.4.1.59699.4	Certificato qualificato di sigillo elettronico su dispositivo QSCD
1.3.6.1.4.1.59699.5	Certificato qualificato di sigillo elettronico su dispositivo remoto QSCD
1.3.6.1.4.1.59699.6	Certificato qualificato di sottoscrizione automatica su dispositivo QSCD
1.3.6.1.4.1.59699.7	Certificato qualificato di sottoscrizione automatica su dispositivo remoto QSCD
	Servizio di Marca Temporale

1.3.6.1.4.1.59699.8	Certificato di Time Stamping Unit

OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. La presenza dei limiti d'uso non modifica in alcun modo le regole stabilite nel resto del Manuale Operativo.

Inoltre, tutti i certificati che rispettano le raccomandazioni della Determinazione AgID n. 121/2019 con le rettifiche della successiva Determinazione AgID n. 147/2019, dal 5 luglio 2019, conterranno un ulteriore elemento PolicyIdentifier con valore agIDcert (OID 1.3.76.16.6) nel campo CertificatePolicies (OID 2.5.29.32).
Nel caso di eventuali discrepanze tra il presente Manuale Operativo e l'ulteriore documentazione, contenente le condizioni di fornitura e/o le procedure relative ai servizi offerti da TeamSystem, prevarrà quanto stabilito nel presente Manuale Operativo.
TeamSystem si riserva di apportare modifiche al presente Manuale Operativo per esigenze tecniche o modifiche procedurali intervenute durante la gestione del servizio.
Al verificarsi di ogni variazione TeamSystem notificherà ad AgID la versione aggiornata del Manuale Operativo che sarà pubblicata sul relativo sito web istituzionale.
Questo documento è anche pubblicato sul sito web di TeamSystem al seguente indirizzo: https://www.teamsystem.com/trust-services/documentazione.

2.5. Partecipanti ai servizi di certificazione

2.5.1.1. Prestatore Qualificato di Servizi Fiduciari (Qualified Trust Service Provider - QTSP)

TeamSystem opera in qualità di Qualified Trust Service Provider (QTSP). I dati identificativi dell'Organizzazione sono i seguenti:

Ragione Sociale:	TeamSystem S.p.A.
Partita IVA:	01035310414
Sede legale	Via Sandro Pertini 88 (61122) – Pesaro (PU)
Tel:	0721 426601
E-mail:	info@teamsystem.com

TeamSystem eroga i seguenti servizi fiduciari:

a. rilascio e gestione dei certificati qualificati (firma elettronica qualificata e sigillo elettronico qualificato), in conformità alle disposizioni di cui al Regolamento eIDAS (UE) n. 910/2014 (di seguito anche solo

"*Regolamento eIDAS*"), alla normativa tecnica "ETSI" applicabile al rilascio e alla gestione dei certificati qualificati, con particolare riferimento allo standard "EN 319 411- 1" e "EN 319 411-2" nonché alla normativa Nazionale di riferimento (D.Lgs. 7 marzo 2005 n. 82 e s.m.i. – di seguito anche solo "Codice dell'Amministrazione Digitale" o "CAD").

b. rilascio di marche temporali qualificate, in conformità alle disposizioni di cui al Regolamento (UE) n. 910/2014 (più brevemente citato come "Regolamento eIDAS") e alla normativa tecnica "ETSI" applicabile al rilascio e alla gestione dei certificati qualificati, con particolare riferimento allo standard "EN 319 421".

In particolare, con riferimento ai certificati qualificati di firma elettronica qualificata di cui alla precedente lett. a) TeamSystem può emettere anche tale tipologia di certificati in modalità "*One-Shot*" con durata e finalità limitate a specifici ambiti di applicazione e di utilizzo (v. Par. 2.6.1.3.).

Per la fornitura di servizi fiduciari qualificati, TeamSystem si avvale delle chiavi di certificazione di cui ai paragrafi seguenti, le quali soddisfano i requisiti di cui al Regolamento eIDAS e si conformano *in toto* alle Raccomandazioni di cui alla Determinazione n. 147/2019 emessa da AgID.

La fornitura dei servizi fiduciari qualificati di TeamSystem avviene avvalendosi dell'infrastruttura e dei servizi della società Uanataca S.A. unipersonale; inoltre la stessa società fornisce ed eroga il servizio fiduciario qualificato di la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza, di cui all'art. 3 punto 16 del Regolamento eIDAS.

Di seguito i riferimenti societari del Fornitore:

Ragione Sociale:	Uanataca S.A. unipersonale
Partita IVA:	09156101215
Sede legale (ES)	Avenida Meridiana, 350 – Planta 3, 08027 (Barcellona) - Spagna
Sede secondaria (IT)	Via Diocleziano n. 107 – 80125 (Napoli) - NA
Tel:	081 / 7625600
E-mail:	info.it@uanataca.com

2.5.1.2. TeamSystem CA

Si tratta della CA che rilascia i seguenti profili di certificati:

- Certificato qualificato di sottoscrizione in QSCD;
- Certificato qualificato di sigillo elettronico in QSCD;

Il certificato di CA è autofirmato (*self-signed*).

Dati identificativi:

CN:	2.5.4.97 = VATIT-01035310414 CN = TeamSystem Qualified Electronic Signature CA 2023 OU = Qualified Trust Service Provider O = TeamSystem S.p.A. C = IT
Fingerprint (SHA1):	4280ddfe5bb9e7b06145fb633b1fe50170ea2a7f
Valido dal:	16 maggio 2023 10:26:10
Scadenza:	16 maggio 2043 10:26:10
Lunghezza Chiave RSA	4096

2.5.1.3. TeamSystem TSA

Si tratta della CA che rilascia i certificati per l'emissione di marche temporali e il cui certificato è autofirmato (*self-signed*).

Dati identificativi:

CN:	C = IT O = TeamSystem S.p.A. OU = Qualified Time Stamping Authority CN = TeamSystem Qualified Time Stamping Authority 2023 2.5.4.97 = VATIT-01035310414
Fingerprint (SHA1):	5195145deff84aac254eb21b87574bbf203da0bb
Valido dal:	16 maggio 2023 10:38:26
Scadenza:	16 maggio 2043 10:38:26
Lunghezza Chiave RSA	4096

2.5.1.4. Utenti finali

Gli utenti finali (di seguito anche solo "Utenti" o "Richiedenti") si identificano nelle persone fisiche o giuridiche destinatarie del servizio di emissione, gestione ed utilizzo dei certificati qualificati emessi da TeamSystem.

In particolare, rientrano tra gli utenti finali, ai sensi del presente Manuale, le seguenti categorie:

1) **Richiedenti:** persone fisiche o giuridiche che domandano alla CA il rilascio di un certificato digitale (firma o sigillo elettronico);

2) **Titolari:** persone fisiche o giuridiche titolari del certificato qualificato, coincidono con i Richiedenti a seguito dell'emissione del certificato;
3) **Relying parties:** soggetti che ricevono un documento informatico sottoscritto con il certificato digitale del Titolare e che fanno affidamento sulla validità del certificato medesimo (e/o sulla firma/sigillo digitale ivi presente) per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

2.5.1.5. Richiedenti

Sono le persone fisiche o giuridiche che richiedono il rilascio di certificati digitali, rivolgendosi direttamente alla CA.
Il Richiedente, al momento della richiesta formale di certificato, dichiara di accettare le Condizioni Generali di contratto stabilite dalla CA (le "Condizioni Generali") e, pertanto, acconsente all'esercizio dei diritti e al rispetto degli obblighi dettati da quest'ultima.
Le condizioni contrattuali disposte dalla CA si aggiungono ed integrano i diritti e gli obblighi dei Richiedenti e/o Titolari sanciti nella normativa italiana ed europea che disciplina i servizi fiduciari e l'utilizzo dei certificati qualificati nonché negli standard tecnici, di matrice europea, relativi all'emissione dei certificati qualificati, con particolare riferimento allo standard "ETSI EN 319 411", sezioni 5.4.2 e 6.3.4..
A seguito dell'emissione del certificato, il Richiedente si identifica nel Titolare.

2.5.1.6. Titolare del certificato

Il Titolare del certificato è il soggetto che possiede ed utilizza la chiave privata relativa ad un certificato qualificato di firma o un certificato qualificato di sigillo elettronico corrispondente alla chiave pubblica contenuta nel certificato.
Il Titolare del certificato qualificato corrisponderà alla persona fisica che lo richiede in caso di certificato di firma, mentre corrisponderà alla persona giuridica (identificata attraverso la sua denominazione, il codice fiscale o la partita iva), nel caso di certificati di sigillo elettronico.
Il Titolare è identificato all'interno del certificato attraverso un "*Distinguished Name*" (DN), nel campo *Subject*, conforme allo standard ITU-T X.500.
Nel campo *Subject* sono inseriti i dati identificativi del Titolare del certificato, senza che sia possibile, in genere, l'utilizzo di pseudonimi.
La chiave privata di un Titolare, generata da TeamSystem, non può essere recuperata o ricavata dalla CA una volta consegnata, in quanto i Titolari identificati nei rispettivi certificati sono gli unici responsabili della loro protezione.
Essi, pertanto, sono tenuti a tenere in debita considerazione le conseguenze, indicate all'interno del presente Manuale Operativo, derivanti dallo smarrimento della chiave privata.

2.5.1.7. Relying parties

Le Relying Parties (RP) si identificano nei soggetti che fanno affidamento sulle informazioni contenute nei certificati qualificati emessi da TeamSystem.

In particolare, per quanto riguarda il servizio descritto nel presente Manuale Operativo, per RP si intendono:

- tutti i soggetti che verificano le firme elettroniche e i sigilli elettronici attraverso i certificati qualificati emessi secondo le modalità descritte nel presente Manuale Operativo.

Tutti coloro che devono fare affidamento sulle informazioni contenute nei certificati qualificati hanno l'obbligo, prima di accettare un certificato, di effettuare le necessarie verifiche, secondo quanto disposto nel presente Manuale Operativo, ovvero nelle istruzioni disponibili sulla pagina web di TeamSystem.

2.5.1.8. Agenzia per l'Italia Digitale - AgID

L'Agenzia per l'Italia Digitale (AgID) è l'organismo che, ai sensi dell'articolo 17 del Regolamento eIDAS, svolge attività di vigilanza (*ex ante* ed *ex post*) sui Prestatori di servizi fiduciari qualificati stabiliti nel territorio italiano allo scopo di garantirne la rispondenza ai requisiti stabiliti dal Regolamento.

2.5.1.9. Organismo di valutazione della conformità (CAB)

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

2.6. Utilizzo dei certificati

La presente sezione indica le possibili applicazioni di ciascuna tipologia di certificato emesso da TeamSystem e i limiti caratterizzanti l'utilizzo di alcune tipologie di certificati.

2.6.1.1. Uso previsto dei certificati

I certificati emessi da TeamSystem, secondo le modalità indicate dal presente Manuale Operativo, sono Certificati Qualificati ai sensi del CAD e del Regolamento eIDAS e rispettano le "*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*" di cui al regolamento pubblicato da AgID nella sua ultima versione.

Il certificato emesso dalla CA sarà usato per verificare la firma qualificata o il sigillo elettronico del Titolare cui il certificato appartiene.

Altri usi dei certificati non sono previsti e sono da evitarsi.

In particolare, è vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel presente Manuale Operativo, nella documentazione contrattuale e in violazione dei limiti d'uso e di valore (*key usage*, *extended key usage*, *user notice*) indicati nel certificato stesso.
TeamSystem si riserva la facoltà di revocare i certificati, ove applicabile, qualora venga a conoscenza che questi siano utilizzati in modo improprio o contrario alle disposizioni del presente Manuale.

2.6.1.2. Certificato qualificato di sottoscrizione in QSCD

Questi certificati sono contrassegnati dagli OID di cui al Par. 2.4 del presente Manuale. Si tratta di certificati qualificati emessi per la firma elettronica qualificata emessa su HSM ovvero su dispositivo fisico (smart card o token) e sono conformi alla politica di certificazione QCP-n-qscd con OID 1.3.6.1.4.1.59699.1 e 1.3.6.1.4.1.59699.2, come dichiarato nei certificati.
Tali certificati, emessi in QSCD costituiscono certificati qualificati secondo quanto stabilito nell'art. 28 del Regolamento eIDAS.
Funzionano con dispositivi qualificati di creazione di firma (QSCD), nel rispetto degli articoli 29 e 51 del Regolamento eIDAS, e in accordo a quanto disposto dalla regolamentazione tecnica rilasciata dall'Istituto Europeo per gli Standard nelle Telecomunicazioni, identificata con il riferimento EN 319 411-2.
Inoltre, garantiscono l'identità del Titolare e consentono di generare una "*firma elettronica qualificata*", ossia una firma elettronica avanzata, creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche, la quale è equiparata, per tutti gli effetti di legge, ad una firma autografa senza che sia necessario la sussistenza di ulteriori requisiti.
Il campo "*key usage*" consente di realizzare esclusivamente la funzione di "*Content commitment*" (non ripudio).

2.6.1.3. Certificato qualificato di sottoscrizione "One-Shot"

Si tratta di un certificato qualificato di sottoscrizione emesso su dispositivo HSM (di firma remota) avente un periodo di validità limitato nel tempo, non superiore a 60 minuti. Il suo utilizzo è consentito mediante sistemi di autenticazione consentiti dalla normativa e solo nei modi e nei termini delle limitazioni di uso inserite nel certificato, stabilite da TeamSystem e accettate dal Titolare in fase di richiesta di emissione del certificato.
In maniera congiunta all'apposizione della firma, al documento informatico oggetto di sottoscrizione viene inserita anche una validazione temporale qualificata, per garantire un riferimento temporale certo secondo quanto previsto dalla normativa.
Per questa tipologia di certificato, non è prevista la revoca o la sospensione. È previsto uno specifico limite d'uso, così come indicato al punto 5.5.1.5.

2.6.1.4. Certificato qualificato di sottoscrizione "Automatico"

Questi certificati sono contrassegnati dagli OID di cui al Par. 2.4 del presente documento.
Si tratta di certificati qualificati emessi per la firma elettronica qualificata su HSM (di firma remota).
Tali certificati sono generati tramite una "*particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo*", ai sensi dell'art. 1, co.1., lett. r) del DPCM 22 febbraio 2013, quale disciplina di dettaglio rispetto ai principi generali indicati nell'art. 35, co.2 e 3, del CAD (D.lgs. 7 marzo 2005, n.82).
I predetti certificati consentono la sottoscrizione di documenti informatici, anche in grande quantità (ragion per la quale tali certificati vengono definiti anche come certificati di "firma massiva"), da parte del Titolare senza che vi sia la presentazione effettiva, chiaramente e senza ambiguità, di ciascun documento informatico al Titolare stesso prima dell'apposizione della firma.
Tale procedura, tuttavia, presuppone il previo consenso del Titolare all'utilizzo di tale modalità (ai sensi dell'art. 35, co.3, CAD (D.lgs. 7 marzo 2005, n.82)) e, pertanto, viene avviata sotto il suo esclusivo controllo anche in assenza di un presidio puntuale e continuo, nel rispetto di quanto indicato nell'art. 5, co.2 e 3, del DPCM 22 febbraio 2013.
In particolare, detta ultima disposizione stabilisce che per la procedura di firma "automatica" vi sia l'utilizzo di una coppia di chiavi specificamente dedicata a tale procedura ed il relativo certificato qualificato debba contenere un'indicazione specifica dell'utilizzo della predetta procedura, con specifico richiamo al limite d'uso definito da AgID "Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.".

2.6.1.5. Certificato qualificato di sigillo elettronico in QSCD

Questi certificati sono contrassegnati dal seguente OID 1.3.6.1.4.1.59699.4 per l'emissione su HSM (sigillo remoto).
Tali certificati, emessi in "*Qualified Seal Creation Device*" (di seguito anche solo "*QSealCD*" o anche "QSCD", costituiscono certificati qualificati ai sensi dell'art. 38 del Regolamento eIDAS: "*Certificati Qualificati di Sigilli Elettronici*".
Funzionano con dispositivi qualificati di creazione di firma e sigilli elettronici (QSCD), nel rispetto degli articoli 39 e 51 del Regolamento eIDAS, e in accordo a quanto disposto dalla regolamentazione tecnica rilasciata dall'Istituto Europeo per gli Standard nelle Telecomunicazioni, identificata con il riferimento EN 319 411-2.
Inoltre, garantiscono la piena validità legale e riconducibilità ad una persona giuridica determinata (Titolare) di un documento informatico e consentono di generare un "sigillo elettronico qualificato", il quale gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato., facendo piena prova circa il rilascio del documento informatico da parte di una persona giuridica, garantendo la certezza dell'origine e dell'integrità del documento.

Il campo "*key usage*" consente di realizzare esclusivamente la funzione di "*Content commitment*" (non ripudio).

2.6.1.6. Certificato qualificato di Time Stamping Unit

Questo certificato è contrassegnato dall' OID 1.3.6.1.4.1.59699.8 e viene emesso in accordo con la politica di certificazione QCP-l-qscd.
I certificati di Time Stamping Unit sono generati per emettere validazioni temporali elettroniche qualificate ai sensi dell'art. 42 del Regolamento eIDAS.
La sincronizzazione del sistema di emissione di marche temporali di TeamSystem si effettua attraverso il protocollo NTP, puntando a un server con un livello di sincronizzazione *Stratum 3*.

2.6.1.7. Limiti e divieti nell'utilizzo dei certificati

I certificati emessi da TeamSystem vengono impiegati per la funzione che è propria loro, anche specificata nel campo *"key usage"*, e per le finalità stabilite nel presente Manuale Operativo, essendo precluso un loro impiego per altre funzioni o altre finalità diverse rispetto a quelle per le quali sono stati rilasciati.
Allo stesso modo, i certificati emessi da TeamSystem devono essere impiegati unicamente nel rispetto della normativa vigente.
I certificati non possono essere impiegati per firmare certificati di chiave pubblica di nessun tipo, né per firmare Liste di Revoca dei certificati (CRL).
TeamSystem non sarà considerata in nessun caso responsabile per l'uso fatto dei certificati in relazione a situazioni critiche che comportino, a titolo esemplificativo, rischi specifici per l'incolumità delle persone, danni ambientali, rischi specifici in relazione a servizi di trasporto di massa, alla gestione di impianti nucleari e chimici e di dispositivi medici.
L'impiego dei certificati emessi da TeamSystem in operazioni che contravvengono al presente Manuale Operativo, alle Condizioni Generali di Contratto, alla documentazione inerente a ciascuna tipologia di certificato, costituisce un utilizzo indebito e contrario agli effetti di legge, esimendo, pertanto, TeamSystem, da ogni responsabilità per ogni eventuale danno derivante da un utilizzo indebito dei certificati compiuto dal Titolare o da qualsiasi altra Parte.
TeamSystem non assume, in nessun caso, alcuna responsabilità per le informazioni, i dati, i contenuti, immessi o trasmessi, associati all'utilizzo del certificato, essendo unicamente il Titolare il soggetto responsabile dell'utilizzo del certificato e dei contenuti ad esso associati.
Parimenti, sarà imputabile al Titolare qualsiasi responsabilità che possa derivare dall'utilizzo del certificato al di fuori dei limiti e delle condizioni indicate nel presente Manuale Operativo, nelle Condizioni Generali di Contratto, nella documentazione inerente a ciascuna tipologia di certificato, così come da qualsiasi altro utilizzo considerato indebito dalla normativa vigente in materia.

Inoltre, l'utilizzo del certificato remoto sarà limitato ai documenti elettronici resi disponibili dal Cliente per l'apposizione del certificato da parte del Titolare esclusivamente nell'ambito degli applicativi TeamSystem, senza possibilità di utilizzo generalizzato.

2.6.1.8. Certificati non qualificati rilasciati da TeamSystem CA

TeamSystem eroga, oltre ai certificati qualificati, anche una tipologia di certificato non qualificato contraddistinto dall'OID: 1.3.6.1.4.1.59699.20.1. Questo certificato riporta la seguente Notice: "Certificato emesso ai fini della creazione di firme elettroniche non qualificate. Non è un certificato qualificato ai sensi del Regolamento (UE) n. 910/2014 (eIDAS)."

Tale certificato è destinato esclusivamente agli operatori TeamSystem per l'esecuzione di operazioni sulla piattaforma di gestione dei certificati (CMS). La sua emissione risponde a esigenze operative interne e non abilita l'uso per firme elettroniche qualificate.

2.7. Amministrazione del Manuale Operativo

2.7.1.1. Organizzazione responsabile

Il presente Manuale Operativo è aggiornato alla versione risultante dal "Controllo delle Versioni" o dal "Controllo Documentale" di cui alle "Informazioni Generali" del presente Manuale Operativo e viene redatto, pubblicato ed aggiornato da TeamSystem, che ne è anche responsabile.
I dati di contatto del TSP sono i seguenti:
Ragione Sociale: TeamSystem S.p.A.
Partita Iva: 01035310414
Sede legale: Via Sandro Pertini 88 (61122) – Pesaro (PU)
Tel: 0721 426601
Sito internet: https://www.teamsystem.com/
PEC: teamsystemgroup_qtsp@pecteamsystem.com

2.7.1.2. Procedura di approvazione e gestione

TeamSystem esegue un controllo di conformità di questo Manuale Operativo al processo di erogazione del servizio di certificazione e alle condizioni associate al medesimo.

Il presente documento viene riesaminato (ed eventualmente aggiornato, se necessario) almeno con frequenza annuale.

3. PUBBLICAZIONE DELLE INFORMAZIONI E REPOSITORY

3.1. Repository

TeamSystem dispone di un archivio on-line (c.d. Repository) attraverso il quale rende pubbliche e liberamente accessibili le informazioni relative ai servizi di certificazione. Suddetto archivio è pubblicato sul sito di TeamSystem raggiungibile al seguente indirizzo https://www.teamsystem.com/trust-services/documentazione.
Il "*Repository*" è accessibile in modo continuo (24x7x365).
Nell'ipotesi in cui si verifichi un arresto del sistema, al di fuori del controllo di TeamSystem, quest'ultima si impegnerà nel miglior modo possibile affinché il servizio ritorni di nuovo disponibile nel termine stabilito nella sezione 5 del presente Manuale Operativo.

3.2. Elenco delle informazioni pubblicate dalla CA

TeamSystem pubblica le seguenti informazioni:

- La Lista dei certificati revocati (CRL);
- Le *PKI Disclosure Statement* (PDS);
- Il proprio Manuale Operativo/*Certification Practice Statement*;
- Le Condizioni generali di contratto (Terms and Conditions o Condizioni Generali);
- La Modulistica relativa ai Servizi Fiduciari;
- I certificati della PKI.

3.3. Frequenza delle pubblicazioni

Le informazioni relative alla CA, incluso il presente Manuale Operativo, e la documentazione correlata, sono pubblicate non appena disponibili.
Le modifiche al Manuale Operativo sono soggette alle disposizioni di cui alla sezione 1 del presente documento.
Le informazioni relative allo stato di revoca dei certificati vengono pubblicate in accordo con quanto stabilito nella sezione 5.9 del presente Manuale Operativo.

3.4. Controllo degli accessi

TeamSystem non limita l'accesso alle informazioni stabilite nella sezione 2, tuttavia predispone un sistema di controllo atto ad impedire che soggetti non autorizzati possano aggiungere, modificare o cancellare i dati dalla stessa registrati, allo scopo di tutelare l'integrità e l'autenticità delle informazioni.

4. IDENTIFICAZIONE E AUTENTICAZIONE

4.1. Nomi

4.1.1.1. Tipologia dei nomi

Tutti i certificati sono contraddistinti da un nominativo identificativo (DN o *Distinguished Name*), conforme allo standard X.501, inserito nel campo *Subject*, il quale include un componente *Common Name* (CN=), relativo all'identità del Richiedente, congiuntamente ad altre informazioni addizionali, inserite nel campo *SubjectAlternativeName*.

Le regole di valorizzazione degli attributi del DN rispettano le norme ETSI EN in relazione ai profili dei certificati per persone fisiche/giuridiche nonché le specifiche contenute nella RFC 5280 e si conformano alle Raccomandazioni di cui alla Determinazione n. 147/2019 emessa dall'AgID.

Come previsto dagli standard ETSI EN 319 412-2 par. 4.2.4 e 319 412-3 par. 4.2.1, TeamSystem ha fissato i limiti dei campi givenName, surname, pseudonym, commonName, organizationName and organizationalUnitName a 500 (cinquecento) caratteri.

In particolare, i certificati emessi secondo questo documento CPS sono conformi ai seguenti standard:

- **ETSI EN 319-401**: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- **ETSI EN 319 411-1**: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- **ETSI EN 319 411-2**: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- **ETSI EN 319 412-1**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- **ETSI EN 319 412-2**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural person.
- **ETSI EN 319 412-5**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

4.1.1.2. Significato dei nomi

I nomi contenuti nei certificati sono i seguenti

- *Country;*

- *Organization;*
- *Organization Unit;*
- *Organization Identifier;*
- *Title;*
- *Surname;*
- *Given Name;*
- *Serial Number;*
- *Common Name;*

I nomi contenuti nei campi *SubjectName* e *SubjectAlternativeName* dei certificati sono comprensibili nel linguaggio naturale e dovranno essere significativi per consentire la corretta identificazione dei Titolari dei certificati e dei certificati di *Time Stamp Unit*.

Qualora, per realizzare prove tecniche di interoperabilità, l'Organismo supervisore competente (AgID) richieda, al fine di effettuare le sue valutazioni, di emettere certificati di prova, in questo caso, i relativi campi *DN* o *Subject* all'interno dei relativi certificati, saranno valorizzati con alcuni dei seguenti valori (a titolo esemplificativo e non esaustivo): "*Organizzazione test*", "*Nome test*", "*Cognome test*" o parole che inequivocabilmente ne denotano l'invalidità (es. "TEST", "PROVA" o "NON VALIDO").

I suddetti certificati vengono emessi al fine di realizzare prove tecniche di interoperabilità e permettere all'Organismo supervisore competente (AgID) di effettuare le sue valutazioni

4.1.1.3. Impiego di dati anonimi e pseudonimi

In nessun caso è possibile utilizzare pseudonimi al fine di identificare un Titolare persona fisica. Allo stesso modo, in nessun caso verranno emessi certificati anonimi.

Diversamente vale per il caso in cui Richiedente sia una persona giuridica: in questa circostanza è ammessa la possibilità di utilizzare uno pseudonimo per la sua identificazione all'interno del certificato.

4.1.1.4. Regole di interpretazione dei nomi

Per le regole di interpretazione dei nomi, viene rispettato lo standard ITU-T relativo ai servizi di directory (ITU-T X.500 ovvero ISO/IEC 9594).

4.1.1.5. Unicità dei nomi

Per garantire la correlazione univoca tra Titolare e certificato, la sezione *Subject* di quest'ultimo non può mai essere identica per due distinti titolari. Pertanto, secondo quanto indicato dalla norma ETSI EN 319 412 in merito ai profili di emissione dei certificati, il campo *Subject* (*SubjectDistinguishedName o SubjectDN*) contiene attributi identificativi specifici in base alla natura del Titolare stesso.

In particolare, l'unicità viene garantita dai seguenti attributi:

- il *SerialNumber* (OID 2.5.4.5) contenente il codice fiscale del soggetto (indicato con il prefisso *TIN*) o, in alternativa, un codice identificativo in ottemperanza alla norma ETSI EN 319 412-1 (come il numero del passaporto o della carta d'identità elettronica del titolare);
- l'*OrganizationName* (OID 2.5.4.10) utilizzato per indicare l'appartenenza o l'affiliazione del titolare all'organizzazione. Nel caso in cui l'*OrganizationName* sia presente, in medesimi vincoli si applicano anche all'eventuale codifica dell'attributo *Title*. Nel caso in cui il soggetto da identificare sia una persona giuridica l'attributo verrà valorizzato in accordo al paragrafo 4.2.1 della norma ETSI 319 412-3.
- il *Givenname* (OID 2.5.4.42) contenente il nome del soggetto;
- il *Surname* (OID 2.5.4.44) contenente il cognome del soggetto;

È, inoltre, prevista la possibilità di inserire nell'attributo *description* (OID 2.5.4.13) il codice EORI (*Economic Operator Registration and Identification*) di cui al Regolamento (UE) n. 312/2009 del 16 aprile 2009 e s.m.i.

Per le persone giuridiche, con riferimento all'uso della sintassi dell'identificatore "*legal person identifier*" di cui al capo 5.1.4. dello standard ETSI EN 319 412-1, in caso di organizzazioni non dotate di partita IVA, ma solo di codice fiscale si seguirà la modalità di cui al n. 3 del capo 5.1.4. citato (tramite l'utilizzo dei caratteri "CF").

L'unicità per i certificati qualificati di marca temporale (TSU) viene parimenti assicurata da TeamSystem, che si conforma alla specifica RFC-5280 nonché alle Raccomandazioni di cui all'art. 4.2 della Determinazione n. 147/2020 di AgID rubricato "Profilo dei Certificati di certificazione e validazione temporale".

4.1.1.6. Eventuali limitazioni d'uso

Ulteriori limiti d'uso del certificato saranno inseriti nell'attributo *explicitText* del campo *userNotice* dell'estensione *certificatePolicies*.

TeamSystem garantisce, in conformità all'art. 4.1 n. 7 della Determinazione n. 147/2019 di AgID, almeno i seguenti limiti di utilizzo:

- i titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato;
- il presente certificato è valido solo per firme apposte con procedura automatica;
- l'utilizzo del certificato è limitato ai rapporti con (indicazione del soggetto).

Per ulteriori informazioni sulle limitazioni di uso si rimanda al Par. 5.5. del presente Manuale.

4.1.1.7. Soluzione dei conflitti relativi ai nominativi

TeamSystem non è tenuta a verificare previamente che un Richiedente il certificato sia titolare del diritto all'uso del nome che compare in una richiesta di certificato ma, salvo tale circostanza non risulti evidente, provvederà al rilascio del certificato.

La medesima modalità sarà applicata anche nel caso in cui il Richiedente agisca in rappresentanza di una persona giuridica.
Parimenti, non agirà come arbitro o mediatore né in nessun altro modo dovrà dirimere alcuna disputa riguardante la titolarità dei nomi delle persone fisiche o giuridiche, i nomi del dominio, i marchi o i nominativi commerciali.
Nel caso in cui TeamSystem riceva una notifica relativa alla sussistenza di un conflitto sui nomi, sulla base della legislazione vigente nello Stato del Richiedente, potrà intraprendere le azioni pertinenti orientate a bloccare o ritirare il certificato emesso.
In ogni caso, la CA si riserva il diritto di rigettare una richiesta di certificato, nell'ipotesi in cui sussista un conflitto sui nomi.

4.2. Verifica iniziale dell'identità

La CA, verifica con certezza l'identità di ogni Richiedente alla richiesta di emissione di un certificato qualificato al fine di assicurare che quel certificato possa riferirsi in maniera accurata e completa a quest'ultimo (sia esso persona fisica o giuridica); prima di procedere al rilascio del certificato richiesto, dunque, la CA dovrà svolgere tutte le attività necessarie all'identificazione del Richiedente.
L'identità del Richiedente viene solitamente verificata tramite modalità elettroniche che garantiscono l'identificazione certa del richiedente.
Tutte le evidenze dell'identificazione così effettuata e verificata sanno conservate dalla CA, in conformità a quanto disposto dal Regolamento (UE) 2016/679, per tutto il tempo necessario ad assicurare la fruizione e la continuità del servizio richiesto, e comunque per un periodo di 20 (venti) anni dalla scadenza/revoca del certificato come richiesto dal CAD.
Per garantire il rispetto del principio di trasparenza e correttezza ai sensi del Regolamento (UE) 2016/679 e, in generale, la tutela e la gestione dei dati personali acquisiti nel corso delle procedure di registrazione, inoltre, sarà preventivamente fornita ad ogni richiedente una specifica informativa sulla privacy.
Per il dettaglio della procedura di identificazione di una persona fisica o di una persona giuridica è possibile fare riferimento ai par. 4.2.1.2. e seguenti.

4.2.1.1. Prova del possesso della chiave privata

Il possesso della chiave privata è comprovato dal corretto svolgimento del procedimento di rilascio ed accettazione del certificato da parte del Richiedente e/o Titolare.
In particolare, TeamSystem verifica che il Richiedente sia in possesso della chiave privata corrispondente alla chiave pubblica da certificare.

4.2.1.2. Autenticazione dell'identità di una persona fisica

Questa sezione illustra i metodi di verifica dell'identità di una persona fisica identificata in un Certificato.
La CA le operazioni di identificazione secondo le modalità previste nel presente Manuale Operativo, in conformità alle linee guida di cui al Par. 6.2 dell'ETSI EN 319 411-2 e s.m.i. e ai criteri di cui alla "*Baseline Requirements Guidelines*" e alla clausola 11 dell'"*Extended Validation Certificate Guidelines*" e ogni altra normativa nazionale ed europea applicabile.
L'identità dei Richiedenti, identificati nei Certificati, è comprovata dalle modalità descritte di seguito.
Le modalità di identificazione previste sono:

Modalità di identificazione	**Soggetti abilitati all'identificazione**	**Strumenti necessari**
Firma digitale o qualificata (QES)	Certification Authority (CA)	Un certificato di firma elettronica qualificata emesso da un Prestatore di Servizi Fiduciari Qualificato
Videoidentificazione da remoto	Registration Authority (RA)	Device con strumenti per l'esecuzione di videochiamata sincrona con operatore
Carta d'Identità Elettronica (CIE)	Certification Authority (CA)	CIE livello 3

4.2.1.3. Procedura di identificazione con certificato di firma digitale o qualificata

L'identificazione si basa sul riconoscimento (già) effettuato da altro Prestatore di Servizi Fiduciari Qualificato per il rilascio di un certificato qualificato a norma del Regolamento eIDAS. L'identità del Richiedente è accertata attraverso procedure di identificazione informatica basate sull'acquisizione del modulo di richiesta firmato elettronicamente con il certificato qualificato, ancora in corso di validità, contenuto nel dispositivo sicuro (QSCD) in possesso del Titolare. Non sono ammessi certificati di firma digitale o qualificata che riportano il limite d'uso <IT: "Il certificato emesso tramite il Sistema Pubblico di Identità Digitale (SPID) non è utilizzabile per richiedere un'altra Identità Digitale (SPID)"; EN: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) is not usable to require another SPID digital identity">, contraddistinti dall'OID "1.3.76.16.5".
Questa procedura di identificazione è l'unica ammessa per il rilascio del certificato qualificato di sigillo.

.

4.2.1.4. Procedura di identificazione mediante videoidentificazione da remoto

La videoidentificazione da remoto è una procedura di identificazione a distanza di tipo assistito (attended remote identity proofing), condotta in tempo reale da un operatore qualificato e adeguatamente formato di un fornitore di servizi di identity proofing (Identity Proofing Service Provider) incaricato da TeamSystem, mediante una sessione audio-video interattiva con il Richiedente. La procedura è conforme all'art. 24, par. 1, lett. d) del Regolamento eIDAS, quale metodo di identificazione che assicura una certezza equivalente alla presenza fisica, ed è realizzata nel rispetto dello standard ETSI TS 119 461 con livello di identity proofing elevato (Extended Level of Identity Proofing), come richiesto per il rilascio di certificati qualificati. La conformità del metodo di videoidentificazione all'art. 24 del Regolamento eIDAS, in termini di garanzia equivalente alla presenza fisica, è confermata da un Organismo di valutazione della conformità (Conformity Assessment Body, CAB).
Nel corso della sessione il Richiedente esibisce un documento di identità in corso di validità, tra carta d'identità elettronica (CIE), passaporto o patente di guida. L'operatore ne verifica l'autenticità e la validità, la coerenza dei dati riportati e la corrispondenza tra il volto del Richiedente e la fotografia del documento. La procedura è dotata di controlli antifrode che comprendono la verifica della presenza in vita (liveness detection) e il rilevamento degli attacchi di presentazione e di iniezione (Presentation Attack Detection, PAD; Injection Attack Detection, IAD), anche al fine di prevenire l'utilizzo di artefatti o contenuti manipolati (deep fake).
La sessione di videoidentificazione è integralmente registrata. Le evidenze dell'identificazione così acquisite, comprese le registrazioni audio-video, sono conservate da TeamSystem, in conformità al CAD e alle Linee Guida AgID, per il medesimo periodo di 20 anni previsto per la restante documentazione di identificazione, decorrente dalla data di scadenza del certificato.

4.2.1.5. Procedura di identificazione mediante Carta d'Identità Elettronica (CIE livello 3)

L'identificazione può essere effettuata mediante la Carta d'Identità Elettronica (CIE) utilizzata con livello di garanzia elevato (CIE livello 3, corrispondente al Level of Assurance "alto"), schema di identificazione elettronica notificato ai sensi del Regolamento eIDAS. Il Richiedente si autentica mediante la lettura del microchip della CIE in modalità di prossimità (NFC) e l'inserimento del PIN associato alla carta, di cui ha conoscenza esclusiva.
Tale modalità è ammessa ai sensi dell'art. 24, par. 1, lett. b) del Regolamento eIDAS, che consente l'identificazione del Richiedente tramite mezzi di identificazione elettronica notificati conformi a un livello di garanzia "alto". I dati identificativi acquisiti dalla CIE lv. 3 sono verificati dalla CA e conservati tra le evidenze dell'identificazione.

4.2.1.6. Autenticazione dell'identità di una persona giuridica

Nel caso in cui il soggetto da identificare sia una persona giuridica, il Richiedente dovrà sottoporsi alle procedure di identificazione previste nel precedente capo 4.2. fornendo, in aggiunta, anche i dati relativi alla persona giuridica (visura, certificato camerale o documento equipollente).
A tal fine, il Richiedente dovrà, quindi, presentare la documentazione necessaria ad attestare il possesso dei poteri di rappresentanza (certificato camerale o visura storica/ordinaria da cui risulti la carica dichiarata) e/o di delega da persona munita di tale potere.

4.2.1.7. Misure anticontraffazione

Al fine di prevenire il verificarsi di ogni possibile furto di identità (mediante impersonificazione *totale* o *parziale*) TeamSystem ha implementato rigide misure per l'adeguata verifica dell'identità dei Richiedenti attuate durante le procedure di identificazione condotte ai sensi del presente Manuale (v. par. 4.2.1.1. e ss.).
TeamSystem si riserva il diritto di sottoporre i dati raccolti in fase di identificazione ad ulteriori controlli eseguiti preliminarmente o successivamente all'emissione dell'identità attraverso dei controlli a campione o sistematici eseguiti da personale interno del Certificatore o di fornitori esterni di cui eventualmente intenderà avvalersi.

4.2.1.8. Informazioni non verificate

TeamSystem non include nei certificati nessuna informazione relativa al Richiedente e/o Titolare che non sia stata correttamente verificata.

4.3. Identificazione e autenticazione per le richieste di revoca o sospensione

TeamSystem ha il compito di gestire le richieste relative alla revoca di un certificato.
L'identificazione dei Richiedenti e/o dei Titolari nel processo di revoca e sospensione dei certificati può essere effettuata:

- dal Richiedente e/o il Titolare:
  - tramite autenticazione presso le pagine di TeamSystem e successiva richiesta seguendo le istruzioni indicate nel sistema messo a disposizione per questo scopo;
  - Inviando una richiesta via email o PEC alla casella PEC teamsystemgroup_qtsp@pecteamsystem.com utilizzando il modello messo a disposizione presso il sito https://www.teamsystem.com/trust-services/documentazione/, allegando la documentazione indicata nel modello stesso.

5. REQUISITI OPERATIVI RELATIVI AL CICLO DI VITA DEI CERTIFICATI

5.1. Domanda di emissione del certificato

5.1.1.1. Legittimazione della richiesta

Il Richiedente è tenuto ad accettare e sottoscrivere i termini e le condizioni generali del servizio di TeamSystem per consentire a quest'ultima di procedere con la richiesta di rilascio del certificato, previa procedura di identificazione da condursi con una delle modalità indicate nel capitolo precedente.

5.1.1.2. Procedure e responsabilità

TeamSystem riceve le richieste di certificati: tali richieste vengono inoltrate tramite un modulo, digitale, tramite appositi servizi Web predisposti da TeamSystem.
La domanda deve essere accompagnata da una documentazione di supporto relativa all'identità e da altre informazioni sulla persona fisica identificata nel certificato, in conformità alle disposizioni della sezione 3. Inoltre, è necessario indicare un indirizzo fisico o altri dati che consentano di contattare la persona fisica/giuridica identificata nel certificato.

5.2. Elaborazione della richiesta

5.2.1.1. Svolgimento delle funzioni di identificazione ed autenticazione

Ricevuta una richiesta di emissione di un certificato qualificato, TeamSystem verifica che quest'ultima sia completa, accurata e debitamente autorizzata, prima di elaborarla.
In caso di esito positivo, TeamSystem analizza le informazioni fornite, verificandone la compatibilità con gli aspetti descritti nel capitolo 3 del presente Manuale.
La documentazione inerente la richiesta ed emissione dei Certificati Qualificati deve essere conservata e debitamente registrata, a cura del Certificatore, e con garanzie di sicurezza e integrità per un periodo di 20 anni dalla data di scadenza del Certificato Qualificato, anche in caso di perdita anticipata della validità del certificato dovuta alla sua revoca.

5.2.1.2. Approvazione o rifiuto della richiesta

Nel caso in cui la verifica dei dati forniti in sede di richiesta di emissione del Certificato Qualificato abbia esito positivo, TeamSystem approverà la richiesta e procederà alla emissione e messa a disposizione del Certificato Qualificato.
Se dalla verifica effettuata emerge che le informazioni fornite sono errate, o nel caso in cui tali informazioni vengano giudicate non affidabili, inesatte, incomplete o incoerenti, TeamSystem rigetterà la richiesta o interromperà la sua approvazione fino a quando non avrà effettuato i controlli che riterrà necessari.
Se, a seguito di eventuale ulteriore verifica, dovesse risultare che le informazioni fornite non sono corrette, TeamSystem rifiuterà definitivamente la richiesta.
TeamSystem comunica al Richiedente l'approvazione o il rifiuto della richiesta.
TeamSystem ha automatizzato le procedure che permettono di verificare la correttezza delle informazioni contenute nei certificati e i processi di approvazione delle domande.

5.2.1.3. Termine per l'elaborazione della richiesta

TeamSystem elabora e lavora le richieste di certificati in ordine di arrivo entro il tempo necessario per gli adempimenti di carattere tecnico.
Le richieste rimangono attive fino alla loro approvazione o rifiuto.

5.3. Emissione del certificato

5.3.1.1. Processo e modalità di emissione

Durante il processo di emissione TeamSystem:

a. garantisce la riservatezza e l'integrità dei dati di registrazione forniti;
b. utilizza sistemi e prodotti affidabili che siano protetti da qualsiasi alterazione possibile e che garantiscono la sicurezza, dal punto di vista tecnico, dei processi in cui vengono adoperati;
c. produce una coppia di chiavi, tramite una procedura sicura di generazione;
d. implementa un processo di generazione di certificati che collega in modo sicuro il certificato alle informazioni di registrazione, inclusa la chiave pubblica certificata;
e. assicura che il certificato sia rilasciato da sistemi protetti da ogni possibile contraffazione e che garantiscono la riservatezza delle chiavi durante il processo di generazione di queste ultime;
f. indica la data e l'ora in cui è stato emesso un certificato;
g. garantisce il controllo esclusivo delle chiavi da parte dell'utente, di modo che terzi non possano detrarle o utilizzarle in alcun modo.

L'emissione del certificato qualificato (di firma o di sigillo) con le modalità indicate potrà avvenire su dispositivo *HSM* (di firma remota). Il certificato qualificato di sottoscrizione di persona fisica può, inoltre, essere emesso su un dispositivo fisico di firma (smart card o token) qualificato come dispositivo per la creazione di una firma qualificata (QSCD).
Nei paragrafi che seguono è descritto il flusso di emissione del certificato qualificato con le diverse modalità sopra indicate.

5.3.1.2. Emissione del certificato su dispositivo HSM (firma remota)

La modalità di emissione del certificato ai sensi del presente paragrafo – emissione del certificato su dispositivo di firma remota (senza che vi sia la presenza di un dispositivo fisico) – prevede che l'emissione avvenga su dispositivo HSM della CA.
In questo caso, la generazione della coppia di chiavi crittografiche avviene direttamente sull'HSM, a cura della CA, eseguendo opportune chiamate autenticate ai servizi di Uanataca, affinché quest'ultima, verificata la validità dell'autenticazione e la provenienza della richiesta da soggetto autorizzato, genera il certificato qualificato, successivamente memorizzato all'interno dell'HSM.
La CA, prima dell'emissione dell'identità, verifica la correttezza dei fattori di sicurezza inviati al Richiedente ed utilizzati in fase di emissione del Certificato.

5.3.1.3. Emissione del certificato di sottoscrizione su dispositivo fisico (smart card o token)

In alternativa all'emissione su HSM, il certificato qualificato di sottoscrizione di persona fisica può essere emesso su un dispositivo fisico di firma consegnato al Titolare, costituito da una smart card, utilizzabile mediante apposito lettore, ovvero da un token USB. Tale dispositivo costituisce un dispositivo qualificato per la creazione della firma (Qualified Signature Creation Device, QSCD) ai sensi degli artt. 29 e 51 del Regolamento eIDAS, conforme allo standard EN 319 411-2.
La coppia di chiavi crittografiche è generata e custodita all'interno del dispositivo, in modo da assicurare al Titolare il controllo esclusivo dei dati per la creazione della firma; la chiave privata non è esportabile dal dispositivo. A seguito dell'esito positivo dell'istruttoria e della verifica dell'identità del Richiedente, la CA genera il certificato qualificato e ne abilita l'uso sul dispositivo, che viene consegnato al Titolare unitamente ai codici di attivazione secondo modalità che ne garantiscono la riservatezza.

5.3.1.4. Emissione del certificato di TSU

La richiesta di certificato viene eseguita manualmente da un operatore di sistema che opera per conto di TeamSystem ed è coinvolto nel processo di conduzione tecnica dei sistemi.

- L'operatore provvede alla generazione di una coppia di chiavi all'interno della partizione dell'HSM dedicata al servizio di marcatura temporale e, contestualmente, alla creazione della richiesta di certificato (CSR) in formato PKCS#10. Successivamente procede all'emissione del certificato di TSU tramite la TSA.
- Il certificato emesso viene quindi associato alla chiave precedentemente generata e installato sull'HSM, completando così la configurazione del servizio di marcatura temporale.

In conformità a quanto previsto dall'art. 49, comma 3, del DPCM 22 febbraio 2013, una volta emesso il certificato di marcatura temporale, le chiavi di marcatura temporale sono gestite in conformità alle procedure interne di sicurezza di TeamSystem, che garantiscono la corretta conservazione, rotazione e tracciabilità delle stesse, indipendentemente dal periodo di validità del certificato di TSU, che viene sostituito dopo non più di tre mesi di utilizzazione.

.

5.3.1.5. Notifica di emissione del certificato

TeamSystem comunica l'emissione del certificato al Richiedente agli indirizzi da quest'ultimo forniti. Inoltre, se la procedura lo prevede, anche il Cliente, su applicativi messi a disposizione da TeamSystem, può ricevere una notifica relativamente all'avvenuta emissione di un certificato.

5.4. Consegna e accettazione del certificato

5.4.1.1. Processo di accettazione del certificato

L'accettazione del certificato qualificato da parte della persona fisica o della persona giuridica identificata nel certificato stesso viene effettuata sottoscrivendo il modulo di richiesta e le condizioni contrattuali che disciplinano il certificato qualificato.

5.4.1.2. Notifica dell'emissione a terzi

TeamSystem non notificherà alcuna emissione del certificato a favore di terzi diversi dal Titolare.

5.5. Uso della coppia di chiavi e del certificato

5.5.1.1. Utilizzo da parte del Richiedente e/o Titolare

Il Titolare del certificato qualificato è tenuto a:

- leggere ed accettare integralmente il contenuto del presente documento prima di richiedere il certificato;
- fornire alla CA informazioni esatte, complete e veritiere in fase di richiesta del certificato;
- esprimere il suo consenso preventivamente all'emissione e alla consegna di un certificato;
- utilizzare la propria chiave privata e il proprio certificato unicamente per gli scopi previsti dal presente documento;
- adottare misure di sicurezza atte a prevenire l'uso non autorizzato della propria chiave privata;
- assicurare la confidenzialità dei codici riservati (come ad esempio PIN, PUK, OTP);
- richiedere tempestivamente alla CA la revoca del certificato nel caso di sospetta compromissione della propria chiave privata;
- nel caso di accertata compromissione della propria chiave privata, richiedere tempestivamente alla CA la revoca del certificato;
- prima di cominciare ad utilizzare la chiave privata, verificare che il certificato emesso abbia il profilo previsto e contenga informazioni corrette, incluse le eventuali limitazioni d'uso così come riportate nel modulo di richiesta;
- fino alla data di scadenza o di eventuale revoca del proprio certificato, informare prontamente la CA nel caso in cui: il proprio dispositivo di firma sia andato perso, sia stato sottratto; abbia perso il controllo esclusivo della propria chiave privata, per esempio a causa della compromissione dei dati di attivazione (PIN o password); alcune informazioni contenute nel certificato siano inesatte o non più valide;
- revocare immediatamente il certificato nel caso di compromissione della propria chiave privata (per esempio, a causa dello smarrimento del PIN o della sua rivelazione a terzi non autorizzata), e cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata;

A seguito della richiesta del certificato il Titolare assume consapevolmente le seguenti responsabilità affinché:

- tutte le informazioni fornite contenute nel certificato siano corrette;
- il certificato sia utilizzato esclusivamente per usi legali e autorizzati, in conformità con il presente Manuale Operativo;
- il certificato sia utilizzato esclusivamente entro le limitazioni di uso eventualmente in esso contenute;
- nessuna persona non autorizzata abbia accesso alla chiave privata del certificato, assumendosi, inoltre, l'esclusiva responsabilità per i danni causati dalla mancata protezione della chiave privata;
- non cedere o concedere in uso in nessuna circostanza la chiave privata (trattandosi di un elemento strettamente personale) a terzi.

5.5.1.2. Utilizzo da parte delle Relying Parties

5.5.1.3. Obblighi delle Relying Parties

Tutti coloro che fanno affidamento sulle informazioni contenute nei certificati (R.P., termine abbreviato per indicare le Relying Parties), in ossequio a quanto disciplinato dal requisito OVR-6.3.5-03 delle norme ETSI EN 319 411-1/411-2 hanno l'obbligo di:

- Verificare che il certificato non sia scaduto;
- verificare lo stato di validità del certificato, vale a dire la sua eventuale revoca utilizzando le informazioni correnti sullo stato di revoca. La convalida deve essere effettuata tenendo in considerazione lo stato del certificato alla data-ora rilevante per la RP, secondo il particolare contesto (es. data-ora corrente, data-ora di apposizione della firma nel caso in cui essa possa essere dimostrabile attraverso una marca temporale apposta al documento).;
- tenere conto di eventuali limitazioni all'uso del certificato.

All'interno dell'Allegato "A" al presente Manuale è presente il link, insieme al relativo manuale, dell'applicativo messo a disposizione da TeamSystem al fine di consentire alle Relying Parties la verifica dei certificati.
Le Relying Parties possono, inoltre, utilizzare gli indicatori e le disposizioni di cui al presente manuale per determinare l'idoneità e l'affidabilità dei certificati nel quadro del Regolamento (UE) n. 910/2014.

5.5.1.4. Responsabilità civile delle Relying Parties

Tutti coloro che fanno affidamento sulle informazioni contenute nei certificati sono responsabili quanto a:

- disporre di informazioni sufficienti per prendere decisioni in merito all'affidabilità di un certificato;
- accettare la veridicità delle informazioni contenute nel certificato;
- rispettare gli obblighi gravanti su di sé come Relying Parties, secondo quanto disposto nel precedente paragrafo.

5.5.1.5. Limiti d'uso e di valore

TeamSystem, in conformità alla Determinazione n. 147/2019 di AgID recante "*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati,* firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" garantisce i limiti di uso di cui al Par. 4.1.1.6. ed informa i Richiedenti circa le seguenti ulteriori limitazioni di uso, specificate nei certificati mediante l'attributo *userNotice* dell'estensione CertificatePolicies o tramite Policy OID dedicati:

a. I certificati digitali qualificati della tipologia "*One-Shot*". contengono almeno uno dei seguenti limiti di uso:
   1) IT: "*L'utilizzo del certificato è limitato esclusivamente alla sottoscrizione dei documenti cui la firma è apposta*".

EN: "*The use of the certificate is limited exclusively to the signature of the underlying documents*".

2) IT: "*L'utilizzo del certificato è limitato esclusivamente alla sottoscrizione dei documenti cui la firma è apposta e, comunque, limitatamente ai rapporti tra il sottoscrittore e (inserire soggetto)*";
EN: "*The use of the certificate is limited exclusively to the signature of the underlying document and, in any case, limited to the relationships between the subscriber and (insert subject name)*".

b. I certificati digitali qualificati automatici (sia di firma che di sigillo) contengono il seguente limite di uso:

3) IT: "Il presente certificato è valido solo per firme apposte con procedura automatica".
EN: "*This certificate is valid only for signatures used through an automated procedure*".

c. I certificati digitali qualificati remoti contengono il seguente limite di uso:

4) IT: "il certificato può essere utilizzato solo nel dominio applicativo TeamSystem".
EN: "*The certificate may only be used within the TeamSystem application domain.*".
Il presente limite d'uso relativo al dominio applicativo TeamSystem non si applica ai certificati qualificati di sottoscrizione emessi su dispositivo fisico (smart card o token), che possono pertanto essere utilizzati dal Titolare anche al di fuori del dominio applicativo TeamSystem.

Fatti salvi i casi di responsabilità della CA normativamente previsti (v. art. 30 co. 1 del CAD) il Titolare è tenuto alla verifica dei limiti di uso e di valore inseriti nel certificato nonché alla loro scrupolosa osservanza.
Specifici limiti d'uso potranno essere introdotti per meglio descrivere e/o delimitare l'ambito di applicazione nel dominio della CA. In particolare, in caso di valorizzazione del limite d'uso inerente al dominio della CA il Titolare potrà utilizzare i certificati qualificati unicamente all'interno dei sistemi applicativi gestiti, anche tramite API (*Application Programming Interface*) dal Certificatore.
La mancata osservanza, da parte del Titolare, dei limiti di uso del certificato non determina e non potrà determinare il sorgere di qualsivoglia responsabilità in capo alla CA (per ulteriori informazioni sui diritti e gli obblighi del Titolare e della CA si rimanda al Capitolo 10 del presente Manuale – v. Par. 10.1.5.5. *infra*).

5.6. Rinnovo di chiavi e certificati

5.6.1.1. Procedura di rinnovo

TeamSystem non ammette in nessuna circostanza il rinnovo del certificato.

5.7. Key Changeover (re-key dei certificati)

TeamSystem non ammette in nessuna circostanza il *rekeying* del certificato.

5.8. Modifica dei certificati

La modifica dei certificati qualificati, applicabile nei casi in cui variano le informazioni identificative del Titolare (ad eccezione della modifica della chiave pubblica che si effettua nel caso di rinnovo) sarà gestita come un'emissione di un nuovo certificato qualificato, applicando quanto descritto nella sezione 4.

5.9. Revoca e sospensione di un certificato

La revoca e la sospensione di un certificato qualificato comportano la cessazione della sua validità. La revoca comporta la cessazione anticipata e definitiva della validità del certificato. È pertanto una condizione irreversibile che non consente la riattivazione del certificato.
La sospensione comporta l'interruzione momentanea della validità di un certificato e consente la successiva riattivazione oppure la revoca definitiva. La riattivazione di un certificato sospeso ne determina la sua validità anche per il periodo di sospensione.
La revoca o sospensione del certificato diventano efficaci con l'inserimento del numero di serie del certificato all'interno della CRL – *Certificate Revocation List*, vale a dire una lista dei certificati revocati.
Questa viene pubblicata da parte di TeamSystem per consentire agli interessati la consultazione necessaria alla determinazione dello stato di validità dei certificati emessi da TeamSystem.
Con la stessa finalità, TeamSystem rende disponibile la stessa informazione mediante il protocollo OCSP.
I certificati qualificati di sottoscrizione One-Shot, non possono essere né revocati né sospesi.

5.9.1.1. Ipotesi di revoca di un certificato

TeamSystem revoca un certificato qualificato quando si presenta una delle seguenti cause (elenco non esaustivo):

1. **circostanze che influenzano le informazioni contenute nel certificato:**
   a) modifica di alcuni dei dati contenuti nel certificato, successivamente all'emissione del certificato corrispondente;
   b) prova della non correttezza dei dati contenuti nella richiesta di certificato;
2. **circostanze che influiscono sulla sicurezza della chiave o del certificato:**
   a) compromissione della chiave privata, dell'infrastruttura o dei sistemi della CA, a condizione che ciò influisca sull'affidabilità dei certificati rilasciati;
   b) violazione dei requisiti previsti nelle procedure di gestione dei certificati, stabiliti nel presente Manuale Operativo;
   c) sospetto o prova di compromissione della sicurezza della chiave o del certificato emesso;
   d) accesso o uso non autorizzato, da parte di terzi, della chiave privata corrispondente alla chiave pubblica contenuta nel certificato;

e) uso improprio del certificato da parte della persona fisica identificata nel certificato o mancanza di diligenza nella custodia della chiave privata o negli strumenti di attivazione della stessa.

3. **circostanze che riguardano il Richiedente e/o il Titolare:**
   a) cessazione del contratto tra la CA e il Richiedente e/o il Titolare;
   b) modifica o risoluzione anticipata del contratto tra la CA e il Richiedente e/o il Titolare;
   c) violazione da parte del Richiedente il certificato dei requisiti prestabiliti per la sua richiesta;
   d) violazione da parte del Richiedente e/o del Titolare degli obblighi contrattuali;
   e) incapacità sopravvenuta del Richiedente e/o Titolare;
   f) decesso del Richiedente e/o Titolare;
   g) richiesta esplicita di revoca del certificato da parte del Titolare e/o del suo rappresentante, per qualsiasi motivo, conformemente alle disposizioni della sezione 3.
4. **altre circostanze:**
   a) cessazione del servizio di certificazione da parte dell'Autorità di certificazione TeamSystem;
   b) utilizzo del certificato non conforme e pregiudizievole per TeamSystem, specie in modo continuativo;
   c) provvedimento dell'Autorità giudiziaria.

Inoltre, un utilizzo è considerato dannoso in base ai seguenti criteri:

- la natura e il numero di reclami ricevuti;
- l'identità dei soggetti che presentano i reclami;
- la legislazione applicabile;
- la risposta fornita dal Richiedente rispetto ai reclami ricevuti.

5.9.1.2. Chi può richiedere la revoca

Può domandare la revoca del certificato il Titolare ed il Richiedente il sigillo con le modalità appresso indicate, oltre che da TeamSystem laddove venisse ravvisata detta necessità.
Inoltre, la revoca può essere richiesta dall'Autorità Giudiziaria e tali segnalazioni, vista la specifica identità del segnalatore, saranno trattate con maggiore priorità rispetto alle altre.

5.9.1.3. Procedura di revoca

Il soggetto che richiede la revoca di un certificato può farlo rivolgendosi direttamente a TeamSystem attraverso il servizio online disponibile sulla pagina web di TeamSystem. La richiesta di revoca dovrà includere le informazioni seguenti:

- data della richiesta di revoca;
- dati identificativi del Titolare o Richiedente;
- recapiti della persona che chiede la revoca;

- motivazione della richiesta di revoca.

Il servizio di revoca è disponibile al sito web di TeamSystem all'indirizzo https://ca.teamsystem.cloud/owner-portal.
La richiesta di revoca può essere attivata anche attraverso la trasmissione dell'apposito modulo disponibile sulla pagina web di Teamsystem https://www.teamsystem.com/trust-services/documentazione/ debitamente compilato e sottoscritto dal soggetto che richiede la revoca, il quale dovrà allegare anche l'apposita documentazione indicata nel modulo medesimo.
Prima di procedere alla revoca, la richiesta deve essere gestita da TeamSystem attraverso il suo personale dedicato.
In seguito all'elaborazione della richiesta di revoca, il cambio di stato del certificato verrà notificato al Richiedente.
Il servizio di revoca è considerato un servizio critico, incluso nel piano di emergenza e di continuità operativa di TeamSystem.

5.9.1.4. Periodo di grazia della richiesta di revoca

TeamSystem esegue la revoca con la massima tempestività e attenzione, garantendo che il tempo necessario per l'elaborazione dell'operazione di revoca o sospensione e il conseguente aggiornamento dello stato del certificato (effettuato tramite pubblicazione di una nuova lista di revoca CRL) sia il più ridotto possibile.

5.9.1.5. Durata dell'elaborazione della richiesta di revoca

Se la revoca viene richiesta inviando il modulo ai canali email e PEC indicati nei paragrafi precedenti, la richiesta sarà elaborata entro il consueto orario d'ufficio di TeamSystem. Se effettuata tramite il servizio online, avrà effetto immediato.
In caso di ricezione da parte di TeamSystem di una richiesta di revoca, questa viene processata immediatamente per ridurre al minimo il tempo dopo il quale la revoca diventa effettiva (che coincide con la pubblicazione del certificato in una nuova CRL).
Il certificato revocato viene inserito nella CRL entro 1 ora dalla revoca e comunque in nessuna circostanza oltre le 24 ore successive all'operazione.

5.9.1.6. Verifica delle informazioni relative alla revoca dei certificati

Tutti coloro che devono fare affidamento sulle informazioni contenute nei certificati (c.d. "Relying Parties") hanno l'obbligo, prima di accettare un certificato, di verificare che quest'ultimo non sia scaduto alla data della verifica e che sia valido alla medesima data.
Un metodo per effettuare tale verifica è consultare la Lista di Revoca dei certificati (CRL) più recente emessa da TeamSystem.
La Lista di Revoca dei Certificati è pubblicata al seguente indirizzo (URL) https://ca.teamsystem.com/pki/crl/teamsystem_ca.crl

Tale indirizzo è riportato in ciascuno dei certificati emessi da TeamSystem, nella sezione "*CRL Distribution Point*".
La verifica, inoltre, può essere compiuta mediante interrogazione del servizio OCSP erogato da TeamSystem al seguente indirizzo: https://ca.teamsystem.com/pki/ocsp.

5.9.1.7. Frequenza di emissione della CRL

TeamSystem emette una nuova CRL quanto meno ogni 24 ore, indipendentemente dalla presenza o meno di nuove richieste di revoca.

5.9.1.8. Pubblicazione delle CRL

Le CRL vengono pubblicate immediatamente dopo essere state create. La latenza tra l'istante della creazione della CRL e quello della sua pubblicazione in nessuna circostanza supera i 60 minuti.

5.9.1.9. Disponibilità dei servizi di verifica on-line della revoca

TeamSystem rende disponibile, in aggiunta alla pubblicazione delle CRL, un servizio di verifica on-line dello stato dei certificati basato sul protocollo OCSP (RFC 6960) (v. allegato A *infra*)
Il servizio OCSP è accessibile 7x24.
In caso di malfunzionamento dei sistemi di verifica dei certificati, TeamSystem si impegna ad assicurare che il servizio rimanga inattivo il minor tempo possibile. In ogni caso il tempo di indisponibilità del servizio di verifica online della revoca non potrà superare le 6 ore.

5.9.1.10. Altre forme disponibili di pubblicazione della revoca

Non è prevista nessuna ulteriore modalità di pubblicazione della revoca a parte di quelle previste nei paragrafi precedenti.

5.9.1.11. Condizioni speciali in caso di compromissione/corruzione della chiave privata

Non previste.

5.9.1.12. Circostanze per la sospensione

La sospensione del certificato di firma elettronica qualificata e del Sigillo elettronico Qualificato è prevista nelle seguenti circostanze:

1. circostanze che influenzano le informazioni contenute nel certificato:
2. sospetta non correttezza dei dati contenuti nella richiesta di certificato;

3. circostanze che influiscono sulla sicurezza della chiave o del certificato:
4. sospetta violazione dei requisiti previsti nelle procedure di gestione dei certificati, stabiliti nel presente Manuale Operativo;
5. sospetto accesso o uso non autorizzato, da parte di terzi, della chiave privata corrispondente alla chiave pubblica contenuta nel certificato;
6. sospetto uso improprio del certificato da parte della persona fisica identificata nel certificato o mancanza di diligenza nella custodia della chiave privata.
7. circostanze che riguardino il Richiedente e/o il Titolare: richiesta esplicita di revoca del certificato da parte del Titolare e/o del suo rappresentante, per qualsiasi motivo, conformemente alle disposizioni della sezione 3.

La sospensione per i certificati di TSU non è prevista in nessun caso.

5.9.1.13. Chi può richiedere la sospensione

Può domandare la sospensione del certificato il Richiedente e i soggetti indicati al Par. 5.9.1.2, attraverso le modalità descritte per la revoca al cap. 5.9.1.3 laddove venga ravvisata detta necessità.

5.9.1.14. Procedura per la sospensione

Ai sensi dell'art. 26 delle Regole Tecniche di cui al DPCM 22 febbraio 2013 la sospensione dei certificati qualificati è effettuata dalla CA mediante l'inserimento del Codice identificativo in una delle liste dei certificati revocati e sospesi (CRL).

Ai sensi del comma 3 dell'art. 26 sopra citato, TeamSystem ha fissato la durata massima del periodo di sospensione dei certificati qualificati in 90 (novanta) giorni; al termine del periodo di sospensione, senza che sia intervenuta indicazione contraria da parte del Titolare, TeamSystem provvederà alla revoca del certificato.

Per la restante parte, la procedura di sospensione si effettua in maniera equivalente a quanto avviene per la revoca, così come descritto nel paragrafo 4.9.1.3.

In ogni caso, la sospensione della validità di un certificato digitale, così come la cessazione della stessa, è annotata, ai sensi dell'art. 26 co. 5 delle Regole Tecniche (DPCM 22 febbraio 2013) nel giornale di controllo con indicazione della data e dell'ora di esecuzione dell'operazione (per maggiori informazioni sulla gestione del giornale di controllo v. par. 5.2. e ss.)

5.9.1.15. Chi può richiedere la riattivazione

Si veda il paragrafo 5.9.1.2.

5.9.1.16. Procuedura per la riattivazione

Se la riattivazione viene richiesta inviando il modulo ai canali email e PEC indicati nei paragrafi precedenti, la richiesta sarà elaborata entro il consueto orario d'ufficio di TeamSystem. Se effettuata tramite il servizio online, avrà effetto immediato.

5.10. Servizi informativi sullo stato del certificato

Lo stato dei certificati qualificati è messo a disposizione attraverso la pubblicazione della CRL mediante protocollo HTTPS ed in formato conforme alla specifica [RFC 5280].
Lo stato dei certificati è inoltre reso disponibile online attraverso un servizio basato sul protocollo OCSP (On-line Certificate Status Protocol) in conformità con la specifica [RFC6960].
Gli indirizzi per l'accesso ai servizi di revoca sono inseriti all'interno dei certificati. L'indirizzo delle CRL è inserito nell'estensione *CRLDistributionPoints*.
L'indirizzo del server OCSP viene inserito nell'estensione *AuthorityInformationAccess*.
I Servizi sono ad accesso pubblico.

5.11. Cessazione del contratto

Il contratto tra la CA e il Titolare si intende cessato alla scadenza o alla revoca del certificato o nelle altre ipotesi previste nelle Condizioni Generali, salvo il caso di eventuali condizioni diverse previste nei contratti stipulati con alcuni clienti.

5.12. Key escrow e recupero della chiave privata

5.12.1.1. Politica e servizi di deposito e recupero delle chiavi

Nell'ambito del servizio di certificazione qui descritto, il "*key escrow*" delle chiavi dei Titolari non è previsto. Non è dunque possibile il recupero della chiave privata del Titolare ("*key recovery*") in nessuna circostanza
Per quanto riguarda le chiavi di CA e di TSA, il recupero è invece previsto in circostanze di emergenza (es: guasto degli apparati HSM). Il ripristino viene condotto seguendo le procedure previste dall'HSM utilizzato.

5.12.1.2. Politica e servizi sui contenuti e recupero chiavi di sessione

Nessuna disposizione

6. MISURE DI SICUREZZA FISICA E OPERATIVA

6.1.1. Sicurezza fisica

TeamSystem ha scelto un Fornitore, il quale ha implementato un sistema di sicurezza relativo al sistema informativo del servizio di certificazione digitale caratterizzato da misure di sicurezza fisica finalizzate alla protezione dell'infrastruttura e dei sistemi di elaborazione utilizzati a supporto dei servizi fiduciari prestati.

In tale contesto, viene assicurato:

- controllo degli accessi fisici;
- protezione contro disastri naturali (es. inondazioni);
- continuità di alimentazione elettrica;
- connettività ad Internet ridondata (doppia linea);
- sistemi antincendio ed antiallagamento;
- protezione antifurto;
- ventilazione e condizionamento ottimali;
- adozione di una politica relativa alla fuoriuscita, non autorizzata, di materiale, informazioni, supporto e ogni ulteriore applicazione relativa a componenti impiegati per i servizi fiduciari e di CA.

Il costante monitoraggio dell'infrastruttura e dei servizi ovvero il tempestivo intervento in caso di necessità è garantito da personale sistemistico qualificato che opera 24h-365 giorni l'anno e assicura assistenza nelle 24 ore che seguono la segnalazione.

Im particolare TeamSystem, per il tramite del Fornitore, si avvale dei servizi di data center e servizi di comunicazione associati (quali *housing*, connettività alla rete Internet, sicurezza fisica) offerti dalla società Adam Data Center BCN – PTV (il "subfornitore") con la quale il Fornitore ha stipulato apposito contratto di servizio.

Detti servizi sono certificati secondo le norme:

- ISO/IEC 27001:2022
- ISO 9001:2015

Il Datacenter è ubicato all'indirizzo: C/ del Artesans, 7 – 08290 Cerdanyola de Vallés, Barcellona (Spagna).

6.1.1.1. Localizzazione e implementazione delle strutture

La protezione delle infrastrutture che consentono l'erogazione dei servizi di certificazione viene assicurata mediante la creazione di perimetri di sicurezza, chiaramente definiti ed individuabili.

Le installazioni sono ubicate in zone a basso rischio di disastri naturali (bassissimo livello di rischio sismico, rischio vulcanico assente, basso rischio di alluvioni).

La qualità e solidità dei materiali di costruzione delle installazioni garantisce livelli di protezione adeguati contro tentativi di intrusione forzate e permette un rapido accesso per eventuali azioni di emergenza.
La sala dove si realizzano le operazioni di crittografia nel Centro di Elaborazione Dati vanta infrastrutture con elevatissimi requisiti tecnologici, così come varie fonti alternative di elettricità e raffreddamento in caso di emergenza.
TeamSystem dispone di strutture che proteggono fisicamente gli ambienti in cui vengono effettuate le operazioni proprie dell'erogazione di servizi fiduciari.

6.1.1.2. Accesso fisico

Il Fornitore ed i subfornitori hanno realizzato un sistema di sicurezza fisica articolato su tre livelli:

- accesso all'edificio dove si trova il CED;
- accesso alla sala;
- accesso al rack

per la protezione dei servizi fiduciari erogati.
L'accesso fisico ai locali dove avvengono i processi di certificazione è protetto attraverso una combinazione di misure fisiche e procedurali.
Tale accesso, in particolare:

- è limitato al personale espressamente autorizzato, con autenticazione all'accesso, registrazione, ripresa video a circuito chiuso e archiviazione;
- si realizza con lettori di badge ed è gestito da un sistema informatico con tracciamento (e relativa generazione di evidenze e log) di ingresso e uscita.

Inoltre, l'accesso al rack dove sono ubicati i moduli crittografici e il "core" dell'infrastruttura avviene esclusivamente previa autorizzazione da parte della Direzione di TeamSystem ovvero del Responsabile della Sicurezza.
TeamSystem identifica i fornitori ai fini dell'erogazione dei suddetti servizi assicurando che i controlli per la sicurezza, le definizioni di servizio e i livelli di erogazione inclusi negli
accordi di erogazione di servizi di terze parti, siano attuati, condotti e mantenuti attivi.

6.1.1.3. Elettricità ed aria condizionata

Le strutture nell'ambito delle quali viene svolto, il servizio di certificazione dispongono di attrezzature per stabilizzare la corrente e di un sistema di alimentazione elettrica supportato da un gruppo elettrogeno.
I locali che accolgono le attrezzature informatiche dispongono di sistemi di controllo della temperatura con aria condizionata.

6.1.1.4. Esposizione all'acqua

I macchinari si trovano in una zona a basso rischio di inondazione.
Le sale dove si trovano le apparecchiature informatiche dispongono di un sistema di rilevamento dell'umidità.

6.1.1.5. Prevenzione e protezione antincendio

Le attrezzature e il materiale hanno un sistema automatico di individuazione e estinzione di incendi.

6.1.1.6. Dispositivi di archiviazione

Solo il personale autorizzato ha accesso ai dispositivi di archiviazione.
Le informazioni di livello superiore sono custodite in una cassaforte fuori le strutture del Centro Elaborazione Dati.

6.1.1.7. Smaltimento dei rifiuti

L'eliminazione dei materiali, cartacei e magnetici, si effettua attraverso meccanismi che garantiscono l'impossibilità di recupero delle informazioni.
Nel caso di materiale magnetico, questo viene fisicamente distrutto o riutilizzato dopo aver provveduto alla cancellazione sicura del contenuto.
In caso di documentazione cartacea, la cancellazione delle informazioni avviene attraverso macchine trita-documenti o cestini che vengono successivamente distrutti sotto stretto controllo.

6.1.1.8. Copia di riserva esterna alle strutture

Per TeamSystem, i Fornitori utilizzano un archivio esterno sicuro per la custodia dei documenti, dispositivi magnetici e elettronici indipendenti dal Centro operativo.

6.1.2. Controlli sulle procedure e sicurezza operativa

TeamSystem garantisce che i suoi sistemi operino in maniera sicura, pertanto ha stabilito e introdotto procedure che stabiliscano in maniera rigorosa la prestazione dei suoi servizi.
Il personale addetto di TeamSystem esegue le procedure amministrative e di gestione in accordo con la politica di sicurezza stabilita da TeamSystem.

6.1.2.1. Ruoli di fiducia

In accordo con le norme vigenti, con gli standard ETSI EN 319 401 e ETSI EN 319 411-1 e con la propria politica sulla sicurezza, TeamSystem ha stabilito i seguenti incarichi o ruoli di fiducia:

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

Inoltre, sono state previste le seguenti ulteriori figure:

Amministratore di sistema: soggetto incaricato di gestire e manutenere il sistema informatico dell'organizzazione e di attenersi alle prescrizioni del Garante per la Protezione dei Dati Personali fornite nel relativo provvedimento oltre ai compiti già affidatogli dal Titolare del Trattamento e sempre e comunque nel pieno rispetto dell'art. 32 del GDPR sulla sicurezza del trattamento dei dati personali;

Operatore di sistema: responsabile della quotidiana operatività del corretto funzionamento dei sistemi preposti all'erogazione dei servizi fiduciari;

Le persone che rivestono i ruoli sopra elencati sono soggette a procedure di controllo e di sicurezza specifiche. La suddivisione dei ruoli, inoltre, secondo criteri definiti nel contesto organizzativo di TeamSystem, costituisce una misura atta a prevenire la commissione di attività fraudolente.

6.1.2.2. Numero di persone per attività

TeamSystem, con il supporto del partner tecnologico, garantisce almeno due persone per realizzare le attività relative alla generazione, al recupero e al back-up della chiave privata dell'Autorità di Certificazione.

6.1.2.3. Identificazione e autenticazione per i diversi ruoli

Le persone assegnate ad ogni ruolo sono identificate dall'auditor interno che si assicurerà che ogni persona effettui le operazioni che le sono state assegnate.

Ogni addetto verifica unicamente le attività relative al proprio ruolo, assicurandosi così che nessuno acceda alle risorse che non gli sono state assegnate.

L'accesso alle risorse avviene a seconda dell'attività attraverso nome utente/codice, certificato digitale, badge e/o chiave. con il supporto del partner tecnologico, garantisce almeno due persone per realizzare le attività relative alla generazione, al recupero e al back-up della chiave privata dell'Autorità di Certificazione.

6.1.2.4. Mansioni che richiedono separazione di compiti

Le seguenti mansioni sono effettuate almeno da due persone:

- i compiti dell'Auditor interno sono incompatibili con quelli relativi all'amministrazione di sistemi e, in generale, con le operazioni correlate all'implementazione dei servizi elettronici fiduciari;

- i compiti relativi all'emissione e revoca di certificati sono incompatibili con quelli concernenti l'amministrazione dei sistemi.

6.1.2.5. Sistema di gestione PKI

Il sistema di PKI si compone dei seguenti moduli:

- componente/modulo di gestione dell'Autorità di Certificazione;
- componente/modulo di gestione dell'Ufficio di Registrazione;
- componente/modulo di gestione delle richieste;
- componente/modulo di gestione delle chiavi (HSM);
- componente/modulo di database;
- componente/modulo di gestione di CRL;
- componente/modulo di gestione dell'Autorità di Validazione.

6.1.3. Sicurezza del personale

6.1.3.1. Qualifica, esperienza ed autorizzazioni richieste

Il personale di TeamSystem, analogamente a quello del proprio Fornitore, è altamente qualificato e/o è stato debitamente formato per effettuare le operazioni che gli sono state assegnate.
Il personale con ruolo di fiducia non ha interessi personali che entrino in conflitto con lo svolgimento del ruolo che gli è stato affidato.
TeamSystem si assicura che il personale addetto alla registrazione sia affidabile per la realizzazione dei compiti di registrazione. Il responsabile della registrazione riceve informazioni per svolgere le mansioni di convalida delle richieste.
In generale TeamSystem solleverà dall'incarico di fiducia un impiegato se a conoscenza dell'esistenza di conflitti di interessi e/o della commissione di un qualsiasi atto illecito avente effetto sullo svolgimento delle sue funzioni.
TeamSystem non assegnerà una mansione confidenziale o di gestione a una persona non ritenuta idonea. Per questo motivo, nei limiti della legislazione vigente, un'indagine preliminare verrà effettuata relativamente ai seguenti aspetti:

- studi, incluso i titoli da allegare;
- lavori effettuati precedentemente all'incarico (fino a cinque anni prima);
- referenze professionali.

6.1.3.2. Procedure di verifica delle informazioni relative al personale

TeamSystem, prima di assumere una persona o consentirgli l'accesso al posto di lavoro, compie accertamenti relativi ai seguenti aspetti:

- referenze sui lavori effettuati negli ultimi anni;
- referenze professionali;
- studi, incluso titoli allegati.

TeamSystem, preliminarmente allo svolgimento di tali accertamenti, fornisce una specifica informativa privacy all'interessato, all'interno della quale rappresenta le modalità e le finalità con cui tratta i dati personali di tali soggetti, nel rispetto della normativa vigente in materia di protezione dei dati personali, di cui al Regolamento Europeo 679/2016 (GDPR) e alla normativa nazionale vigente in materia.

Tutte le verifiche vengono svolte nel rispetto della legislazione vigente.

I motivi che possono indurre a rifiutare il candidato per la copertura di un incarico di fiducia sono i seguenti:

- dichiarazioni false compiute dal candidato nel curriculum vitae;
- referenze professionali molto negative e/o poco affidabili.

6.1.3.3. Requisiti di formazione

TeamSystem forma adeguatamente il personale destinato ad incarichi di fiducia e di gestione, fino al raggiungimento della qualifica da ricoprire, conservando traccia della suddetta formazione.

I programmi di formazione sono rivisti, aggiornati e migliorati periodicamente ed includono almeno i contenuti seguenti:

- principi e meccanismi di sicurezza della gerarchia di certificazione;
- mansioni che deve svolgere la persona;
- politiche e procedimenti di sicurezza di TeamSystem;
- utilizzo e interventi su macchinari e applicazioni installate;
- gestione e risoluzione di incidenti e compromissioni della sicurezza;
- continuità aziendale e procedure di emergenza;
- procedure di gestione e sicurezza in relazione al trattamento dei dati a carattere personale.

6.1.3.4. Requisiti e frequenza dei corsi di aggiornamento

Specialmente quando vengono effettuate modifiche sostanziali alle mansioni relative ai servizi di certificazione, TeamSystem provvede ad aggiornare il proprio personale in maniera accurata e soddisfacente.

6.1.3.5. Rotazione delle mansioni

Non applicabile.

6.1.3.6. Sanzioni per azioni non autorizzate

TeamSystem mette in atto procedure disciplinari nelle ipotesi in cui sia necessario stabilire le responsabilità derivanti da azioni non autorizzate, nei limiti ed in conformità alle norme di diritto del lavoro applicabili.
Proporzionalmente alla gravità dell'azione non autorizzata, le azioni disciplinari includono la sospensione, la separazione dei compiti fino alla risoluzione del rapporto contrattuale di lavoro.

6.1.3.7. Requisiti di assunzione di personale qualificato

Gli impiegati assunti per svolgere incarichi di fiducia firmano in anticipo le clausole sulla riservatezza e i requisiti operativi impiegati da TeamSystem. Qualsiasi azione che comprometta la sicurezza delle procedure accettate potrà, previa valutazione, dar luogo alla risoluzione del contratto di lavoro.
Nel caso in cui tutti o una parte dei servizi di certificazione siano svolti da terzi, costoro saranno tenuti al rispetto dei controlli e delle disposizioni prevista in questa o in altre sezioni del Manuale Operativo. Il riparto di responsabilità tra la CA e tali soggetti viene definito da un apposito accordo tra le Parti.

6.1.3.8. Somministrazione della documentazione al personale

Il Prestatore dei servizi di certificazione somministrerà la documentazione necessaria al proprio personale, affinché quest'ultimo possa adempiere alle proprie attività in maniera competente ed efficace.

6.1.4. Procedure di controllo per la sicurezza

6.1.4.1. Tipi di incidente registrati

TeamSystem produce documenti e salvaguarda informazioni, almeno in merito agli incidenti seguenti, correlati alla sicurezza dell'Autorità di Certificazione:

- avvio e arresto del sistema;
- tentativi di creazione, cancellazione, reimpostazione password o cambio di diritti;
- tentativi di accesso e arresto sessione;
- tentativi di accesso non autorizzato al sistema della CA attraverso la rete;
- tentativi non autorizzati di accesso al sistema di archiviazione;
- accesso fisico ai logs;
- cambio della configurazione del sistema;

- log delle applicazioni della CA e TSA;
- incendio e estinzione dell'applicazione della CA;
- modifiche della CA e/o delle sue chiavi;
- cambio nella creazione di norme relative ai certificati;
- generazione di chiavi proprie;
- creazione e revoca di certificati;
- log sulla distruzione dei dispositivi che contengono chiavi e relativi dati di attivazione;
- eventi legati al ciclo di vita del modulo crittografico, quali rilascio e utilizzo dello stesso;
- la generazione di chiavi e di database di gestione delle chiavi;
- registri di accesso fisico;
- manutenzione e cambi di configurazione del sistema;
- cambio del personale;
- rapporti su compromissioni e discrepanze;
- log sulla distruzione di materiale che contenga informazioni su chiavi, dati di attivazione o informazioni personali;
- rapporti completi sui tentativi di intrusione fisica nelle infrastrutture che supportano l'emissione e gestione dei certificati.

Le voci del Registro includono gli elementi seguenti:

- data e ora;
- numero seriale o sequenza di entrata nei registri automatici (log);
- identità del soggetto che effettua l'accesso.
- tipo di accesso.

6.1.4.2. Frequenza di elaborazione del giornale di controllo

TeamSystem effettua il controllo dei log quando si produce un'allerta del sistema causata da un incidente.

L'elaborazione dei registri di controllo consiste nel riesame degli stessi, finalizzato all'accertamento della non-manipolazione degli stessi, in una breve ispezione di tutti gli accessi registrati e in un'indagine più profonda finalizzata all'analisi di eventi potenzialmente pericolosi.

Le azioni svolte per l'analisi del giornale di controllo sono documentate.

TeamSystem dispone di un sistema che permette di garantire:

- che ci sia spazio sufficiente per la memorizzazione dei log;
- che i log non vengano riscritti;
- che il log registri almeno il tipo di evento, data e ora, utente e risultato dell'operazione.

6.1.4.3. Periodo di conservazione del giornale di controllo

TeamSystem conserva le informazioni del giornale di controllo per un periodo di 20 (venti) anni.

6.1.4.4. Protezione dei registri di verifica

I Log dei sistemi:

- sono protetti da eventuale manipolazione mediante firma digitale;
- sono alloggiati in dispositivi ignifughi.

L'accesso ai log è riservato esclusivamente al personale autorizzato.
Esiste una procedura interna in cui sono dettagliati i processi di gestione dei dispositivi che contengono dati di log di controllo.

6.1.4.5. Procedure di backup

TeamSystem dispone di una procedura adeguata di backup in modo che, in caso di perdita o distruzione di archivi importanti, le rispettive copie di backup dei logs siano disponibili entro un breve periodo di tempo.
TeamSystem ha implementato un sistema di procedura di backup sicuro dei logs di controllo effettuando settimanalmente una copia di tutti i logs in un ambiente esterno. Inoltre une copia è conservata in un centro di custodia esterno.

6.1.4.6. Sistema di memorizzazione del giornale di controllo

L'informazione relativa al giornale di controllo è memorizzata in modo automatico attraverso l'uso di utility sviluppate *ad hoc* dal Fornitore di TeamSystem.
Esclusivamente il personale designato potrà richiedere agli amministratori di sistema il giornale di controllo, che viene firmato e cifrato automaticamente dalle utility suddette. Solo attraverso specifici dispositivi è possibile la decifratura dei log.
Detti dispositivi sono custoditi in maniera sicura in cassaforte e il relativo PIN è a conoscenza esclusiva dell'auditor interno (inoltre si trova anche in una busta chiusa e sigillata nella stessa cassaforte).

6.1.4.7. Notifica in caso di evento sospetto

Nessuna disposizione.

6.1.4.8. Analisi di vulnerabilità

Le analisi di potenziali vulnerabilità dell'infrastruttura di TeamSystem sono soggette alle procedure di controllo implementate dalla stessa.

L'analisi di vulnerabilità deve essere effettuata, esaminata e rivista per effettuare una valutazione degli sviluppi necessari alla risoluzione delle stesse. Tali analisi sono eseguite periodicamente in accordo con la procedura interna prevista a tale scopo. I dati di verifica dei sistemi sono conservati allo scopo di essere utilizzati per eventuali indagini relative a incidenti e per localizzare le vulnerabilità.

6.1.5. Archiviazione delle informazioni

TeamSystem assicura che tutte le informazioni relative ai certificati siano archiviate per un periodo di tempo adeguato e conforme alle norme vigenti.

6.1.5.1. Tipologie di documenti archiviati

I seguenti documenti coinvolti nel ciclo di vita del certificato sono archiviati da TeamSystem:

- tutti i dati di controllo del sistema;
- Log relativi alle richieste di emissione e revoca dei certificati;
- Tutti i certificati emessi o pubblicati:
- CRL emesse:
- Log inerenti lo stato dei certificati;
- informazioni sul ciclo di vita del certificato.

TeamSystem sarà responsabili della corretta archiviazione del materiale sopra indicato.

6.1.5.2. Periodo di archiviazione dei registri

TeamSystem archivia i registri sopra elencati per almeno 20 anni, o per il periodo stabilito dalla legislazione vigente. In particolare, i registri dei certificati revocati saranno accessibili per la consultazione per almeno 20 anni dalla revoca o per il periodo stabilito dalla legislazione in vigore al momento della revoca.

6.1.5.3. Protezione degli archivi

TeamSystem protegge gli archivi in modo tale che solo le persone autorizzate possano accedervi. L'archivio è protetto dalla visualizzazione, la modifica, la cancellazione o qualsiasi altra manipolazione grazie all'implementazione di un sistema affidabile.
TeamSystem garantisce la corretta protezione degli archivi grazie al personale
qualificato che si occupa del trattamento e dell'archiviazione in strutture esterne sicure.

6.1.5.4. Procedure di back-up

TeamSystem dispone di un centro di archiviazione esterno per garantire la disponibilità delle copie dei documenti elettronici. I documenti cartacei sono archiviati in luoghi sicuri con accesso limitato solo al personale autorizzato.

TeamSystem esegue ogni giorno backup incrementali di tutti i dati elettronici e ogni settimana svolge backup completi in caso di recupero dei dati.
Inoltre, TeamSystem (o gli Uffici di Registrazione) conservano una copia dei documenti cartacei in un luogo sicuro e separato dalle strutture dell'Autorità di certificazione.

6.1.5.5. Requisiti della marcatura temporale

I registri sono datati in base ad una fonte affidabile via NTP.
Non è necessario che queste informazioni siano firmate digitalmente.

6.1.5.6. Localizzazione del sistema di archiviazione

TeamSystem dispone di un sistema centralizzato per raccogliere informazioni sull'attività del team coinvolto nel servizio di gestione dei certificati. TeamSystem si avvale di un sistema di conservazione digitale (Archive) che è situato in territorio UE con sito primario a Milano e secondario a Francoforte.

6.1.5.7. Procedure per ottenere e verificare le informazioni di archiviazione

TeamSystem dispone di una procedura che descrive il processo per verificare che le informazioni archiviate siano corrette e accessibili. TeamSystem fornisce le informazioni e i mezzi per la verifica all'auditor.

6.1.6. Rinnovo delle chiavi

Almeno 5 anni prima della scadenza della validità della chiave privata della CA ed almeno dieci anni prima della scadenza dell'ultimo certificato emesso, verrà effettuata da parte di TeamSystem la generazione di una nuova coppia di chiavi di CA.
Il certificato *self-signed* corrispondente a suddetta coppia di chiavi viene trasmesso all'Organismo Nazionale di Supervisione dei Prestatori di Servizi Fiduciari (AgID).
Dopo l'inserimento del nuovo certificato di CA nell'elenco di fiducia (TSL) pubblicato dal precedentemente menzionato Organismo di Supervisione, TeamSystem inizia a firmare i nuovi certificati e le corrispondenti CRL con la nuova chiave di CA.
La vecchia CA e la sua chiave privata saranno utilizzati solo per la firma di CRL.
Il relativo periodo di validità del certificato è quindi determinato in base:

- allo stato tecnologico;
- allo stato dell'arte delle conoscenze crittografiche;
- all'utilizzo previsto per lo stesso certificato;

Ogni sostituzione della chiave privata della CA determinerà una modifica al presente manuale e relativa comunicazione al competente Organismo di Vigilanza (AgID).

6.1.7. Compromissione delle chiavi e disaster recovery

6.1.7.1. Procedure di gestione degli incidenti e delle compromissioni

TeamSystem, ha sviluppato politiche di sicurezza e continuità che consentono di gestire e recuperare i sistemi in caso di incidenti e compromissione delle operazioni, garantendo l'erogazione dei servizi critici per la revoca e la pubblicazione dello stato dei certificati.

6.1.7.2. Corruzione di risorse, applicazioni o dati

In caso di corruzione di risorse, applicazioni o dati, saranno attivate le procedure di gestione appropriate in base alle politiche di sicurezza e di gestione degli incidenti di TeamSystem, che includono escalation, ricerca e risposta alla criticità. Se necessario, verrà avviata la procedura di compromissione della chiave o di *disaster recovery* di TeamSystem.

6.1.7.3. Compromissione della chiave privata della CA

In caso di sospetto o accertamento della compromissione da parte di TeamSystem, verranno attivate le procedure di compromissione delle chiavi in base alle politiche di sicurezza, alla gestione degli incidenti e alla continuità operativa, che consente il recupero dei sistemi critici, se necessario in un centro dati alternativo.

6.1.7.4. Continuità operativa dopo una criticità

TeamSystem adotta tutte le procedure necessarie a garantire la continuità del servizio anche a seguito di situazioni di elevata criticità tramite l'utilizzo di sistemi di riserva.
Il piano si applica al centro di DR designato da TeamSystem, il quale prevede una ridondanza di sistemi sufficiente a soddisfare i requisiti di disponibilità dei sistemi previsti e il ripristino dei servizi di elaborazione sul sito di Disaster Recovery.
TeamSystem ripristinerà i servizi critici (revoca e pubblicazione delle informazioni sullo stato dei certificati) in accordo con il piano di criticità e continuità operativa esistente (conforme allo standard ISO/IEC 27001), garantendo così il funzionamento previsto dei servizi entro i termini previsti dal suddetto piano di continuità.
TeamSystem dispone di un centro di DR, laddove se ne renda necessario la disponibilità per l'implementazione dei sistemi di certificazione descritti nel piano di continuità operativa, situato presso il data center del Fornitore in Napoli alla via Diocleziano n. 107.

6.1.8. Cessazione del servizio

TeamSystem assicura ai Richiedenti e/o Titolari, ai terzi interessati ed alle Relying Parties che le eventuali interruzioni, a seguito della cessazione temporanea dei servizi di certificazione svolti dalla CA, siano minime. In questo modo, TeamSystem garantisce una manutenzione continua dei registri per il tempo stabilito nella sezione 5 del presente Manuale Operativo.

Tuttavia, TeamSystem eseguirà tutte le azioni necessarie per trasferire a terzi o ad un notaio gli obblighi di manutenzione dei registri sopra indicati, per un periodo adeguato, in base alle prescrizioni del presente Manuale Operativo e alle disposizioni normative relative alla prestazione dei servizi fiduciari.

Prima di cessare l'erogazione dei Servizi di Certificazione, TeamSystem ha sviluppato un piano di cessazione dell'attività, con le seguenti disposizioni:

- stanzierà i fondi necessari per dar seguito alle attività di cessazione;
- informerà tutti i Titolari/Richiedenti, le terze parti e le altre CA con cui hanno stipulato accordi o altri tipi di relazioni della cessazione con almeno 60 giorni di anticipo rispetto alla data pianificata di cessazione del servizio;
- revocherà qualsiasi autorizzazione concessa a soggetti terzi per poter agire per conto della CA nella procedura di emissione del certificato;
- trasferirà gli obblighi relativi alla manutenzione delle informazioni dei registri e dei log per il periodo di tempo indicato ai Titolari e agli utenti;
- distruggerà o disabiliterà le chiavi private della CA;
- manterrà i certificati attivi e il sistema di verifica e revoca fino alla scadenza di tutti i certificati emessi;
- eseguirà le attività necessarie per trasferire gli obblighi di manutenzione delle informazioni di registro e degli archivi di registro degli eventi per i rispettivi periodi di tempo indicati al contraente e alle terze parti che utilizzano i certificati;
- comunicherà all'Organismo di vigilanza competente, con almeno 60 (sessanta) giorni di anticipo, la cessazione dell'attività e la destinazione dei certificati specificando se sarà trasferita la gestione e a chi o se il trasferimento non sarà più valido;
- comunicherà all'Organismo di vigilanza competente l'avvio di qualsiasi procedura concorsuale nei confronti di TeamSystem, nonché qualsiasi altra circostanza rilevante che possa impedire il proseguimento dell'attività.

7. MISURE DI SICUREZZA TECNICA

TeamSystem utilizza sistemi e tecniche affidabili atte a garantire la sicurezza tecnica dei processi implementati. Tutte le misure di sicurezza tecnica impiegate da TeamSystem sono conformi ai seguenti standard di riferimento:

- ETSI EN 319 411-1;
- ETSI EN 319 411-2;
- ETSI EN 319 421;

7.1.1. Generazione e installazione della coppia di chiavi

7.1.1.1. Generazione della coppia di chiavi

7.1.1.2. Chiavi della CA

La coppia di chiavi delle CA è generata seguendo una procedura di "*cerimonia di chiavi*" che avviene in un ambiente protetto, all'interno di un perimetro di elevata sicurezza specificatamente destinato a tale scopo.
Le attività svolte durante la "cerimonia" di generazione delle chiavi di certificazione sono registrate, datate e firmate da tutte le persone coinvolte.
Inoltre, l'esecuzione di tali attività avviene in presenza dell'auditor interno ed è documentata in un apposito verbale redatto dal responsabile della sicurezza.
I verbali sono conservati per scopi di controllo e monitoraggio, per un periodo appropriato definito da TeamSystem.
Per la generazione delle chiavi sono stati utilizzati dispositivi HSM conformi FIPS 140-2 livello 3 e Common Criteria EAL4 +.

TEAMSYSTEM Qualified eIDAS CA 2023	**4.096 bits**	**20 anni**
- Certificati di entità finale	2.048 bits	Fino a 3 anni
TEAMSYSTEM Qualified TSA 2023	**4.096 bits**	**20 anni**
Certificati di Time Stamping Unit	2.048 bits	Fino a 8 anni
TEAMSYSTEM Qualified eIDAS CA 2023	**4.096 bits**	**20 anni**
- Certificati di entità finale	2.048 bits	Fino a 3 anni

Nel caso di emissione di un certificato digitale di sottoscrizione "*One-Shot*" la durata del relativo certificato (di entità finale) è differente da quella indicata nella tabella di cui sopra (v. 1.6.1.2. *infra*).

7.1.1.3. Chiavi dei Titolari

Le chiavi dei Titolari sono generate tramite dispositivi hardware sicuri (QSCD – *Qualified Signature Creation Device*), in maniera conforme a quanto indicato nel "*security target*" del dispositivo stesso e attraverso le librerie software fornite dal produttore del dispositivo.
Gli algoritmi e le suite crittografiche utilizzate sono conformi alle specifiche EUCC Guidelines Cryptography v2.
In particolare, le chiavi vengono generate utilizzando l'algoritmo a chiave pubblica RSA, con una lunghezza minima di 3072 bit, in ottemperanza a quanto previsto dall'art. 24, paragrafo 2, lettera e) del Regolamento eIDAS.

7.1.1.4. Chiavi di TSU

Le chiavi di TSU sono generate in un ambiente fisicamente protetto, in conformità con le procedure interne di TeamSystem relative ai sistemi di marcatura temporale.
Il dispositivo utilizzato per la generazione e custodia delle chiavi di TSU è certificato in conformità allo standard di sicurezza FIPS PUB 140-2 Level 3 e Common Criteria EAL 4+.

7.1.1.5. Consegna della chiave privata al Titolare

Nel caso di certificati relativi a chiavi che risiedono su un QSCD (dispositivo qualificato per la creazione della firma), la chiave privata viene generata e archiviata in modo protetto all'interno del suddetto dispositivo qualificato.
Nei certificati presenti in un QSCD remoto, la chiave privata del Titolare viene generata in un HSM remoto, all'interno di una sezione privata destinata al Titolare.
L'accesso alla chiave privata avviene mediante interfacce applicative esposte dal dispositivo ed esclusivamente mediante una procedura di autenticazione sicura.
Le credenziali di accesso alla chiave privata sono inserite dal Titolare e non vengono memorizzate né possono essere dedotte o intercettate dal sistema di generazione e custodia remota.
La chiave privata non viene inviata al Titolare, pertanto non lascia mai l'ambiente di sicurezza che garantisce il controllo esclusivo della chiave privata da parte del Titolare.
Nei certificati emessi su dispositivo fisico (smart card o token), la chiave privata del Titolare è generata e custodita in modo esclusivo all'interno del dispositivo QSCD. La chiave privata non è esportabile dal dispositivo e rimane sotto il controllo esclusivo del Titolare per tutta la durata di validità del certificato.

7.1.1.6. Distruzione della chiave pubblica della CA

Le chiavi pubbliche di TeamSystem sono comunicate a terze parti che utilizzano i certificati, assicurando l'integrità della chiave e autenticandone l'origine, attraverso la pubblicazione sul sito web ufficiale www.teamsystem.com/trust-

services/documentazione e attraverso la pubblicazione sulla Trust-service Status List (TSL) effettuata dall'Organismo di Supervisione Nazionale (AgID).

7.1.1.7. Dimensioni delle chiavi

La lunghezza delle chiavi di CA è di 4.096 bit;
La lunghezza delle chiavi dei Certificati degli utenti finali è di 2.048 bit. La lunghezza delle chiavi dei certificati di TSU è di 2.048 bit.

7.1.1.8. Generazione dei parametri della chiave pubblica

La chiave pubblica delle CA radice, subordinate e dei certificati dei Titolari e di TSU è codificata in conformità con lo standard RFC 5280.

7.1.1.9. Controllo di qualità dei parametri della chiave pubblica

- Lunghezza del Modulo = 4096 bits;
- Algoritmo di generazione delle chiavi: rsagen1;
- Funzioni crittografiche di riepilogo: SHA256.

7.1.1.10. Generazione delle chiavi in applicazioni informatiche o in beni strumentali

Tutte le chiavi si generano con strumenti e procedure, in conformità con quanto indicato nel presente capitolo.

7.1.1.11. Scopo delle chiavi

Le chiavi per i certificati emessi dalle CA sono utilizzate esclusivamente per la firma di certificati e CRL. Le chiavi per i certificati degli utenti finali sono utilizzate esclusivamente per il non ripudio (*content committment*).

7.1.2. Protezione delle chiavi private e sicurezza moduli

7.1.2.1. Standard e sicurezza dei moduli crittografici

In relazione ai moduli che gestiscono le chiavi di TeamSystem, dei contraenti dei certificati di firma elettronica e le chiavi di TSU, è garantito il livello richiesto dagli standard indicati nel paragrafo precedente 6.1. (e sotto paragrafi).
In particolare, le chiavi private della CA sono generate ed utilizzate all'interno di apparati HSM dotati di certificazione FIPS PUB 140-2 a Livello 3 e di certificazione e Common Criteria (ISO 15408) livello EAL4+ superiore.

La chiave privata del Titolare usata per i certificati (di firma o sigillo elettronico) risiede all'interno di un dispositivo crittografico hardware certificato Common Criteria livello EAL4+ o superiore, appropriato per l'uso previsto delle chiavi, in accordo alla Normativa vigente.

7.1.2.2. Controllo da parte di più di una persona (n di m) sulla chiave privata

È richiesto un controllo da parte di più persone per l'attivazione della chiave privata della CA e della TSA.
Nel caso della chiave privata della CA e della TSA di TeamSystem, è richiesta la presenza simultanea di almeno 3 delle 6 persone che hanno partecipato alla corrispondente cerimonia di chiavi. I dispositivi crittografici sono protetti fisicamente come stabilito in questo documento.

7.1.2.3. Ripristino della chiave privata

Non consentito.

7.1.2.4. Backup della chiave privata

TeamSystem effettua una copia di backup delle chiavi private della CA e di TSA che rende possibile il recupero in caso di criticità, perdita o danneggiamento.
Sia la generazione che il recupero della copia richiedono la partecipazione di almeno tre persone.
Questi file di backup in un luogo sicuro, differente da quello in cui si trova la copia operativa.

7.1.2.5. Archivio della chiave privata

Le chiavi private delle CA vengono archiviate per un periodo di **10 (dieci) anni** dopo l'emissione dell'ultimo certificato.
Le predette chiavi private e le relative informazioni saranno archiviate in modo sicuro nei server e nei sistemi della TeamSystem S.A.
TeamSystem S.A. dispone di tutti i requisiti e le necessarie autorizzazioni affinché la gestione delle chiavi private archiviate avvenga nel rispetto dei più elevati standard di sicurezza, facendo in modo che le informazioni siano conservate in archivi ignifughi sicuri e fisicamente isolati dal resto delle infrastrutture e all'interno del centro di custodia.

7.1.2.6. Trasferimento della chiave privata tra moduli crittografici

Le chiavi private vengono generate direttamente nei moduli crittografici di produzione di TeamSystem.
Le operazioni di backup e di ripristino delle chiavi di CA e di TSA vengono condotte secondo quanto specificato nella sezione 6.2 del presente documento.

7.1.2.7. Memorizzazione della chiave privata sul modulo crittografico

Le chiavi private della CA vengono generate nei moduli crittografici HSM, che garantiscono la sicurezza, la confidenzialità e l'impossibilità di esportazione delle chiavi secondo le modalità descritte nella sezione 6 del presente documento.

7.1.2.8. Modalità di attivazione della chiave privata

La chiave privata di TeamSystem viene attivata eseguendo la corrispondente procedura di avvio sicuro del modulo crittografico (così come indicato dal produttore e in accorso al traguardo di sicurezza del dispositivo), da parte delle persone indicate nella sezione 6.

7.1.2.9. Modalità di distruzione della chiave privata

Prima della distruzione delle chiavi di CA e di TSA, i relativi certificati vengono revocati. I dispositivi che contengono parte delle chiavi private di TeamSystem verranno distrutti o riavviati a basso livello. Per l'eliminazione verranno seguite le fasi descritte nel manuale dell'amministratore del dispositivo crittografico.
Infine, le copie di backup saranno distrutte in modo sicuro. Tali operazioni vengono condotte esclusivamente in circostanze che le rendano necessarie, come ad esempio in caso di cessazione del servizio.
In caso di revoca del certificato emesso su dispositivo fisico (smart card o token), ovvero al termine del suo periodo di validità, il Titolare è tenuto a disattivare il dispositivo e a provvedere alla sua distruzione fisica in modo sicuro. La chiave privata contenuta nel dispositivo risulta in ogni caso inaccessibile a seguito della revoca del relativo certificato.

7.1.2.10. Modalità di disattivazione della chiave privata

Non prevista.

7.1.2.11. Classificazione dei moduli crittografici

Vedere il paragrafo 6.1.

7.1.3. Altri aspetti della gestione della coppia di chiavi

7.1.3.1. Archiviazione della chiave pubblica

Secondo quanto stabilito nel capitolo 5 del presente Manuale.

7.1.3.2. Periodi di utilizzo delle chiavi pubbliche e private

I periodi di utilizzo delle chiavi sono quelli determinati dalla durata del certificato, dopodiché non possono continuare ad essere utilizzate.

7.1.4. Dati di attivazione

7.1.4.1. Generazione dei dati di attivazione

I dati di attivazione dei dispositivi che proteggono le chiavi private di CA e di TSA di TeamSystem sono generati in conformità con quanto stabilito nella sezione 6 e con la cerimonia delle chiavi. La creazione e la distribuzione dei suddetti dispositivi è registrata.
Allo stesso modo, TeamSystem genera i dati di attivazione in modo sicuro.

7.1.4.2. Protezione dei dati di attivazione

I dati di attivazione dei dispositivi che proteggono le chiavi private di CA e di TSA sono protetti con PIN, la cui conoscenza è ristretta esclusivamente ai titolari delle carte *dell'Administrative Card Set* dei moduli crittografici utilizzati, così come indicato nel documento di cerimonia della chiave. I dati di attivazione delle chiavi private relative a certificati di firma qualificata sono protetti in fase di emissione in modo tale che il titolare sia l'unico a conoscerle. I titolari sono responsabili della gestione e della protezione in sicurezza dei dati di attivazione privati, prevenendo la loro rivelazione a terzi non autorizzati.

7.1.5. Controlli di sicurezza informatica

TeamSystem utilizza sistemi affidabili per offrire i servizi di certificazione.
TeamSystem effettua controlli e verifiche informatiche al fine di stabilire una gestione delle risorse informatiche in conformità con il livello di sicurezza richiesto per la gestione dei sistemi di certificazione digitale e nello specifico a quanto richiesto dagli standard tecnici ETSI EN 319 411-1 e ETSI EN 319 411-2.
Per quanto riguarda la sicurezza delle informazioni, TeamSystem si avvale dei controlli dello schema di certificazione sui sistemi di gestione delle informazioni conformi ISO 27001.
Le attrezzature utilizzate sono inizialmente configurate secondo i profili di sicurezza appropriati, per quanto concerne gli aspetti di:

- Configurazione di sicurezza del sistema operativo.
- Configurazione di sicurezza delle applicazioni.
- Dimensionamento corretto del sistema.
- Configurazione degli utenti e dei permessi.

- Configurazione dei registri di log.
- Piano di backup e ripristino.
- Configurazione dell'antivirus.
- Requisiti del traffico di rete.

7.1.5.1. Requisiti tecnici specifici per la sicurezza informatica

Ogni server impiegato da TeamSystem include le seguenti funzionalità:

- Controllo dell'accesso ai servizi delle CA subordinate e gestione dei privilegi.
- Imposizione della separazione delle attività per la gestione dei privilegi.
- Identificazione e autenticazione dei ruoli associati alle identità.
- Archivio della cronologia del contraente, delle CA subordinate e dei dati di verifica.
- Verifica degli eventi relativi alla sicurezza.
- Autodiagnostica della sicurezza relativa ai servizi delle CA subordinate.
- Meccanismi di recupero delle chiavi e del sistema delle CA subordinate.

Le suddette funzionalità sono realizzate attraverso una combinazione del sistema operativo, software PKI, protezione fisica e procedure.

7.1.5.2. Valutazione del livello di sicurezza informatica

Le applicazioni delle CA e di registro utilizzate da TeamSystem sono affidabili.

7.1.6. Controlli tecnici del ciclo di vita

7.1.6.1. Controlli di sviluppo dei sistemi

Le applicazioni e i sistemi sono sviluppati, implementati e gestiti secondo gli standard di sviluppo e le procedure interne di *change management* e le applicazioni dispongono di metodi per verificare l'integrità e l'autenticità, nonché per correggere la versione da utilizzare.
I controlli sul ciclo di vita dello sviluppo sono realizzati in conformità con i requisiti di sicurezza contenuti negli standard ETSI EN 319 411-1 e ETSI EN 319 411-2, e sono ulteriormente definiti nelle procedure di qualità ISO 9001 e nelle policy di sicurezza ISO 27001.

7.1.6.2. Controlli di gestione della sicurezza

TeamSystem sviluppa le attività necessarie per la formazione e la consapevolezza dei dipendenti in materia di sicurezza. I materiali utilizzati per la formazione e i documenti che descrivono i processi sono aggiornati dopo esser

stati approvati da un gruppo che si occupa della gestione della sicurezza. Nell'esecuzione di questa funzione viene disposto un piano di formazione annuale.
TeamSystem richiede, tramite apposito contratto, a qualsiasi fornitore esterno coinvolto nella prestazione di servizi qualificati fiduciari le misure di sicurezza equivalenti. Descrizioni dettagliate dei controlli di sicurezza di rete eseguiti sono disponibili come documenti interni.

7.1.7. Controlli di sicurezza della rete

L'accesso ai dispositivi che fanno parte dell'infrastruttura PKI è protetto da firewall che implementano una suddivisione dell'architettura in perimetri di rete ben definiti.
Le comunicazioni tra i differenti elementi dell'architettura avvengono utilizzando protocolli di rete che implementano crittografia (utilizzando i protocolli TSL/SSL) e mediante l'uso di autenticazione a doppio fattore da parte del personale esplicitamente autorizzato. Periodicamente vengono inoltre condotti (da parte di personale qualificato e in grado di garantire un sufficiente livello di indipendenza rispetto all'operatività dei servizi di certificazione) dei Vulnerability Assessment con la finalità di individuare eventuali vulnerabilità.

7.1.8. Controlli ingegneristici dei moduli crittografici

I moduli crittografici vengono sottoposti ai controlli ingegneristici previsti dagli standard indicati nel presente paragrafo.
Gli algoritmi impiegati per la generazione delle chiavi sono comunemente accettati per l'uso della chiave a cui sono destinati.
Tutte le operazioni crittografiche di TeamSystem sono realizzate in moduli con certificazioni FIPS 140-2 livello 3.

7.1.9. Riferimento temporale

TeamSystem utilizza un sistema di sincronizzazione dei sistemi tramite NTP, che accede a due servizi indipendenti:

1. la prima sincronizzazione avviene tramite un servizio basato su antenne e ricevitori GPS che permette un livello di accuratezza STRATUM 1 (con due sistemi in alta disponibilità);
2. la seconda dispone di una sincronizzazione complementare, tramite NTP, con il Real Instituto y Observatorio de la Armada (ROA). Si garantisce in questo modo differenza non superiore al secondo rispetto alla scala di tempo UTC.

7.1.10. Cambiamento di stato di un Dispositivo Sicuro di Creazione di Firma o Sigillo Elettronico (QSCD)

TeamSystem garantisce l'applicazione delle norme per valutare la sicurezza dei prodotti delle tecnologie dell'informazione applicabili alla certificazione dei dispositivi per la creazione di una firma o di un sigillo elettronico qualificato a norma dell'art. 30, co. 3, lett. a) e art. 39 co. 2 del Regolamento eIDAS.

Le norme cui si fa riferimento sono indicate all'art. 1 co. 1 e nel relativo Allegato alla Decisione di Esecuzione (UE) n. 650/2016 della Commissione del 25 aprile 2016.

In particolare, in caso di modifiche dello stato di certificazione dei dispositivi qualificati di creazione di firma o sigillo elettronico (QSCD), TeamSystem procederà come descritto di seguito:

1. TeamSystem dispone di una lista di vari QSCD certificati, così come di una stretta relazione con i fornitori di questi dispositivi, al fine di garantire alternative alla possibile perdita di certificazione dei dispositivi QSCD;
2. in caso di cessazione del periodo di validità o perdita della certificazione, TeamSystem non utilizzerà detti QSCD per l'emissione di nuovi certificati digitali, né in nuove emissioni, né in eventuali possibili revoche.
3. Procederà immediatamente ad utilizzare QSCD con una certificazione valida.
4. Nel caso in cui un dispositivo QSCD dimostri di non esserlo mai stato, per falsificazione o qualsiasi altro tipo di frode, TeamSystem procederà immediatamente a comunicarlo ai suoi clienti e all'organismo regolatore, a revocare i certificati digitali emessi in questi dispositivi e a rimpiazzarli emettendoli in QSCD validi;
5. In ogni caso in cui si manifesti ovvero vi sia chiara evidenza di una compromissione dei dispositivi QSCD, TeamSystem provvederà immediatamente alla revoca di tutti i certificati le cui coppie di chiavi siano state generate mediante il suddetto dispositivo, dandone espressa comunicazione ai titolari e alle eventuali terze parti interessate. Procederà inoltre alla sostituzione del dispositivo interessato con un QSCD valido.

8. PROFILO DEI CERTIFICATI, CRL, OCSP

8.1.1. Profilo dei certificati

I certificati emessi secondo questo Manuale sono conformi alla specifica pubblica RFC 3739, basata sullo standard ITU-T X.509 v3, nonché alla norma europea ETSI EN 319 412 (n. 1, 2, 3, 4 e 5).
Le regole di valorizzazione degli attributi del DN rispettano le norme ETSI EN in relazione ai profili dei certificati per persone fisiche/giuridiche nonché le specifiche contenute nella RFC 5280 e si conformano alle Raccomandazioni di cui alla Determinazione n. 147/2019 emessa dall'AgID.
La documentazione relativa al profilo dei certificati emessi in conformità alla norma europea ETSI EN 319 412 può essere richiesta in qualsiasi momento a TeamSystem.

8.1.1.1. Numero di versione ed estensioni del certificato

La versione del certificato è v3, basata sullo standard ITU-T X.509.
Le estensioni caratterizzanti i certificati emessi secondo questo Manuale sono indicate, nel dettaglio, all'interno della documentazione relativa a ciascun profilo di certificato, disponibile sul sito web di TeamSystem https://www.teamsystem.com/trust-services/documentazione.

8.1.1.2. Identificatori degli algoritmi

Tutti i certificati emessi secondo questo Manuale sono firmati con algoritmo *sha256WithRSAEncryption*, identificato dall'OID 1.2.840.113549.1.1.11.
La chiave pubblica è contraddistinta da algoritmo *rsaEncryption*, identificato dall'OID 1.2.840.113549.1.1.1.

8.1.1.3. Forme dei nomi

Il campo *Subject* del certificato contiene un *Distinguished Name* (DN) conforme allo standard ITU-T X.500 e alla norma ETSI EN 319 412.
Il DN è composto da attributi definiti nella specifica pubblica RFC 5280.

8.1.1.4. OID (Object Identifier)

Come previsto nel par. 2.4., ciascun profilo di certificato, emesso secondo questo Manuale, è identificato da uno specifico OID (*Object Identifier*).

8.1.2. Profilo delle CRL

Le CR emesse da TeamSystem sono conformi alla specifica pubblica RFC 5280.

8.1.2.1. Numero di versione

Nel campo Versione della CRL è indicato il valore 2, come richiesto nella specifica di cui al par. precedente.

8.1.3. Profilo OCSP

Il servizio OCSP erogato da TeamSystem è conforme alla specifica pubblica RFC 6960.

9. AUDIT DI CONFORMITÀ

TeamSystem, in qualità di prestatore di Servizi Fiduciari è soggetta a verifiche di conformità.

9.1.1. Frequenza degli audit

Con frequenza annuale, un Organismo di Valutazione accreditato (Conformity Assessment Body, CAB) provvede a verificare la conformità dei servizi CA di TeamSystem al presente Manuale, al Regolamento (UE) n. 910/2014 e agli standard ETSI applicabili.
Sempre su base annuale, relativamente ai servizi di certificazione digitale, TeamSystem dispone e svolge un'attività di auditing interno.
Le verifiche di conformità interne, inoltre, possono aver luogo in qualsiasi momento, qualora si sospetti il verificarsi di una qualsiasi violazione di misure di sicurezza.

9.1.2. Identità e qualificazione degli auditor

Gli audit di conformità, nel rispetto di quanto dettato dalla norma ETSI EN 319 403, sono svolti esclusivamente da personale altamente qualificato, specializzato nella conduzione di audit relativi a servizi fiduciari, e competente in materia, dipendente da un Organismo di Valutazione (CAB) accreditato in conformità al Regolamento (CE) n. 765/2008.

9.1.3. Relazione tra la CA e gli auditor

Tra l'Organismo di Valutazione (CAB) e TeamSystem non intercorre alcun rapporto che possa compromettere la genuinità delle verifiche di conformità ovvero determinare un conflitto d'interessi idoneo a distorcere le attività di auditing realizzate dal primo nei confronti di TeamSystem.

9.1.4. Elementi soggetti a verifica

Le attività di auditing riguardano, più nel dettaglio, i seguenti aspetti:

a. la conformità dei servizi di certificazione digitale resi da TeamSystem al presente Manuale nonché alla ulteriore documentazione applicabile al servizio di CA (per es. procedure operative interne);
b. l'implementazione delle previste misure di sicurezza fisica, tecnica ed operativa nonché quelle relative alla sicurezza del personale;
c. la conformità del presente Manuale e degli altri documenti applicabili al servizio di CA alla normativa vigente;
d. la predisposizione di un sistema informativo e di gestione che garantisca la qualità del servizio fornito;

e. il corretto svolgimento, da parte della CA, delle attività che concernono i servizi di certificazione digitale (es.: identificazione ed autenticazione dei soggetti che richiedono i certificati; gestione della relativa documentazione; gestione delle chiavi).

In sintesi, potranno costituire oggetto delle verifiche di conformità i seguenti elementi:

a. procedure operative della CA;
b. sistemi informatici della CA;
c. misure atte alla protezione del centro di elaborazione dati;
d. documentazione inerente ai servizi di CA.

Oggetto di verifica, in accordo alla normativa di settore applicabile e allo standard ETSI EN 319 401 (REQ-7.13-03), è anche l'accessibilità dei servizi fiduciari da parte di persone con disabilità.

9.1.5. Azioni successive alle non-conformità

Ricevuto il report, la Direzione Aziendale provvede ad esaminare, con la collaborazione del CAB le eventuali non-conformità riscontrate durante gli audit.

A seconda della natura e della severità della non-conformità evidenziata, la Direzione Aziendale definisce il piano di azioni conseguenti e dispone l'adozione delle misure correttive necessarie, anche tenendo conto delle procedure interne relative alla gestione delle non-conformità.

Nelle ipotesi in cui le misure definite si rivelino non adeguate a correggere le carenze riscontrate ovvero nei casi in cui tali carenze rappresentino una minaccia a pregiudizio della sicurezza ed integrità dei servizi di certificazione digitale, la Direzione aziendale, potrà provvedere a:

- cessare temporaneamente, e in via transitoria, le operazioni in corso;
- revocare la chiave di CA e rigenerare l'infrastruttura;
- cessare il servizio di CA;
- adottare ogni ulteriore misura necessaria.

9.1.6. Comunicazione dei risultati

Il CAB comunica il risultato dell'attività di auditing alla Direzione Aziendale di TeamSystem.

Il report prodotto dal CAB, inoltre, viene trasmesso all'AgID.

10. CONDIZIONI ECONOMICHE E LEGALI

10.1.1. Tariffe

10.1.1.1. Tariffe per l'emissione o rinnovo del certificato

I servizi di certificazione di TeamSystem sono forniti principalmente nei confronti della clientela dei professionisti ed aziende anche attraverso i gestionali messi a disposizione nei vari settori nei quali opera. I costi per l'emissione del certificato sono sostenuti dal Cliente diretto di TeamSystem e non dal Titolare, in base a tariffe definite dal contratto di servizi tra il Cliente stesso.

In ogni caso TeamSystem si riserva di stabilire tariffe specifiche per l'emissione e il rinnovo dei certificati richiesti dagli utenti.

Tuttavia, TeamSystem si riserva la facoltà di modificare le tariffe per i servizi di certificazione erogati senza obbligo di previa notifica agli utenti e di rinegoziare le condizioni economiche con i singoli clienti in ragione del volume richiesto.

10.1.1.2. Tariffa per l'accesso ai certificati

L'accesso al pubblico registro dei certificati pubblicati è libero e gratuito: per tale motivo TeamSystem non ha stabilito alcuna tariffa economica per l'accesso alla lista di tali certificati.

10.1.1.3. Tariffa per l'accesso alle informazioni di stato dei certificati

TeamSystem non ha stabilito alcuna tariffa economica per l'accesso ai servizi informativi (CRL, OCSP) sullo stato dei certificati. Tale accesso è libero e gratuito.

10.1.1.4. Tariffa per altri servizi

Nessuna condizione.

10.1.1.5. Politica per il rimborso – Recesso

Ai sensi e per gli effetti degli artt. 49 e ss. del D.lgs. 6 settembre 2005 n. 206 e s.m.i. (Codice del Consumo) il Richiedente - consumatore ha diritto di recedere dal contratto, anche senza indicarne le ragioni, entro il termine di 14 (quattordici) giorni decorrenti dalla data della sua conclusione e di ottenere il relativo rimborso.

Il diritto di recesso può essere esercitato unicamente da Richiedenti che, nella stipulazione del contratto, hanno agito per scopi estranei all'attività imprenditoriale (e, dunque, da coloro che sono qualificabili come consumatori ai sensi dell'art. 3 co. 1 lett. a) del Codice del Consumo).

Per poter esercitare il diritto di recesso il Richiedente - consumatore è tenuto ad informare TeamSystem, della sua decisione di recedere dal contratto tramite una dichiarazione esplicita, ai recapiti riportati al sito https://www.teamsystem.com/.

La comunicazione del recesso potrà avvenire tramite:

1) Posta raccomandata con avviso di ricevimento all'indirizzo indicato;
2) messaggio e-mail all'indirizzo di posta elettronica reperibile sul sito sopra indicato.

Il diritto di recesso di cui al presente paragrafo è esercitabile unicamente da parte dei Richiedenti cui non è stato ancora rilasciato il certificato digitale qualificato.

A seguito del rilascio del certificato, il Titolare non potrà esercitare il diritto di recesso in quanto trattasi di prodotto personalizzato ai sensi e per gli effetti dell'art. 59 co. 1 lett. c) del Codice del Consumo, che recepisce in Italia la Direttiva 2011/83/UE del Parlamento Europeo e del Consiglio del 25 ottobre 2011, e per il quale il diritto di recesso è escluso di diritto.

Per ulteriori informazioni si invitano gli utenti a consultare i Termini e le Condizioni Generali del servizio di TeamSystem.

10.1.2. Capacità finanziaria

In relazione alla gestione dei servizi di CA e al piano di cessazione delle attività, TeamSystem garantisce di possedere e poter disporre di sufficienti risorse finanziarie necessarie a garantire l'operatività dei propri servizi, ad assicurare l'adempimento dei propri obblighi e ad affrontare i rischi e le responsabilità eventualmente derivanti dall'erogazione del servizio di certificazione.

10.1.2.1. Copertura assicurativa

In conformità con la normativa richiamata nel paragrafo precedente e per lo svolgimento e l'esecuzione di tutte le attività legate ai servizi di cui al presente Manuale Operativo, TeamSystem ha stipulato polizza assicurativa a copertura di tutti i rischi, con compagnia di primaria importanza in campo assicurativo.

La predetta polizza assicurativa garantisce la copertura per lo svolgimento di tutte le attività di "*servizi di certificazione digitale e/o elettronica, come fornitore di servizi di certificazione che emette certificati qualificati, nonché la sua attività come autorità di registrazione [...]*" ed è posta a copertura di tutti i rischi derivanti dall'erogazione dei servizi di certificazione prevedendo un massimale unico per sinistro e per periodo di assicurazione pari ad €. 1.500.000,00 (unmilionecinquecentomila,00//).

10.1.2.2. Altri asset

Nessuna condizione.

10.1.2.3. Copertura assicurativa per gli utenti finali

Si rinvia al precedente paragrafo 10.1.2.1.

10.1.3. Tutela delle informazioni trattate

10.1.3.1. Informazioni confidenziali

TeamSystem si impegna a trattare e a gestire, qualificandole come confidenziali, tutte le seguenti informazioni:

- richieste di emissione certificati, approvate o negate, nonché tutti i dati personali ottenuti per l'emissione e il mantenimento dei certificati, ad eccezione delle informazioni che devono essere inserite nei certificati o che per altre ragioni, ai sensi del paragrafo seguente, sono da considerarsi non confidenziali;
- chiavi private dei Titolari qualora siano generate e/o memorizzate dalla CA;
- log dei sistemi di elaborazione della CA;
- documenti di controllo, interni ed esterni, creati e/o gestiti dalla CA e dai suoi auditor;
- business continuity e piani di emergenza;
- piani di sicurezza;
- ogni altra informazione identificata come "Confidenziale".

Tutte le informazioni confidenziali sono trattate da TeamSystem nel rispetto delle norme applicabili. Laddove si tratti di dati personali, TeamSystem si impegna a trattarli in conformità al D.lgs. 196/03 e s.m.i. e al Regolamento (UE) 2016/679.

La CA assicura che le informazioni confidenziali siano adeguatamente protette fisicamente e/o logicamente dagli accessi non autorizzati nonché dal rischio di perdita a seguito di disastri (si veda a tal riguardo la sezione apposita).

10.1.3.2. Informazioni non confidenziali

Non sono considerate confidenziali le seguenti informazioni:

- certificati emessi o in corso di emissione;
- periodo di validità del certificato, nonché la data di emissione del certificato e la data di scadenza;
- numero di serie del certificato;
- differenti stati del certificato (ad esempio: in attesa di generazione e/o consegna, valido, revocato, sospeso o scaduto), la data di inizio di ciascuno di essi e il motivo che ha determinato il cambiamento di stato;
- liste dei certificati sospesi o revocati (CRL), nonché le altre informazioni sullo stato di revoca;

- informazioni contenute all'interno del certificato;
- informazioni sui Titolari ottenibili dalla consultazione delle fonti pubbliche;
- informazioni che il Titolare stesso ha chiesto alla CA di rendere pubbliche;
- qualsiasi altra informazione che non rientri nell'ambito di applicazione nel paragrafo precedente.

Tutte le informazioni non confidenziali sono nondimeno trattate da TeamSystem nel rispetto delle norme applicabili. Laddove si tratti di dati personali, TeamSystem si impegna a trattarli in conformità al D.lgs. 196/03 e s.m.i. e al Regolamento (UE) 2016/679.

10.1.3.3. Ipotesi di divulgazione delle informazioni

TeamSystem non divulga le informazioni confidenziali di cui al paragrafo 10.3.1., salvo che tale circostanza non gli sia imposta da un obbligo giuridico/normativo di divulgazione e/o richieste di un'autorità.
I dati personali del Titolare potranno essere comunicati alle forze di polizia, all'autorità giudiziaria, agli organismi di informazione e sicurezza o ad altri soggetti pubblici, ai sensi del D.lgs. 196/2003 e s.m.i. o del Reg. (UE) 679/2016, nel caso in cui ciò sia richiesto per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, nonché all'Autorità che esercita attività di vigilanza sui servizi dei Prestatori Fiduciari Qualificati.
Le circostanze che legittimano la divulgazione, da parte di TeamSystem, delle informazioni confidenziali e, in particolare, dei dati personali dei soggetti richiedenti e/o titolari, sono indicate nell'informativa sul trattamento dei dati personali predisposta e rilasciata dalla CA.

10.1.4. Diritti di proprietà intellettuale

10.1.4.1. Proprietà dei certificati

TeamSystem gode di tutti i diritti di proprietà intellettuale e sfruttamento economico, riconosciuti dalla legge, e/o del diritto d'uso, su tutti i certificati emessi in esecuzione dei rapporti contrattuali con i Richiedenti e applicazione del presente Manuale Operativo.

10.1.4.2. Proprietà del Manuale Operativo – Servizi di Certificazione digitale

Il presente Manuale Operativo è di proprietà di TeamSystem S.p.A.; la traduzione, l'adattamento totale o parziale, la riproduzione con qualsiasi mezzo (comprese le fotocopie) nonché la memorizzazione elettronica sono riservate.

10.1.4.3. Proprietà dei marchi

TeamSystem è titolare di tutti i diritti di proprietà intellettuale e di utilizzazione economica sul marchio "TeamSystem" ai sensi della normativa attualmente vigente.

I Richiedenti garantiscono che l'utilizzo delle informazioni relative alla richiesta del certificato non interferiscono né danneggino i diritti di una qualsiasi terza parte, di qualunque giurisdizione, in merito a marchi, marchi di identificazione di servizio, nomi commerciali, denominazioni societarie e ogni altro diritto di proprietà intellettuale.
I Titolari del certificato e i Terzi interessati del certificato saranno tenuti a manlevare e indennizzare TeamSystem contro qualunque perdita o danno derivanti dall'utilizzo del certificato e delle informazioni in esso contenute per scopi illegali, nell'ambito dei quali sono ricompresi, a titolo esemplificativo e non esaustivo, interferenze illecite su vantaggi contrattuali o potenziali vantaggi aziendali, concorrenza sleale, azioni volte a ledere la reputazione di altra persona, pubblicità ingannevole, e ingenerare confusione su persone fisiche o giuridiche.

10.1.5. Obblighi, Garanzie e responsabilità

10.1.5.1. Garanzie offerte da TeamSystem

TeamSystem si impegna a:

- erogare il servizio di certificazione in conformità alle disposizioni del Manuale Operativo;
- fornire un servizio di revoca e sospensione dei certificati;
- fornire un servizio informativo sullo stato dei certificati;
- fornire informazioni chiare e complete sui requisiti e le condizioni del servizio;
- rendere disponibile una copia di questo Manuale a chiunque ne faccia richiesta;
- trattare i dati personali conformemente alle norme vigenti.

Inoltre:

a) provvede con certezza alla identificazione della persona che fa richiesta della certificazione. Con l'emissione del certificato, TeamSystem attesta e garantisce che i dati identificativi, contenuti nel certificato erano, alla data di emissione del certificato, esatti e veritieri;
b) informa i Richiedenti, prima della sottoscrizione dell'accordo tra quest'ultimo e la CA, in modo completo e trasparente, delle condizioni che regolano la procedura di certificazione;
c) utilizza sistemi di sicurezza affidabili, finalizzati, non solo a garantire che soltanto le persone autorizzate possano compiere inserimenti e modifiche ma anche che l'autenticità delle informazioni sia verificabile;
d) garantisce il corretto funzionamento e la continuità del sistema;
e) si conforma alla normativa di cui al Regolamento (UE) n. 679/2016 e pubblica l'informativa ai sensi dell'art. 13 del citato Regolamento;
f) garantisce che i dati raccolti non vengano utilizzati o elaborati per fini diversi da quelli oggetto del servizio, o comunque per fini non espressamente indicati all'interno dell'informativa di cui al punto precedente.

10.1.5.2. Esclusione di garanzie

TeamSystem non è responsabile e non si assume ulteriori obblighi eccetto quanto espressamente previsto dalla normativa vigente in materia ovvero rispetto a quanto indicato nel presente Manuale o nelle Condizioni Generali di Contratto relative ai servizi di certificazione digitale.

10.1.5.3. Limitazioni di responsabilità

Nei limiti e nel rispetto di quanto indicato nelle Condizioni Generali, TeamSystem è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e successive modifiche ed integrazioni, dalla normativa italiana di settore, ove applicabile, (D.Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale e s.m.i., D.P.C.M. 22 febbraio 2013 e s.m.i., e ulteriori disposizioni normative e regolamentari pertinenti per materia), dal D.Lgs. n. 196/2003 nonché di quelle previste dal Regolamento UE 2016/679.
Salva l'applicazione della normativa su richiamata, le uniche ipotesi di responsabilità in capo a TeamSystem sono circoscritte, esclusivamente, a quelle dettati dal presente Manuale Operativo e dal Contratto relativo ai servizi di certificazione.
Fermo restando quanto indicato nelle Condizioni Generali, in nessun altro caso, per nessun titolo e/o ragione, salvo le ipotesi di dolo e colpa grave, TeamSystem potrà essere ritenuta responsabile nei confronti del Richiedente e/o Titolare, ovvero verso altri soggetti, direttamente o indirettamente, connessi o collegati a questi ultimi, per danni, diretti o indiretti, perdite di dati, violazione di diritti di terzi, ritardi, malfunzionamenti, interruzioni, totali o parziali, che si dovessero verificare a fronte dell'erogazione del Servizio, ove connessi, direttamente o indirettamente, o derivanti da:

- cause di forza maggiore, caso fortuito, eventi catastrofici (a titolo esemplificativo ma non esaustivo: incendi, esplosioni, scioperi, sommosse, ecc.);
- manomissioni o interventi sul Servizio o sulle apparecchiature effettuati dal Titolare e/o dal Richiedente e/o da parte di terzi non autorizzati da TeamSystem.

In particolare, ai sensi dell'art. 13 del Regolamento eIDAS richiamata dalla normativa ETSI EN 319 401 punto 7.1.1., TeamSystem sarà responsabile unicamente per quei danni causati con dolo o negligenza nei confronti di qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi di cui al Regolamento eIDAS, sempre nel rispetto e nei limiti di quanto indicato nelle Condizioni Generali.
Va precisato, tuttavia, che ai sensi dell'art. 13 co. 2 del Regolamento eIDAS è consentito alla CA di provare l'assenza della presunzione di responsabilità a suo carico se dimostra che il danno si è verificato senza suo dolo o negligenza.

10.1.5.4. Obblighi del Certificatore

Il Certificatore TeamSystem è l'ente che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche, abilitato ai sensi della normativa vigente richiamata al cap. 2.3 e con gli ulteriori dettagli richiamati nelle Condizioni Generali del servizio.

10.1.5.5. Obblighi del Titolare

In aggiunta a quanto espressamente stabilito nelle Condizioni Generali del Servizio, il Titolare si impegna a:

a. fornire a TeamSystem informazioni accurate e complete in conformità ai requisiti del presente documento, in particolare per quanto riguarda la registrazione;
b. utilizzare la coppia di chiavi solo in conformità alle limitazioni notificate;
c. non utilizzare, se non autorizzato, la chiave privata del Titolare in caso di sigillo;
d. mantenere la propria chiave privata sotto il proprio controllo esclusivo;
e. notificare a TeamSystem, senza alcun ritardo, il verificarsi di uno dei seguenti eventi fino alla fine del periodo di validità indicato nel certificato:
    i. la chiave privata del soggetto è stata smarrita, rubata o potenzialmente compromessa;
    ii. il controllo sulla chiave privata è stato perso a causa della compromissione dei dati di attivazione (ad es. codice PIN) o per altri motivi;
    iii. inesattezza o modifiche del contenuto del certificato, come notificato al sottoscrittore o al soggetto;
f. interrompere, in seguito alla compromissione della chiave privata, immediatamente e definitivamente l'utilizzo di tale chiave, ad eccezione della decifrazione della stessa; e
g. nel caso in cui si venga informati che il certificato del soggetto è stato revocato o che la CA emittente è stata compromessa, di garantire che la chiave privata non venga più utilizzata dal soggetto.

10.1.5.6. Obblighi delle Relying Party

Tutte le Relying Party, prima di considerare affidabile il certificato si impegnano a:

a. verificare la validità, la sospensione o la revoca del certificato utilizzando le informazioni sullo stato di revoca corrente indicate alla parte facente affidamento;
b. tenere conto di eventuali limitazioni all'uso del certificato indicate sul certificato o nei termini e condizioni forniti; e
c. adottare qualsiasi altra precauzione prescritta negli accordi o altrove.

10.1.5.7. Erogazione del Servizio e Assistenza

Funzionalità del Servizio	Livello di disponibilità	Modalità
Accesso all'archivio dei certificati	24x7	Fino a 3 anni
Sospensione/Revoca/Riattivazione via portale self	24x7	Self
Sospensione/Revoca/Riattivazione via canale mail/PEC	dal lunedì al giovedì dalle 09:00 alle 13:00 e dalle 14:00 alle 18:00 ed il venerdì dalle 09:00 alle 13:00	Servizio di assistenza
Rilascio certificato di firma	24x7	Applicativa
Rilascio certificato di sigillo	dal lunedì al giovedì dalle 09:00 alle 13:00 e dalle 14:00 alle 18:00 ed il venerdì dalle 09:00 alle 13:00	Applicativa

Con riferimento alle modalità di contatto del Centro Assistenza di TeamSystem è possibile inoltrare tutte le richieste attraverso il sistema di ticketing messo a disposizione presso il portale Digital o presso il sito https://www.teamsystem.com/assistenza.

10.1.5.8. Indennizzi a favore di TeamSystem

Fermo quanto previsto dalle Condizioni Generali di Contratto relative ai servizi di certificazione, il Titolare si obbliga a risarcire i danni e le perdite, eventualmente sofferte da TeamSystem, nelle ipotesi seguenti:

a) falsa dichiarazione nella richiesta del certificato (es. falsità dei dati del Richiedente);
b) omissioni relativamente ad atti o fatti essenziali, sia nel caso di negligenza che in caso di omissione intenzionale;
c) custodia fallace dei dati di attivazione (es. PIN) della propria chiave privata;
d) utilizzo di nomi in violazione dei diritti di proprietà intellettuale di altri soggetti.

10.1.5.9. Durata e risoluzione del contratto

Le disposizioni di cui al presente documento trovano applicazione dalla data di conclusione del Contratto come indicato nelle Condizioni Generali e perdurano sino alla scadenza del periodo di validità del certificato emesso dalla CA.

La durata del contratto è comunque subordinata al periodo di validità dei certificati digitali emessi dalla CA: tale circostanza determina, in caso di revoca del certificato, per qualsiasi motivo l'immediata caducazione di tutti gli effetti del Contratto.
Analoga conseguenza deriva dalla risoluzione del Contratto che determina la revoca del certificato da parte della CA emittente.

10.1.5.10.Cessione del contratto

Non è consentito al Richiedente e/o Titolare la cessione di tutto o parte degli obblighi e dei diritti nascenti dal Contratto.

10.1.5.11.Legge applicabile

Il contratto tra la CA e il Richiedente e/o Titolare è soggetto alla Legge Italiana e come tale sarà interpretato ed eseguito. In relazione agli aspetti non espressamente previsti nel Contratto, i servizi di certificazione erogati da TeamSystem sono sottoposti alle norme vigenti.

10.1.5.12.Foro competente

Per tutte le controversie nascenti dal presente Manuale Operativo, dalle Condizioni Generali o da ulteriori eventuali contratti stipulati per la fruizione dei servizi messi a disposizione da TeamSystem, compresi quelle inerenti alla loro esistenza, validità, estinzione, interpretazione, esecuzione e risoluzione sarà, competente in via esclusiva il Foro di Milano, con espressa esclusione di ogni altro Foro concorrente.
Qualora il Richiedente/Titolare sia qualificabile come "consumatore" ai sensi del Codice del Consumo sarà competente il Foro del luogo dove lo stesso ha la propria residenza o domicilio, se ubicati sul territorio dello Stato italiano.
Ai sensi dell'art. 141 sexies del Codice del Consumo, il consumatore può comunque servirsi, su base volontaria, dei metodi di risoluzione extragiudiziale delle controversie previsti dal Codice del Consumo e dalle altre norme di legge applicabili in materia.

10.1.6. Disposizioni finali

10.1.6.1. Modifiche al presente accordo

Il presente Manuale Operativo e le disposizioni in esso contenute sono suscettibili di essere modificate, integrate, sostituite o eliminate dalla predisponente in qualunque momento senza necessità di preavviso nei confronti dell'Utente, salvo il rispetto degli obblighi normativamente previsti in tema di pubblicità.

10.1.6.2. Intero accordo

Il presente Manuale è suscettibile di essere integrato o meno da Condizioni Generali o particolari di contratto sottoscritte specificamente dall'Utente, previo accordo con la CA, e costituisce la disciplina che regola l'utilizzo del certificato da parte del Titolare oltre che regolare i rapporti tra Titolare e CA.
La richiesta del certificato implica l'accettazione integrale e incondizionata delle disposizioni contenute all'interno del presente Manuale.

10.1.6.3. Forza maggiore

TeamSystem non potrà essere ritenuta responsabile della mancata esecuzione delle obbligazioni assunte in forza delle disposizioni di cui al presente Manuale qualora tale mancata esecuzione sia dovuta a cause non imputabili alla stessa, quali - a titolo esemplificativo e non esaustivo - caso fortuito, disfunzioni di ordine tecnico assolutamente imprevedibili e poste al di fuori di ogni controllo, interventi dell'autorità, cause di forza maggiore, calamità naturali, scioperi anche aziendali - ivi compresi quelli presso soggetti di cui le parti si avvalgano nell'esecuzione delle attività connesse al servizio qui descritto - ed altre cause imputabili a terzi.

ALLEGATO A - SISTEMA DI VERIFICA DELLA VALIDITA' DEI CERTIFICATI

Indicazione del Sistema di verifica dei certificati

TeamSystem, in conformità a quanto previsto dall'art. 14 co.1 del D.P.C.M. del 22 febbraio 2013 e dall'art. 32 del Regolamento eIDAS, fornisce ed indica ai soggetti interessati un applicativo che permette la verifica dei certificati (secondo gli standard CAdES, PAdES e XAdES).

In particolare, è messo a disposizione gratuitamente il seguente applicativo on-line, raggiungibile all'indirizzo:

https://vol..com/it

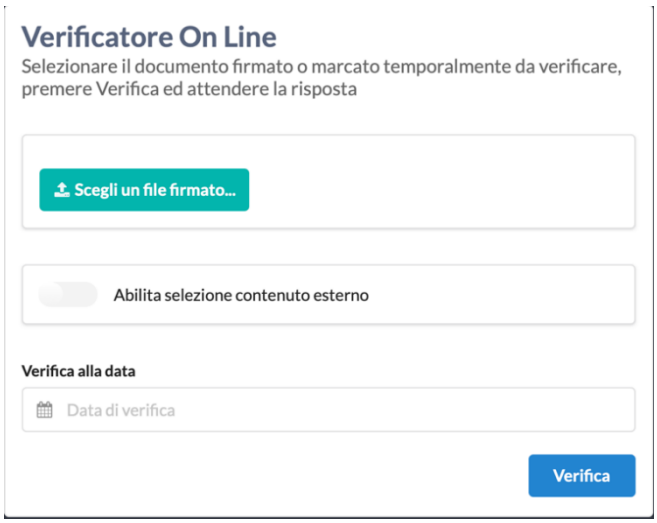
Il predetto software consente, nello specifico, di verificare:

a. l'hash del documento firmato e i dati del soggetto firmatario (persona fisica o giuridica);
b. l'autenticità e l'affidabilità del certificato utilizzato per la firma del documento;
c. eventuali stati di sospensione o revoca dei certificati utilizzati per la firma.

Modalità operative per l'utilizzo dell'applicativo di verifica

Per poter procedere alla verifica dei certificati secondo le modalità che seguono è necessaria la presenza di una connessione ad internet.

Una volta raggiunta la pagina web dell'applicativo al link innanzi indicato l'utente si troverà di fronte la finestra visibile nell'illustrazione che segue:



- Sarà sufficiente, quindi, selezionare la casella "*Scegli un file firmato*" e scegliere, tra i documenti presenti sul computer locale dell'utente, il file da verificare;

- una volta selezionato il file da caricare, l'utente dovrà indicare la data in cui è stato firmato il documento ed infine cliccare sul tasto "*Verifica*" così da verificarne la validità;
- a questo punto, il software restituirà il risultato della verifica tramite visualizzazione di una schermata nel quale saranno indicati tutti i dati necessari alla verifica.
- L'utente, inoltre, potrà scaricare, tramite l'apposito pulsante "*Report PDF*" il *Rapporto di verifica*, ovvero un documento in formato PDF (visualizzabile tramite il programma gratuito Adobe Reader o similari) nel quale è riportato l'esito della procedura di verifica.

L'applicativo, presente all'indirizzo **https://vol.uanataca.com/it**, consente all'utente di effettuare una verifica sui certificati di firma digitale o qualificata il cui risultato è pienamente conforme ai requisiti di cui all'art. 14 co. 2 del D.P.C.M. sopra richiamato.