PKI Disclosure Statement

Informativa per i certificati di firma elettronica e sigillo elettronico qualificati

INDICE

INFORMAZIONI GENERALI

Controllo documentale

Livello di sicurezza:	Pubblico
Ente di Emissione:	TeamSystem S.p.A.
Versione:	1.0
Data ultima edizione:	23/03/2023
Codice Documento:	PKI_Disclosure_Statement_v.1.0_IT

Controllo formale

Redatto da:	Revisionato da:	Approvato da:
Uanataca	Alessandro Capobianco	Simone Braccagni

Controllo delle versioni

Versione	Parti modificate	Descrizione delle modifiche	Data
1.0	Originale	Prima versione del documento	23/3/2023

1. INFORMATIVA

1.1. Introduzione

Il presente documento PKI Disclosure Statement (di seguito anche solo "*Informativa*" o "*Dichiarazione di Trasparenza*"), redatto ai sensi della normativa ETSI EN 319 411-1 fa parte dei termini e delle condizioni contrattuali TeamSystem S.p.A. (di seguito anche solo "*TeamSystem*") che opera in qualità di Fornitore di Servizi Fiduciari Qualificati relativamente alle operazioni di PKI ivi descritte.

L'informativa, redatta in conformità alla "*PDS structure*" di cui alla lett. A2 dell'Annex A contenuto nella norma ETSI sopra richiamata, contiene le informazioni essenziali da conoscere in relazione ai servizi di certificazione di Uanataca.

Per tutti i termini e le definizioni utilizzate all'interno del presente documento è possibile fare riferimento al Manuale Operativo di TeamSystem disponibile al seguente indirizzo https://www.teamsystem.com/trust-services/documentazione, ovvero alle definizioni fornite dalla normativa applicabile in materia.

1.2. Nome del documento e regole di identificazione

Il presente documento è aggiornato alla versione risultante dal "*Controllo delle Versioni*" o dal "*Controllo Documentale*" di cui alle "*Informazioni Generali*" del presente documento TeamSystem assicura una costante verifica e un costante aggiornamento del documento che tenga conto di ogni eventuale e successivo aggiornamento normativo.

TeamSystem, inoltre, si impegna a rendere noto e disponibile il presente documento ai soggetti interessati tramite pubblicazione sul proprio sito web, laddove è sempre possibile consultare l'ultima versione approvata.

1.3. Informazioni di contatto

1.3.1. Organizzazione

Di seguito sono indicati i dati societari di TeamSystem S.p.A. e relativi contatti:

TEAMSYSTEM S.P.A.

Sede legale: Via Sandro Pertini n.88, 61122, Pesaro (PU)

Partita Iva: 01035310414

Telefono: 0721 42661

E-mail: info@teamsystem.com

Sito Web: https://www.teamsystem.com/

1.3.2. Emissione dei certificati

I certificati descritti in questo documento sono erogati da TeamSystem S.p.A., identificata mediante i dati sopra indicati (v.1.3.1. *infra*).

1.3.3. Contatto per le procedure di revoca

Per le richieste di revoca dei certificati, i Titolari e gli interessati possono rivolgersi a TeamSystem tramite comunicazione ad uno dei contatti di seguito indicati (per la revoca si applicano le disposizioni del Manuale Operativo):

TEAMSYSTEM S.P.A.

Telefono: 0721 42661

E-mail: info@teamsystem.com

1.4. Tipologia di certificati

I certificati emessi da TeamSystem sono qualificati in ottemperanza agli artt. 28 e 38 nonché all'Allegato I del Regolamento (UE) 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 (di seguito anche solo "Regolamento eIDAS") e sono conformi a quanto disposto dalla normativa tecnica di riferimento ETSI EN 319 411-1/2 nelle sue ultime versioni approvate. L'*Object Identifier* (OID) che identifica la CA TeamSystem è il seguente:

1.3.6.1.4.1.59699

TeamSystem, inoltre, ha assegnato a ciascun tipo di certificato un *Object identifier* (OID) come di seguito specificato:

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 remoto QSCD

TeamSystem si impegna, per ogni tipologia di certificato qualificato emesso, a rendere disponibile le CRL (*Certificate Revocation List*) per tutto il periodo di validità dei certificati in accordo con il punto 6.3.10 - 02 della ETSI 319 411-2.

1.5. Finalità di certificati

1.5.1. Previsioni comuni

I certificati qualificati descritti in questo documento garantiscono l'identità del firmatario e della persona fisica/giuridica indicata nel certificato, consentendo la generazione della "*firma elettronica qualificata*" e del "*sigillo elettronico qualificato*".
I suddetti certificati, emessi in QSCD (su Smartcard/Token o HSM – Firma remota), funzionano con dispositivi qualificati di creazione di firma, in accordo con il Regolamento eIDAS e in conformità a quanto disposto dalla normativa tecnica dell'Istituto Europeo per gli Standard nelle Telecomunicazioni EN 319 411-2 già citata.

1.5.2. 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 sia su token (chiavetta USB o Smart Card) che su HSM 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, il quale viene dichiarato nei certificati.
Tali certificati, emessi in QSCD costituiscono certificati qualificati secondo quanto stabilito nell'art. 28 del Regolamento (UE) 910/2014 eIDAS.
Funzionano con dispositivi qualificati di creazione di firma (QSCD), nel rispetto degli articoli 29 e 51 del Regolamento (UE) 910/2014, 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, basata su un certificato qualificato e generata impiegando un dispositivo qualificato, la quale è equiparata, per tutti gli effetti di legge, ad una firma autografa scritta senza che sia necessario la sussistenza di ulteriori requisiti.
Inoltre, il certificato in questione può essere utilizzato per quelle applicazioni che non richiedono una firma elettronica equivalente alla firma scritta, come ad esempio:

a) Firma di posta elettronica sicura;
b) Altre applicazioni di firma elettronica.

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

1.5.3. Certificato qualificato di sottoscrizione "One-Shot"

Si tratta di un certificato qualificato di sottoscrizione emesso su dispositivo HSM (di firma remota) con un periodo di validità più limitato nel tempo, tipicamente non superiore a 60 minuti o come altrimenti concordato con il cliente / terzo interessato e, comunque, con una durata di utilizzo non superiore a 60 minuti decorrenti dall'emissione del certificato. Inoltre, 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 ed accettate dal Titolare in fase di richiesta di emissione del certificato.
In maniera congiunta all'apposizione della firma, viene inserita anche una marca temporale, per garantire un riferimento temporale certo secondo quanto previsto dalla normativa.
È previsto uno specifico limite d'uso, da concordare con il cliente. Per i limiti d'uso si rimanda al paragrafo 4.5.3. del Manuale Operativo.
Per questa tipologia di certificato, non è prevista la revoca o la sospensione. È previsto uno specifico limite d'uso, da concordare con il cliente / Terzo Interessato. Per i limiti d'uso si rimanda al paragrafo dedicato. È previsto uno specifico limite d'uso,

1.5.4. 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, per ciascun documento, la presentazione effettiva a quest'ultimo prima dell'apposizione della firma, chiaramente e senza ambiguità.
Tale procedura, tuttavia, presuppone il consenso "a monte" del Titolare (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, tale 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 deve contenere un'indicazione specifica dell'utilizzo della predetta procedura.
Generalmente tali certificati vengono utilizzati per la sottoscrizione di documenti che necessitano di firma qualificata in ambito di processi automatici (file telematici, dichiarazioni, Registri IVA, LUL, fatture elettroniche, altri doc. da conservare, ecc.). È anche utilizzata al termine dei processi di firma elettronica avanzata (FEA) come strumento tecnico per sigillare la documentazione sottoscritta.

1.5.5. Certificato qualificato di sigillo elettronico in QSCD

Questi certificati sono contrassegnati rispettivamente dai seguenti OID: 1.3.6.1.4.1.59699.4 per l'emissione su Smartcard/Token e da OID 1.3.6.1.4.1.59699.4 per l'emissione su HSM (sigillo remoto).
Tale certificati, emesso in "*Qualified Seal Creation Device*" (di seguito anche solo "*QSealCD*" o anche "QSCD", costituiscono certificati qualificato ai sensi dell'art. 38 del Regolamento (UE) 910/2014 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 (UE) 910/2014, 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, garantisce la piena validità legale e riconducibilità ad una persona giuridica determinata (Titolare) e consente di generare un "*sigillo elettronico qualificato*", il quale è equiparato, a tutti gli effetti di legge, ad una sottoscrizione in forma scritta senza che sia necessaria la sussistenza di ulteriori requisiti.
Il sigillo elettronico qualificato, infatti, gode della presunzione di integrità dei dati e della correttezza delle origini di tali dati, cui è collegato il sigillo elettronico qualificato e fa piena prova circa il rilascio del documento 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).

1.6. Limiti di utilizzo del certificato

1.6.1. Limiti di utilizzo dei Titolari

Il Titolare deve utilizzare il servizio di certificazione dei certificati erogato da TeamSystem esclusivamente in conformità alle disposizioni del Manuale Operativo pubblicato sul sito web

dell'organizzazione al seguente indirizzo www.teamsystem.com/trust-services/documentazione e, comunque, per gli usi autorizzati nel contratto sottoscritto tra TeamSystem e il Titolare.

Per ulteriori informazioni si invita il Titolare a consultare i termini e le condizioni generali di contratto dei servizi di certificazione.

Parimenti, il Titolare si impegna a utilizzare il servizio di certificazione digitale in accordo con le istruzioni, i manuali o i procedimenti forniti da TeamSystem.

Il Titolare deve attenersi a qualsiasi normativa e regolamentazione che possa influire sul suo diritto all'utilizzo degli strumenti crittografici che impiega.

I certificati possono essere utilizzati unicamente per le funzioni e le finalità stabiliti dal Manuale Operativo e dagli eventuali Termini e Condizioni sottoscritti dai Titolari al momento della richiesta del certificato, con espressa esclusione di qualsiasi altro utilizzo.

Ne consegue che i certificati non possono essere utilizzati per firmare certificati di chiave pubblica di nessun tipo, né firmare elenchi di revoca di certificati (CRL).

È fatto salvo il rispetto della normativa applicabile per l'utilizzo dei certificati.

Devono, inoltre, tenersi in conto dei limiti indicati nei diversi campi dei profili dei certificati pubblicato sul sito web dell'organizzazione al seguente indirizzo www.teamsystem.com/trust-services/documentazione.

In caso di utilizzo dei certificati in violazione delle disposizioni contenute all'interno della presente Informativa o in violazione delle disposizioni sopra richiamate, il Titolare sarà tenuto a manlevare TeamSystem da qualsiasi responsabilità dovesse sorgere relativamente all'utilizzo illegittimo dei certificati in conformità alla normativa vigente.

TeamSystem si impegna a conservare per un periodo pari a 20 (venti) anni, in accordo con la normativa applicabile, le seguenti informazioni sui certificati di registrazione:

- le informazioni sui soggetti relative alle procedure di identificazione e registrazione;
- le informazioni sul ciclo di vita dei certificati;
- registri di eventi significativi per fini di sicurezza.

Ulteriori informazioni sulla conservazione sono indicate nei paragrafi successivi e nel Manuale Operativo.

1.6.2. Obblighi dei Richiedenti

I Richiedenti, ovvero coloro che richiedono l'emissione di un certificato qualificato a TeamSystem, sono tenuti a conformarsi alle disposizioni di cui alla presente informativa, al Manuale Operativo, ai Termini e alle Condizioni accettate in fase di conclusione del contratto ed altre eventuali regole stabilite dalla CA, le quali sono messe adeguatamente e pubblicamente a disposizione dei Richiedenti.

1.7. Generazione delle chiavi

Il Richiedente autorizza TeamSystem a gestire in accordo, con i metodi e i procedimenti concordati l'emissione di chiavi private e pubbliche e sollecita a suo nome l'emissione del certificato, in accordo con le proprie politiche di certificazione.

1.8. Richiesta dei certificati

Il Richiedente si impegna a soddisfare i requisiti definiti da TeamSystem per la richiesta di certificati qualificati. Tale richiesta avviene in accordo con la procedura definita da TeamSystem e in conformità con quanto stabilito nel Manuale Operativo/Certification Practice Statement e nella restante documentazione contrattuale di TeamSystem cui espressamente si rinvia per la relativa disciplina.

1.9. Obblighi del Richiedente

Il Richiedente del certificato è responsabile circa la veridicità e la completezza di tutte le informazioni fornite all'atto della richiesta del certificato.
Il Richiedente e il Titolare devono informare immediatamente TeamSystem in merito a:

- qualsiasi inesattezza rilevata nel certificato una volta che sia stato emesso;
- cambiamenti che si verifichino nelle informazioni riportate e/o registrate per l'emissione del certificato;
- perdita, del furto o di qualsiasi altro tipo di perdita di controllo della chiave privata da parte del Titolare.

Inoltre, il Richiedente è tenuto a verificare la data indicata all'interno del certificato.

1.10. Obblighi dei Titolari

1.10.1. Obblighi di custodia

Il Titolare si impegna a conservare con la dovuta premura ed attenzione eventuali dispositivi e/o codici segreti fornitigli da TeamSystem.
In caso di perdita o di furto della chiave privata del certificato o nel caso in cui il Titolare sospetti che la chiave privata abbia perso affidabilità per qualsiasi motivo, tali circostanze devono essere immediatamente notificate all'Autorità di Registrazione di riferimento e/o a TeamSystem.

1.10.2. Obblighi di uso corretto

Il Titolare deve utilizzare i certificati digitali forniti da TeamSystem esclusivamente per gli usi autorizzati nel Manuale Operativo e in qualsiasi altra istruzione, manuale o procedimento

fornito al momento della richiesta di emissione e presente sul sito internet https://www.teamsystem.com/trust-services/documentazione.

Il Titolare deve attenersi a qualsiasi normativa e regolamentazione che possa influire sul suo diritto all'utilizzo degli strumenti crittografici che impiega.

Il Titolare non può impiegare mezzi di controllo, alterazione o decompilazione dei servizi di certificazione digitale erogati.

Il Titolare, inoltre, si impegna:

a) ad attenersi alle suddette disposizioni circa l'utilizzo del certificato;
b) in caso di eventuale compromissione della chiave privata, a interrompere immediatamente e permanentemente il suo utilizzo e procedere alle opportune notifiche riportate in questo documento.

1.11. Obblighi delle Relying Parties

1.11.1. Decisione informata

TeamSystem assicura alle *Relying Parties* (ovvero coloro che fanno affidamento o richiedono la verifica della validità del certificato) l'accesso a tutte le informazioni sufficienti a consentire loro di prendere una decisione informata al momento della verifica di un certificato assicurando, a contempo, la completezza delle informazioni ivi contenute.

Le *Relying Parties* riconoscono che l'uso del Registro e degli elenchi di revoca dei Certificati ("CRL") di TeamSystem sono disciplinati dal Manuale Operativo di TeamSystem e si impegnano ad adempiere ai requisiti tecnici, operativi e di sicurezza descritti nel predetto Manuale.

1.11.2. Requisiti di verifica della firma o del sigillo elettronico

La verifica sarà eseguita normalmente in maniera automatica dal software di verifica e, in ogni caso, in accordo con il Manuale Operativo con i requisiti seguenti:

- l'utilizzo di un *software* o di un applicativo appropriato per la verifica, capace di effettuare le operazioni crittografiche necessarie utilizzando algoritmi e lunghezze di chiavi indicate nel certificato;
- verifica dello stato di revoca dei certificati della catena di "*trust*" con l'informazione fornita al Registro di TeamSystem (con CRL per esempio) per determinare la validità di tutti i certificati della catena di certificati, dal momento che può unicamente considerarsi verificata correttamente una firma elettronica se tutti e ognuno dei certificati della catena sono corretti e sono in vigore;
- verifica tecnica della firma di tutti i certificati della catena prima di accertare il certificato utilizzato dal Titolare.

TeamSystem mette a disposizione delle *Relying Parties*, un applicativo (raggiungibile al seguente indirizzo: https://vol.uanataca.com/it che consente la verifica dei certificati qualificati di firma e sigillo elettronico: tale applicativo e la relativa procedura viene indicata e descritta nell'Allegato A al Manuale Operativo/CPS di TeamSystem.

1.11.3. Attendibilità di un certificato non valido

TeamSystem non potrà, in nessun caso, essere ritenuta responsabile nel caso in cui le *Relying Parties* considereranno attendibile un certificato non valido; in tale evenienza, infatti, queste ultime si assumeranno tutti i rischi derivati da tale comportamento.

1.11.4. Effetto della verifica

In virtù della corretta verifica dei certificati in conformità con questa informativa, le *Relying Parties* possono avere certezza dell'identificazione e, in tal caso, della paternità della chiave pubblica del Titolare entro i limiti d'uso corrispondenti.

1.11.5. Utilizzo corretto e attività proibite

Le *Relying Parties* si impegnano a non utilizzare alcuna informazione relativa ai certificati o di nessun altro tipo che sia stata fornita da TemSystem nella realizzazione di transazioni vietate per legge.

I servizi di certificazione digitale erogati da TeamSystem non sono stati progettati né permettono l'utilizzo o la rivendita come apparecchiature di controllo per situazioni pericolose non autorizzate o per usi che richiedano azioni soggette a errore, quali le operazioni di installazioni nucleari, sistemi di navigazione, comunicazione aerea o sistemi di controllo degli armamenti, ove un errore possa causare la morte, danni fisici o danni ambientali gravi.

1.11.6. Clausola d'indennità

Il terzo che verifica la validità del certificato s'impegna a mantenere indenne TeamSystem da tutti i danni provenienti da qualunque azione o omissione che si concretizzi nella responsabilità, nel danno, nella perdita o in un costo di qualunque tipo, compresi quelli legali e di assistenza legale nella quale possano incorrere, per la pubblicazione e l'uso del certificato, quando concorra una delle cause seguenti:

- inadempimento degli obblighi da parte del terzo che accerta il certificato;
- autorizzazione imprudente di un certificato a seconda delle circostanze;
- mancato accertamento dello stato di un certificato per determinare che non sia stato sospeso o revocato;
- mancato accertamento della totalità delle misure assicurative prescritte nel Manuale Operativo.

1.12. Obblighi di TeamSystem S.P.A.

1.12.1. Fornitura dei servizi di certificazione digitale

TeamSystem si impegna a:

a. emettere, consegnare, gestire, sospendere, riattivare, revocare e rinnovare i certificati in accordo con le istruzioni fornite dal Richiedente e/o dal Titolare nei casi e per i motivi descritti nel Manuale Operativo di TeamSystem;
b. eseguire i servizi con i mezzi tecnici e materiali adeguati e con personale che rispetti le condizioni di qualifica e d'esperienza stabilite nel Manuale Operativo;
c. rispettare i livelli di qualità del servizio, in conformità con quanto stabilito nel Manuale Operativo per quanto riguarda gli aspetti tecnici, operativi e di sicurezza;
d. notificare al Richiedente e al Titolare, anteriormente alla data di scadenza dei certificati, la possibilità di rinnovarli, così come la sospensione, la proroga della sospensione o la revoca dei certificati, qualora si manifestino le suddette circostanze;
e. comunicare ai terzi che ne facciano richiesta lo stato dei certificati in accordo con quanto stabilito nel Manuale Operativo per i diversi servizi di verifica dei certificati.

1.12.2. In relazione alle verifiche del registro

TeamSystem emetterà i certificati in base ai dati e alle informazioni fornite dai Richiedenti: a tal fine ha adottato una rigida procedura di identificazione dei Richiedenti, in conformità alla normativa vigente, accuratamente descritta nel Manuale Operativo, con la quale effettuerà le verifiche che ritenga opportune per l'accertamento dell'identità e delle altre informazioni personali e complementari dei sottoscrittori e dei firmatari.

Tali verifiche potranno includere qualsiasi altro documento e informazione rilevante fornita dal Richiedente e/o dal firmatario.

Nel caso in cui TeamSystem riscontri errori nei dati che si devono includere nei certificati, prima di emettere il certificato o sospendere il processo di emissione potrà realizzare le modifiche che consideri necessarie solo dopo aver gestito il caso con il Richiedente.

TeamSystem si riserva il diritto di non emettere il certificato qualora consideri che la giustificazione documentale sia insufficiente per la corretta identificazione e autenticazione del Richiedente e/o del firmatario.

Gli obblighi precedenti sono sospesi nei casi nei quali il Richiedente agisca come autorità di registrazione e disponga degli elementi tecnici inerenti alla generazione delle chiavi, all'emissione dei certificati e alla registrazione dei dispositivi di firma aziendale.

1.12.3. Periodo di conservazione

TeamSystem archivia le registrazioni corrispondenti alle richieste di emissione e di revoca dei certificati per almeno 20 anni.
TeamSystem conserverà le informazioni dei logs per un periodo compreso tra 1 e 20 anni in funzione del tipo di informazione registrata in accordo a quanto previsto dalle sue politiche e procedimenti.
Per ulteriori informazioni sui periodi di conservazione si invita a consultare il Manuale Operativo.

1.13. Garanzia

1.13.1. Garanzia di TeamSystem S.p.A.per i servizi di certificazione digitale

TeamSystem garantisce al Titolare:

a. che non ci siano errori di fatto nelle informazioni contenute nei certificati noti o realizzati dall'Autorità di Certificazione;
b. che non ci siano errori di fatto nelle informazioni contenute nei certificati dovute a mancanza della dovuta diligenza nella gestione della richiesta del certificato o nella creazione dello stesso;
c. che i certificati rispettino tutti i requisiti materiali stabiliti nel Manuale Operativo;
d. che i servizi di revoca rispettino tutti i requisiti materiali stabiliti nel Manuale Operativo.

TeamSystem garantisce al terzo che accerta il certificato:

a. che le informazioni contenute o incluse come riferimento nel certificato siano corrette, tranne quando sia indicato il contrario;
b. in caso di certificati pubblicati nel deposito, che il certificato sia stato emesso al Richiedente e al firmatario identificato nello stesso e che il certificato sia stato accettato;
c. che nell'approvazione della richiesta di certificato e nell'emissione del certificato siano stati rispettati tutti i requisiti materiali stabiliti nel Manuale Operativo;
d. la velocità e la sicurezza nell'erogazione dei servizi, in particolare dei servizi di revoca e deposito.

In aggiunta, TeamSystem garantisce al Richiedente e al terzo che accerta il certificato:

- che il certificato qualificato per la firma o per il sigillo contenga le informazioni che debba contenere un certificato qualificato, in accordo con quanto stabilito negli artt. 28 e 38 del Regolamento (UE) 910/2014 e in conformità a quanto disposto dalla normativa tecnica identificata con il riferimento ETSI EN 319 411-2;

- che, nel caso in cui si generi la chiave privata del Richiedente o, all'occorrenza, della persona fisica identificata nel certificato, se ne mantenga la confidenzialità durante il processo;
- la responsabilità dell'Autorità di Certificazione, con i limiti che vengano stabiliti.

In nessun caso TeamSystem risponderà per caso fortuito o per forza maggiore.

1.14. Esclusioni della garanzia

TeamSystem rigetta tutte le altre garanzie diverse alla precedente che non siano legalmente esigibili.
In particolare, TeamSystem non garantirà alcun software utilizzato da qualsivoglia persona per firmare, verificare le firma, cifrare, decifrare o utilizzare in altra forma alcun certificato digitale emesso da TeamSystem, tranne nei casi in cui esista una dichiarazione scritta in senso contrario.

2. ACCORDI APPLICABILI AL MANUALE OPERATIVO

2.1. Accordi applicabili

Gli accordi applicabili ai certificati sono i seguenti:

- Condizioni generali di contratto per i servizi di certificazione digitale disciplinanti il rapporto tra TeamSystem e il Richiedente/Titolare dei certificati disponibile al seguente indirizzo https://www.teamsystem.com/trust-services/documentazione;
- Condizioni generali del servizio ed informative incluse in questo documento;
- Manuale Operativo che disciplina la fornitura dei servizi di certificazione (v. par. 2.2. *infra*);
- eventuali ulteriori Moduli e/o documentazione contrattuale espressamente richiamati dai documenti di cui sopra.

2.2. Manuale Operativo (CPS)

I servizi fiduciari di TeamSystem sono regolati tecnicamente e operativamente dal Manuale Operativo per i servizi di certificazione, dagli aggiornamenti successivi così come dalla documentazione complementare.

La documentazione è modificata periodicamente e può essere consultata al sito internet https://www.teamsystem.com/trust-services/documentazione.

2.3. Politica sulla privacy

TeamSystem, con riferimento al trattamento dei dati personali, si conforma alla normativa vigente in materia, sia nazionale che comunitaria, con particolare riferimento al D.lgs. 196/03, e s.m.i., ed il Regolamento (UE) 2016/679 (di seguito anche solo "GDPR").

TeamSystem non può divulgare né può essere obbligata a divulgare informazioni confidenziali a meno di una richiesta specifica proveniente da:

a) dall'interessato, ovvero la persona rispetto alla quale TeamSystem ha l'obbligo di mantenere le informazioni confidenziali, o
b) un mandato giudiziario, amministrativo o di qualsiasi altro genere previsto dalla legislazione vigente.

TeamSystem, in conformità a quanto disposto dall'art. 13 del GDPR, ha predisposto e reso disponibile una precisa Informativa sul Trattamento dei Dati Personali che descrive i trattamenti effettuati da TeamSystem, in qualità di Titolare del Trattamento, relativamente all'erogazione dei servizi fiduciari.

L'Informativa in formato esteso è disponibile all'interno del Manuale Operativo di TeamSystem nonché sul sito internet all'indirizzo: https://www.teamsystem.com/trust-services/documentazione.

2.4. Politica di rimborso

Per la Politica di rimborso è necessario fare riferimento alla relativa sezione all'interno del Manuale Operativo di TeamSystem.

2.5. Normativa applicabile e Foro competente

Le relazioni con TeamSystem sono disciplinate esclusivamente dalla normativa italiana.
In caso di disaccordo tra le parti, queste tenteranno la conciliazione amichevole. A tal fine le parti dovranno indirizzare una comunicazione a TeamSystem tramite uno dei contatti indicati nel presente documento.
Per il Foro competente si rinvia al Manuale Operativo di TeamSystem che qui abbia a intendersi come integralmente richiamato e trascritto.

2.6. Elenco dei Prestatori di servizi fiduciari

Di seguito si riporta il link attraverso il quale è possibile consultare la lista dei prestatori di servizi fiduciari attivi in Italia: https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia

2.7. Disposizioni finali, accordo integrale e notifiche

Le clausole della presente informativa sono indipendenti tra di loro, ragione per la quale se qualsivoglia clausola è considerata invalida o inapplicabile le restanti clausole del Manuale Operativo continueranno a essere applicabili.
I requisiti contenuti nelle sezioni 9.6 (Obblighi, Garanzie e responsabilità), 8 (Audit di conformità) e 9.3 (Tutela delle informazioni trattate) di cui al Manuale Operativo di TeamSystem resteranno in vigore anche dopo la cessazione del servizio.
Questo testo esprime la volontà completa e tutti gli accordi tra le parti.
Le notifiche tra le parti avvengono tramite l'invio di mail all'indirizzo indicato dal Titolare nel contratto con TeamSystem.