PKI DISCLOSURE STATEMENT

(PDS)

INFORMATIVA PER I CERTIFICATI DI FIRMA ELETTRONICA E SIGILLO ELETTRONICO QUALIFICATI

Indice

INFORMAZIONI GENERALI

CONTROLLO DOCUMENTALE

Classificazione di sicurezza:	Pubblico
Versione:	1.1
Data di edizione:	30/03/2020
File:	PKI_Disclosure_Statement_v.1.1_IT

CLASSIFICAZIONE FORMALE

Preparato da:	Rivisto da:	Approvato da:
Legal & Compliance - Luca Santalucia - Margherita Mirabella	Area Servizi *Legal & Compliance*	Direzione

CONTROLLO DELLE VERSIONI

Versione	Parti modificate	Descrizione modifica	Data
1.0	Originale	Creazione del documento	31/03/2020
1.1	Struttura e formattazione del documento /Capitolo 1	- Capitolo 1: inserimento riferimenti normativi: - Inserimento nuovo logo; - Adeguamento formattazione per uniformità documentale;	01/12/2020

1. INFORMATIVA APPLICABILE AI CERTIFICATI DI FIRMA E SIGILLO ELETTRONICO

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 è parte dei termini e delle condizioni della CA Uanataca 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 al servizio di certificazione del Prestatore di Servizi Fiduciari Uanataca S.A. unipersonale (di seguito anche solo "Uanataca").

Per tutti i termini e le definizioni utilizzate all'interno del presente documento è possibile fare riferimento al Manuale Operativo di Uanataca ovvero alle definizioni fornite dalla normativa applicabile in materia.

1.1. Informazioni di contatto

1.1.1. Organizzazione e relativi contatti

UANATACA S.A. (SOCIEDAD ANONIMA UNIPERSONAL)

CALLE RIERA DE CAN TODÀ 24-26 - BARCELLONA

VIA DIOCLEZIANO N. 107, 80125 - NAPOLI

VAT NUMBER (ES): A66721499

PARTITA IVA (IT): 09156101215

PHONE: +34 935 272 290, +39 081 7625600

EMAIL: info.it@uanataca.com

Sito Web: https://web.uanataca.com/it/

1.1.2. Prestatore dei servizi fiduciari elettronici di emissione

I certificati descritti in questo documento sono erogati da Uanataca S.A., identificata mediante i dati sopra indicati.

1.1.3. Contatto per le procedure di revoca

Per le richieste di revoca dei certificati gli interessati possono rivolgersi a Uanataca tramite uno dei contatti di seguito indicati:

UANATACA S.A.
TELEFONO: +34 935/272-290, +39 081/7625600
EMAIL: info.it@uanataca.com

1.2. Tipologia di certificati

I certificati emessi da Uanataca 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.

Uanataca ha assegnato a ciascun tipo di certificato un *object identifier* (OID), per la sua identificazione nelle applicazioni:

Numero OID	Tipologia di certificato
1.3.6.1.4.1.47286.10.1.1	*Certificato qualificato di sottoscrizione in QSCD rilasciato a persone fisiche – Firma elettronica*
1.3.6.1.4.1.47286.10.1.10	*Certificato qualificato di sottoscrizione in QSCD rilasciato a persone giuridiche – Sigillo elettronico*

Uanataca 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.

1.3. Finalità dei certificati

1.3.1. 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, 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.

1.3.2. Certificato qualificato di firma di persona fisica in QSCD

Questo certificato dispone dell'*OID* 1.3.6.1.4.1.47286.10.1.1.

È un certificato qualificato emesso per la firma elettronica qualificata in accordo con la politica di certificazione *QCP-n-qscd* con l'*OID* 0.4.0.194112.1.2, dichiarato all'interno del certificato.

Tale certificato, emesso in QSCD, è un certificato qualificato in accordo con quanto previsto nell'articolo 28 del Regolamento (UE) 910/2014 eIDAS.

È possibile, inoltre, l'utilizzo in applicazioni diverse della firma elettronica qualificata, come:

a) firma di posta elettronica sicura;

b) altre applicazioni di firma elettronica.

Il campo "*key usage*" attiva esclusivamente la funzione di *Content Commitmen*t.

1.3.3. Certificato qualificato di sigillo di persona giuridica in QSCD

Questo certificato dispone dell'*OID* 1.3.6.1.4.1.47286.10.1.10.

È un certificato qualificato emesso per il sigillo elettronico qualificata in accordo con la politica di certificazione *QCP-n-qscd* con l'*OID* 0.4.0.194112.1.3., dichiarato all'interno del certificato.

Tale certificato, emesso in QSCD, è un certificato qualificato in accordo con quanto previsto nell'articolo 38 del Regolamento (UE) 910/2014 eIDAS.

Il campo "*key usage*" attiva esclusivamente la funzione di *Content Commitment*.

1.4. Limiti di utilizzo del certificato

1.4.1. Limiti di utilizzo indirizzati ai firmatari

Il firmatario deve utilizzare il servizio di certificazione dei certificati erogato da Uanataca esclusivamente in conformità alle disposizioni del Manuale Operativo pubblicato sul sito web dell'organizzazione e, comunque, per gli usi autorizzati nel contratto sottoscritto tra Uanataca e il firmatario, enunciati al capo 2.6: "*Obblighi dei firmatari*".

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

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

1.4.2. Limiti di utilizzo indirizzati ai verificatori

I certificati possono essere utilizzati unicamente per le funzioni e le finalità stabiliti dal Manuale Operativo e dagli eventuali Termini e Condizioni sottoscritti dai clienti al momento della richiesta del certificato senza 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 visibili sul sito web di Uanataca (https://web.uanataca.com/it/).

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

Uanataca 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.

1.5. Obblighi dei Richiedenti

I Richiedenti, ovvero coloro che richiedono l'emissione di un certificato qualificato a Uanataca, 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.

1.5.1. Generazione delle chiavi

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

1.5.2. Richiesta dei certificati

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

1.5.3. Obblighi

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 deve informare immediatamente Uanataca:

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

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

1.6. Obblighi dei Titolari

1.6.1. Obblighi di custodia

Il Titolare si impegna a conservare con la dovuta premura ed attenzione eventuali dispositivi e/o codici segreti fornitigli da Uanataca.

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 Uanataca.

1.6.2. Obblighi di uso corretto

Il Titolare deve utilizzare il servizio di certificazione dei certificati fornito da Uanataca esclusivamente per gli usi autorizzati nel Manuale Operativo e in qualsiasi altra istruzione, manuale o procedimento fornito al Richiedente.

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 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.

1.7. Obblighi delle Relying Parties

1.7.1. Decisione informata

Uanataca 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 Uanataca sono disciplinati dal Manuale Operativo di Uanataca e si impegnano ad adempiere ai requisiti tecnici, operativi e di sicurezza descritti nel predetto Manuale.

1.7.2. 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:

- è necessario utilizzare un software appropriato per la verifica, capace di effettuare le operazioni crittografiche necessarie utilizzando algoritmi e lunghezze di chiavi indicate nel certificato;
- è necessario verificare lo stato di revoca dei certificati della catena di "*trust*" con l'informazione fornita al Registro di Uanataca (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;

– è necessario verificare tecnicamente la firma di tutti i certificati della catena prima di accertare il certificato utilizzato dal firmatario.

Uanataca mette a disposizione delle Relying Parties, un applicativo 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 Uanataca.

1.7.3. Attendibilità di un certificato non valido

Uanataca 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.

1.7.4. 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 firmatario entro i limiti d'uso corrispondenti.

1.7.5. 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 Uanataca nella realizzazione di transazioni vietate per legge.

I servizi di certificazione digitale erogati da Uanataca 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.

1.7.6. Clausola d'indennità

Il terzo che verifica la validità del certificato s'impegna a mantenere indenne Uanataca 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.

1.8. Obblighi di Uanataca S.A.

1.8.1. In relazione alla prestazione del servizio di certificazione digitale

Uanataca 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 firmatario nei casi e per i motivi descritti nel Manuale Operativo di Uanataca;

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 firmatario, 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.

1.8.2. In relazione alle verifiche del registro

Uanataca emetterà i certificati in base ai dati e alle informazioni fornite dai sottoscrittori: 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 Uanataca 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.

Uanataca 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.

1.8.3. Periodo di conservazione

Uanataca archivia le registrazioni corrispondenti alle richieste di emissione e di revoca dei certificati per almeno 20 anni.

Uanataca 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.

1.9. Garanzia

1.9.1. Garanzia di Uanataca S.A. per i servizi di certificazione digitale

Uanataca garantisce al Richiedente:

- che non ci siano errori di fatto nelle informazioni contenute nei certificati noti o realizzati dall'Autorità di Certificazione;
- 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;
- che i certificati rispettino tutti i requisiti materiali stabiliti nel Manuale Operativo;
- che i servizi di revoca rispettino tutti i requisiti materiali stabiliti nel Manuale Operativo.

Uanataca garantisce al terzo che accerta il certificato:

- che le informazioni contenute o incluse come riferimento nel certificato siano corrette, tranne quando sia indicato il contrario;
- 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;

- che nell'approvazione della richiesta di certificato e nell'emissione del certificato siano stati rispettati tutti i requisiti materiali stabiliti nel Manuale Operativo;
- la velocità e la sicurezza nell'erogazione dei servizi, in particolare dei servizi di revoca e deposito.

In aggiunta, Uanataca 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 Uanataca risponderà per caso fortuito o per forza maggiore.

1.9.2. Esclusioni della garanzia

Uanataca rigetta tutte le altre garanzie diverse alla precedente che non siano legalmente esigibili.

In particolare, Uanataca 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 Uanataca, tranne nei casi in cui esista una dichiarazione scritta in senso contrario.

2. Accordi applicabili e Manuale Operativo

2.1. Accordi applicabili

Gli accordi applicabili ai certificati sono i seguenti:

- Contratto dei servizi di certificazione che disciplina la relazione tra Uanataca e il Richiedente dei certificati;
- Condizioni generali del servizio incluse in questo documento;
- Dichiarazione delle Pratiche di Certificazione che disciplinano l'emissione e l'utilizzo dei certificati.

2.2. Manuale Operativo (CPS)

I servizi fiduciari di Uanataca sono regolati tecnicamente e operativamente dal Manuale Operativo (CPS) di Uanataca, dagli aggiornamenti successivi così come dalla documentazione complementare.
La documentazione è modificata periodicamente e può essere consultata al sito internet https://web.uanataca.com/it/politiche-di-certificazione.

2.3. Politica sulla privacy

Uanataca, 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").
Uanataca non può divulgare né può essere obbligata a divulgare informazioni confidenziali a meno di una richiesta specifica proveniente da:

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

Tuttavia, il Richiedente accetta che una determinata informazione personale o di altro tipo, fornita nella richiesta di certificati, sia inclusa nei certificati e nel meccanismo di verifica dello stato dei certificati, e che l'informazione menzionata non abbia carattere confidenziale per legge.
Uanataca, in conformità a quanto disposto dall'art. 13 del GDPR, ha predisposto ed adottato una precisa Informativa sulla Privacy relativamente al processo di registrazione, alla confidenzialità della registrazione, alla protezione dell'accesso alle informazioni personali e al consenso dell'utente.

L'Informativa in formato esteso è disponibile all'interno del Manuale Operativo di Uanataca.
Infine, si informa l'utente che la documentazione giustificativa di approvazione della richiesta deve essere conservata e debitamente registrata e con garanzie di sicurezza e integrità per 20 anni dalla scadenza del certificato, compreso il caso di perdita anticipata di validità per revoca.

2.4. Politica di rimborso

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

2.5. Normativa applicabile e Foro competente

Le relazioni con Uanataca sono disciplinate da quanto previsto dal Regolamento (UE) 910/2014 eIDAS e dalla normativa italiana vigente in materia.
In caso di disaccordo tra le parti, queste tenteranno la conciliazione amichevole. A tal fine le parti dovranno indirizzare una comunicazione a Uanataca tramite uno dei contatti indicati nel punto 1 di questo documento.
Per il Foro competente si rinvia al punto 9.6.9 del Manuale Operativo di Uanataca che qui abbia a intendersi come integralmente richiamato e trascritto.
Un approfondimento delle informazioni relative alla risoluzione delle dispute è disponibile all'indirizzo https://web.uanataca.com/it/politiche-di-certificazione.

2.6. Elenco dei Prestatori qualificati di servizi fiduciari elettronici

https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-servizi-fiduciari-qualificati

2.7. Divisibilità delle disposizioni, 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 della PDS continueranno a essere applicabili.
I requisiti contenuti nelle sezioni 9.6.1 (Obblighi e responsabilità), 8 (Audit di conformità) e 9.3 (Confidenzialità) del Manuale Operativo di Uanataca resteranno in vigore 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 firmatario nel contratto con Uanataca.