# Manuale Operativo

Certificate Practice Statement /
Certificate Policy

Firmato digitalmente da CHELLO ANTONIO C: IT

# *INDICE*

# INFORMAZIONI GENERALI

## *Controllo documentale*

| | |
|---|---|
| **Livello di sicurezza:** | Pubblico |
| **Ente di Emissione:** | Uanataca S.A. Unipersonale |
| **Versione:** | 1.7 |
| **Data ultima edizione:** | 30/07/2021 |
| **Codice Documento:** | Manuale_Operativo_Trust_Services_v.1.7_IT |

## *Controllo formale*

| Redatto da: | Revisionato da: | Approvato da: |
|---|---|---|
| *Legal & Compliance*<br>- Luca Santalucia<br>- Margherita Mirabella | *Legal & Compliance*<br>- Luca Santalucia<br>- Margherita Mirabella | *Direzione* |

## *Controllo delle versioni*

| Versione | Parti modificate | Descrizione delle modifiche | Data |
|---|---|---|---|
| 1.0 (Versione precedente la qualificazione ex art. 29 del CAD) | Originale | Prima versione del documento | 03/03/2020 |
| 1.1 (Versione precedente la qualificazione ex art. 29 del CAD) | Par. 3.2.2 | Introduzione Procedura di Identificazione da remoto | 23/03/2020 |
| 1.2 (Versione precedente la qualificazione ex art. 29 del CAD) | Aggiunta delle sezioni relative al servizio di Sigillo elettronico qualificato | Servizio di Sigillo elettronico qualificato | 27/03/2020 |
| 1.3 (Versione precedente la qualificazione ex art. 29 del CAD) | Aggiornamento del documento | - Recepimento Determina n. 147/2019 (AgID); | 11/06/2020 |

| | | | |
|---|---|---|---|
| 1.4<br>(Versione precedente la qualificazione ex art. 29 del CAD) | Par. 3.1.1; 3.1.3; 3.2.2; 3.2.2.1; 3.2.2.2; 4.5.2.1; 4.9.2; 4.9.14. | - Inserimento nuovo logo;<br>- Revisione e aggiornamento dei seguenti paragrafi: | 30/06/2020 |
| 1.5 | Par. 9.4. | - Aggiornamento Informativa sulla Privacy; | 01/12/2020 |
| 1.6 | Par. 1.1., 1.2., 1.3.1, 1.3.1., 1.3.1.3, 1.3.2., 1.3.3., 1.4.1.4., 3.2.2., 3.2.3., 9.4.1., 9.6.4, 9.6.4.1., 9.6.4.2., 9.6.4.3., 9.6.4.4., 9.6.4.5. | - Introduzione delle sezioni relative all'emissione dei certificati di CNS. | 03/05/2021 |
| 1.7 | Par. 3.2.2.3, 3.2.2.4, 3.2.2.5, 3.2.2.6, 3.2.4; 9.4.1. | - Introduzione di nuove modalità di Identificazione dei Richiedenti;<br>- Aggiornamento dell'Informativa sulla Privacy. | 30/07/2021 |

# 1. INTRODUZIONE

## 1.1. Presentazione

Il presente documento pubblico, "*Manuale Operativo*" o anche "*Certification Practice Statement*" (CPS), descrive le procedure operative seguite da Uanataca 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 marcatura temporale qualificata;
- emissione della Carta Nazionale dei Servizi;

Uanataca S.A. (Società anonima) unipersonale (di seguito anche solo "Uanataca") è una società per azioni costituita in Spagna, all'interno dello Spazio Economico Europeo.

Nell'anno 2019 ha aperto la propria sede secondaria in Italia, tramite iscrizione al Registro delle Imprese di Napoli.

Il 100% del capitale sociale di Uanataca è detenuto dalla società Bit4 Group S.r.l. con sede in Napoli alla Via Diocleziano n. 107 il cui rapp.te legale e amm.re unico è identificato nella persona del sig. Antonio Chello, già rapp.te legale della sede secondaria di Uanataca in Italia.

Per ulteriori informazioni in merito ai dati societari si veda il successivo capo 1.5.1.

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;
- **Certificato di autenticazione:**
  - Carta Nazionale dei Servizi.

I Servizi Fiduciari qualificati erogati da Uanataca 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.

Inoltre, Uanataca 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.

La struttura del presente Manuale si basa sulla specifica pubblica RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*".

## 1.2. Nome e identificativo del documento

Questo documento è il "*Manuale Operativo*" (o *Certification Practice Statement* / CPS) di Uanataca. La versione vigente del presente Manuale è indicata nell'intestazione del documento e nella sezione "*Controllo delle versioni*".

### 1.2.1. 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 Uanataca e sono specificate all'interno di ciascun certificato.

| OID | Tipo di certificato |
|---|---|
| | **Servizio di firma elettronica** |
| 1.3.6.1.4.1.47286.10.1.1 | Certificato qualificato di sottoscrizione in QSCD |
| 1.3.6.1.4.1.47286.10.1.10 | Certificato qualificato di sigillo elettronico in QSCD |
| | **Servizio di Marca Temporale** |
| 1.3.6.1.4.1.47286.10.2.1 | Certificato di Time Stamping Unit |
| | **Servizio di emissione della Carta Nazionale dei Servizi** |
| 1.3.6.1.4.1.47286.10.3.1 | Certificato di autenticazione |

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 Uanataca, prevarrà quanto stabilito nel presente Manuale Operativo.

Uanataca 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 Uanataca 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 Uanataca al seguente indirizzo: https://web.uanataca.com/it/politiche-di-certificazione.

## 1.3. Partecipanti ai servizi di certificazione

### 1.3.1. Prestatore Qualificato di Servizi Fiduciari (Qualified Trust Service Provider - TSP)

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

| | |
|---|---|
| **Ragione Sociale:** | Uanataca S.A. (Sociedad Anonima Unipersonal) |
| **Partita IVA (NIF):** | A66721499 |
| **Sede legale** | Calle Riera de Can Toda, 24-26 - 08024 Barcellona (Spagna) |
| **Tel:** | +34 935 272 290 |
| **Sede Secondaria** | Via Diocleziano, 107 - 80125 Napoli (Italia) |
| **Tel:** | +39 081/7625600 |

Uanataca eroga i seguenti servizi fiduciari:

- rilascio e gestione dei certificati qualificati (firma elettronica qualificata e sigillo elettronico qualificato), in conformità alle disposizioni di cui al Regolamento (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").
- 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".
- rilascio, in qualità di ente Certificatore, della Carta Nazionale dei Servizi in conformità al Decreto interministeriale 9 dicembre 2004 e s.m.i. recante "*regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi*" e a tutta la relativa disciplia applicabile in ambito nazionale.

Per la fornitura di servizi fiduciari qualificati, Uanataca si avvale delle seguenti chiavi di certificazione, 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.

#### *1.3.1.1. Uanataca CA Qualificata eIDAS 2020*

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:** | **UANATACA Qualified eIDAS CA 2020** |
| **Fingerprint (SHA1):** | 207786e20d9de8393230285d299f5429c93f6b28 |
| **Valido dal:** | 07/04/2020 |
| **Scadenza:** | 02/04/2040 |
| **Lunghezza Chiave RSA** | 4096 |

#### *1.3.1.2. Uanataca TSA Qualificata eIDAS 2020*

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:** | **UANATACA Qualified TSA 2020** |
| **Fingerprint (SHA1):** | e74ff9f7012d7a1ae44ef759cfe86d5e009c5eda |
| **Valido dal:** | 07/04/2020 |
| **Scadenza:** | 02/04/2040 |
| **Lunghezza Chiave RSA** | 4096 |

#### *1.3.1.3. Uanataca CNS CA 2020*

Si tratta della CA che rilascia i certificati di autenticazione e sottoscrizione tramite Carta Nazionale dei Servizi, in qualità di Certificatore a favore dell'Ente Emettitore, amministrazione pubblica con la quale Uanataca ha sottoscritto apposita Convenzione, il cui certificato è autofirmato (*self-signed*).

**Dati identificativi:**

| | |
|---|---|
| **CN:** | **UANATACA CNS CA 2020** |
| **Fingerprint (SHA1):** | eae79fa0da7b40c0e180a24ea297b5092755739a |

| | |
|---|---|
| **Valido dal:** | 07/04/2020 |
| **Scadenza:** | 02/04/2040 |
| **Lunghezza Chiave RSA** | 4096 |

### *1.3.2. Ente Emettitore*

Ai sensi del Decreto Interministeriale 9 dicembre 2004 recante regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi, l'Ente Emettitore è responsabile della formazione e del rilascio della CNS.

Nell'ambito delle attività di emissione dei certificati di CNS l'Ente Emettitore è, quindi, la Pubblica Amministrazione, responsabile di tutto il circuito di emissione della CNS, garantendone in termini di sicurezza tutte le fasi del ciclo di vita mentre il ruolo di Certificatore, definito quale "Ente che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche" è svolto, appunto, da Uanataca.

La registrazione dei Richiedenti il certificato per la CNS è svolta direttamente dall'Ente Emettitore che può delegare tali attività al Certificatore Uanataca.

La registrazione può avvenire anche per mezzo di strutture opportunamente delegate dall'Ente Emettitore o dallo stesso Certificatore che prendono il nome di Uffici di Registrazione (Registration Authorities – R.A.)

### *1.3.3. Uffici di Registrazione (Registration Authorities – R.A.)*

Lo svolgimento delle attività di identificazione ed autenticazione dei Richiedenti (ovvero i soggetti che richiedono i certificati) può essere svolta sia dallo stesso personale della CA, sia da Uffici di Registrazione (R.A. - "*Registration Authorities*") di terze parti delegate da Uanataca, attraverso la stipula di appositi mandati.

Gli Uffici di Registrazione (RA) costituiscono, dunque, terze parti cui Uanataca affida, tramite mandati *ad hoc*, l'incarico per lo svolgimento delle attività di identificazione ed autenticazione dei soggetti che richiedono i certificati.

Gli Uffici di Registrazione nominati da Uanataca saranno adeguatamente formati e sottoposti a tutte le necessarie verifiche finalizzate alla verifica circa il regolare adempimento degli impegni e degli obblighi derivanti dal mandato.

In particolare, una RA svolge le seguenti attività:

- identificazione e autenticazione (I&A) del Richiedente;
- verifica dei requisiti necessari e dei dati identificativi di colui che figurerà come Titolare del certificato;
- registrazione dei dati del Richiedente;
- autorizzazione all'emissione di certificati digitali attraverso appositi strumenti messi a disposizione da Uanataca;

- custodia della documentazione relativa: a) all'identificazione del Richiedente; b) alla registrazione del Richiedente; c) alla gestione del ciclo di vita dei certificati.

In conclusione, i soggetti che possono agire in qualità di RA di Uanataca possono essere costituiti da:

- personale appartenente a Uanataca;
- qualsiasi persona fisica o giuridica, esterna a Uanataca, espressamente autorizzata da quest'ultima tramite apposito mandato per lo svolgimento di attività di Ufficio di Registrazione.

Uanataca, infatti, si impegna a formalizzare contrattualmente ogni tipo di rapporto intercorrente con i soggetti che agiranno per suo conto come Uffici di Registrazione.

La R.A., a sua volta, potrà autorizzare una o più persone ad agire come "Operatori di Registrazione". Quest'ultimo, previa stipula di un apposito accordo con la R.A., potrà essere delegato a svolgere le attività di identificazione ed autenticazione dei Richiedenti per conto della R.A.

È onere della RA nominata di fornire i nominativi di tutto il personale impiegato nelle operazioni di identificazione in conformità al presente Manuale Operativo.

Le R.A. sono attivate solo a seguito di un'opportuna formazione del personale impiegato.

Uanataca si riserva il diritto di non abilitare e/o di disabilitare uno o più Operatori di Registrazione che operino in maniera non conforme alle disposizioni del presente Manuale Operativo.

Le R.A. sono inoltre soggette a verifiche periodiche da parte di Uanataca con lo scopo di verificare il rispetto degli accordi sottoscritti con la CA e delle procedure definite nel presente documento.

### *1.3.4. 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 Uanataca.

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

1) **Richiedenti:** persone fisiche o giuridiche che domandano alla C.A. 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.

#### *1.3.4.1. Richiedenti*

Sono le persone fisiche o giuridiche che richiedono il rilascio di certificati digitali, rivolgendosi direttamente alla C.A. o ad una sua RA.

Il Richiedente, pertanto, può anche qualificarsi come "Cliente" della C.A.: questi, al momento della richiesta formale di certificato, dichiara di accettare le Condizioni Generali di contratto stabilite dalla CA e, pertanto, acconsente all'esercizio dei diritti e al rispetto degli obblighi dettati da quest'ultima.

Le condizioni contrattuali disposte dalla C.A. si aggiungono ed integrano i diritti e gli obblighi dei Richiedenti e/o Titolari sanciti nella normativa tecnica, di matrice europea, relativa all'emissione dei certificati qualificati, con particolare riferimento allo standard "ETSI EN 319 411", sezioni 5.4.2 e 6.3.4.e.

A seguito dell'emissione del certificato, il Richiedente si identifica nel Titolare.

### *1.3.4.2. Titolare del certificato*

Il Titolare del certificato è il soggetto che possiede ed utilizza la chiave privata relativa ad un certificato di firma o un certificato di sigillo elettronico corrispondente alla chiave pubblica contenuta nel certificato.

È evidente che il Titolare del certificato 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 Uanataca, 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 derivanti dallo smarrimento della chiave privata indicate all'interno del presente Manuale.

## *1.3.5. Relying parties (R.P.)*

Le Relying Parties (R.P.) si identificano nei soggetti che fanno affidamento sulle informazioni contenute nei certificati emessi da Uanataca.

In particolare, per quanto riguarda il servizio descritto nel presente Manuale, per R.P. si intendono:

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

Tutti coloro che devono fare affidamento sulle informazioni contenute nei certificati 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 Uanataca.

### 1.3.6. Autorità

#### 1.3.6.1. 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.

#### 1.3.6.2. 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 del Prestatore di servizi fiduciari qualificati e dei servizi fiduciari qualificati da esso prestati alle normative e agli standard applicabili.

## 1.4. Utilizzo dei certificati

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

### 1.4.1. Uso previsto dei certificati

I certificati emessi da Uanataca, 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.
Uanataca si riserva la facoltà di revocare i certificati qualora venga a conoscenza che questi siano utilizzati in modo improprio o contrario alle disposizioni del presente Manuale.

#### 1.4.1.1. Certificato qualificato di sottoscrizione in QSCD

Questo certificato è contrassegnato da OID 1.3.6.1.4.1.47286.10.1.1. Si tratta di un certificato qualificato emesso per la firma elettronica qualificata, in conformità alla politica di certificazione *QCP-n-qscd* con OID 0.4.0.194112.1.2, il quale viene dichiarato nel certificato.

Tale certificato, emesso in QSCD, costituisce un certificato qualificato secondo quanto stabilito nell'art. 28 del Regolamento (UE) 910/2014 eIDAS.

Funziona 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, garantisce l'identità del Titolare e consente 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 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).

### *1.4.1.2. Certificato qualificato di sigillo elettronico in QSCD*

Questo certificato è contrassegnato da OID 1.3.6.1.4.1.47286.10.1.10 Si tratta di un certificato qualificato emesso per il sigillo elettronico qualificato, in conformità alla politica di certificazione *QCP-l-qscd* con OID 0.4.0.194112.1.3, il quale viene dichiarato nel certificato.

Tale certificato, emesso in "*Qualified Seal Creation Device*" (di seguito anche solo "*QSealCD*" o anche "QSCD", costituisce un certificato qualificato ai sensi dell'art. 38 del Regolamento (UE) 910/2014 eIDAS: "*Certificati Qualificati di Sigilli Elettronici*".

Funziona 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).

#### 1.4.1.3. Certificato qualificato di Time Stamping Unit

Questo certificato è contrassegnato dall' OID 1.3.6.1.4.1.47286.10.1.1 e viene emesso in accordo con la politica di certificazione QCP-l-qscd recante l'OID 0.4.0.194112.1.3.
I certificati di Time Stamping Unit sono generati per emettere marche temporali.
La sincronizzazione del sistema di emissione di marche temporali di Uanataca si effettua attraverso il protocollo NTP, puntando a un server con un livello di sincronizzazione *Stratum 3*.

#### 1.4.1.4. Certificato con profilo "CNS – Carta Nazionale dei Servizi"

I certificati di CNS sono emessi da Uanataca che opera in qualità di certificatore per conto dell'Ente Emettitore, nella definizione di cui al Decreto Ministeriale 9 dicembre 2004, secondo le modalità indicate dal presente Manuale Operativo, come mezzo di autenticazione in rete.
In particolare, l'ambito del certificato CNS è circoscritto ad un browser (applicazione di navigazione web) per la *client authentication* mediante protocollo sicuro (*suite SSL/TLS*) ed una firma elettronica avanzata nel formato S/MIME. La firma elettronica assicura la paternità (origine) e integrità delle informazioni.
L'affidabilità della chiave privata è garantita dalla validità del certificato della corrispondente chiave pubblica ovvero che tale certificato non sia né scaduto, né revocato o sospeso.
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, nella documentazione contrattuale nonché in violazione dei limiti d'uso e di valore (*key usage*, *extended key usage*, *user notice*) indicati nel certificato.
Uanataca si riserva la facoltà di revocare i certificati qualora venga a conoscenza che tali certificati siano stati utilizzati in modo improprio.

### 1.4.2. Limiti e divieti nell'utilizzo dei certificati

I certificati emessi da Uanataca vengono impiegati per la funzione che gli è propria 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 Uanataca 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).
Uanataca 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 Uanataca in operazioni che contravvengono al presente Manuale Operativo, alle Condizioni Generali di Contratto, alla documentazione inerente a ciascuna

tipologia di certificato, ai contratti tra la RA e i Richiedenti, costituisce un utilizzo indebito e contrario agli effetti di legge, esimendo, pertanto, Uanataca, da ogni responsabilità per ogni eventuale danno derivante da un utilizzo indebito dei certificati compiuto dal Titolare o da qualsiasi altra Parte.

Uanataca 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 Richiedente il soggetto responsabile dell'utilizzo del certificato e dei contenuti ad esso associati.

Parimenti, sarà imputabile al Richiedente ovvero al soggetto autorizzato alla custodia del certificato 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, nei contratti tra la RA e i Richiedenti, così come da qualsiasi altro utilizzo considerato indebito dalla normativa vigente in materia.

## 1.5. Amministrazione del Manuale Operativo

### 1.5.1. Organizzazione responsabile

Il presente documento CPS di Uanataca è aggiornato alla versione risultante dal "Controllo delle Versioni" o dal "Controllo Documentale" di cui alle "Informazioni Generali" del presente Manuale e viene redatto, pubblicato ed aggiornato da Uanataca.

I dati di contatto del TSP sono i seguenti:

Ragione Sociale: **Uanataca S.A. (Sociedad Anonima Unipersonal)**

Partita Iva (N.I.F.): A66721499

**Sede legale**: Riera de Can Toda, 24-26 - 08024 Barcelona (España)

Tel: +34 935 272 290

**Sede Secondaria**: Via Diocleziano, 107 - 80125 Napoli (Italia)

P.IVA: 04741241212

Tel: 081 7625600

Fax: 081 7352517

**Sede Operativa**: Calle Marie Curie, 8-14 – 08042 Barcellona (Spagna)

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

**Rappresentante legale**: Gabriel Garcia Martinez

**Rappresentante legale (sede secondaria)**: Antonio Chello

### 1.5.2. Procedura di approvazione e gestione

Uanataca 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.

## 1.6. Definizioni e acronimi

Di seguito una breve lista degli acronimi utilizzati; qualora, all'interno del Manuale, 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**: Agenzia per l'Italia Digitale;
- **CA**: Certification Authority;
- **CAB**: Conformity Assessment Body;
- **CAD**: Codice dell'Amministrazione Digitale (D.lgs. n.82/2005);
- **CNS**: Carta Nazionale dei Servizi;
- **CP**: Certificate Policy;
- **CRL**: Certificate Revocation List;
- **CSP**: Certification Practice Statement;
- **ETSI**: European Telecommunications Standards Institute;
- **FQDN**: Fully Qualified Domain Name;
- **GDPR**: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
- **HSM**: Hardware Security Module;
- **HTTP**: Hyper-Text Transfer Protocol;
- **I&A**: Identificazione e Autorizzazione;
- **IR**: Incaricato di Registrazione;
- **OCSP**: On-line Certificate Status Protocol;
- **OID**: Object IDentifier;
- **PKI**: Public Key Infrastructure;
- **QSCD**: "Qualified Signature-Creation Device" o anche "Qualified Seal Creation Device";
- **RA**: Registration Authority;
- **TLS**: Transport Layer Security;
- **TSL**: Trust-service Status List;
- **TSP**: Trust Service Provider;
- **QTSP**: Qualified Trust Service Provider;

# 2. PUBBLICAZIONE DELLE INFORMAZIONI E REPOSITORY

## 2.1. Repository

Uanataca 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 Uanataca https://web.uanataca.com/it/.

Il "*Repository*" è accessibile in modo continuo (24x7x365).

Nell'ipotesi in cui si verifichi un arresto del sistema, al di fuori del controllo di Uanataca, 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.

## 2.2. Elenco delle informazioni pubblicate dalla C.A.

Uanataca pubblica le seguenti informazioni:

- La Lista dei certificati revocati (CRL);
- Le *PKI Disclosure Statement* (PDS);
- la *Certification Practice Statement* (CPS);
- Le Condizioni generali di contratto (Terms and Conditions);
- La Modulistica relativa ai Servizi Fiduciari;
- I certificati della PKI.

## 2.3. 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 4 del presente Manuale Operativo.

## 2.4. Controllo degli accessi

Uanataca 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.

# 3. IDENTIFICAZIONE E AUTENTICAZIONE

## 3.1. Nomi

### 3.1.1. 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.

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 persons.
- **ETSI EN 319 412-5**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

### 3.1.2. 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*.

Nell'ipotesi in cui i dati indicati nel campo *DN* o *Subject* siano fittizi (es. "*Organizzazione test*", "*Nome test*", "*Cognome test*") o vengano indicate parole che inequivocabilmente ne denotano l'invalidità (es. "TEST", "PROVA" o "NON VALIDO"), il certificato risulterà privo di valenza legale e, pertanto, si escluderà ogni responsabilità da parte di Uanataca circa il suo utilizzo.

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

### 3.1.3. 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.

### 3.1.4. 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).

### 3.1.5. 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 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 Uanataca, 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".

### 3.1.6. Eventuali limitazioni d'uso

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

Uanataca garantisce, in conformità all'art. 4.1 n. 7 della Determinazione n. 147/2019 di AgID e su richiesta del Titolare del Certificato, 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 (indicare il soggetto).

### 3.1.7. Soluzione dei conflitti relativi ai nominativi

Uanataca 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 Uanataca 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 C.A. si riserva il diritto di rigettare una richiesta di certificato, nell'ipotesi in cui sussista un conflitto sui nomi.

## 3.2. Verifica iniziale dell'identità

La C.A., anche mediante un Ufficio di registrazione (R.A.), verifica con certezza l'identità di ogni Richiedente alla prima richiesta di emissione di un certificato qualificato al fine di assicurare che quel certificato possa riferirsi in maniera accurata e completa al soggetto Richiedente (sia esso persona fisica o giuridica); prima di procedere al rilascio del certificato richiesto, dunque, la C.A. oppure la R.A. dovrà svolgere tutte le attività necessarie all'identificazione del Richiedente.

L'identità del Richiedente il certificato viene solitamente verificata tramite un documento di identità nonché tramite specifici attribuiti che possono essere: l'associazione con l'Organizzazione di appartenenza, il ruolo posseduto all'interno dell'organizzazione, il certificato di attribuzione di codice fiscale/partita iva, nel caso di persone giuridiche.

L'operazione di identificazione è svolta in ottemperanza a quanto previsto dalla vigente normativa: il soggetto incaricato ad effettuare le attività di identificazione sarà, quindi, tenuto a verificare l'identità del richiedente tramite il riscontro con uno dei documenti aventi validità legale ai sensi dell'art. 35 d.P.R. del 28 dicembre 2000 n. 445 tra cui sono ricompresi (Carta di identità, Passaporto, Patente di guida, Patente di abilitazione al comando di unità da diporto, Libretto di pensione, Patentino di abilitazione alla conduzione di impianti termici, Porto d'armi).

Tutta la documentazione così acquisita e verificata sarà conservata dalla C.A., in conformità a quanto disposto dal Regolamento (UE) 2016/679 – GDPR - del Parlamento Europeo e del Consiglio del 27 aprile 2016 e s.m.i., per tutto il tempo necessario ad assicurare la fruizione e la continuità del servizio richiesto.

Per garantire la tutela e la gestione dei dati personali acquisiti nel corso delle procedure di registrazione, inoltre, sarà preventivamente fornita ad ogni richiedente l'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. 3.2.2. e seguenti.

### 3.2.1. 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, Uanataca verifica che il Richiedente sia in possesso della chiave privata corrispondente alla chiave pubblica da certificare.

### 3.2.2. Autenticazione dell'identità di una persona fisica

Questa sezione illustra i metodi di verifica dell'identità di una persona fisica identificata in un certificato.

Gli operatori incaricati di verificare l'identità delle persone fisiche che richiedono il Certificato eseguono le operazioni di identificazione secondo le modalità previste nel presente Manuale Operativo, in conformità alle linee guida di cui al Pr. 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 delle Richiedenti, identificate nei certificati, è comprovata dalla presentazione di un documento di riconoscimento valido agli effetti di legge (Carta di identità, Passaporto, Patente di guida, Patente di abilitazione al comando di unità da diporto, Libretto di pensione, Patentino di abilitazione alla conduzione di impianti termici, Porto d'armi ovvero uno dei documenti di identità aventi validità legale ai sensi degli artt. 1 e 35 d.P.R. del 28 dicembre 2000 n. 445 e s.m.i.).

È necessario che il documento di riconoscimento valido agli effetti di legge, ai sensi della normativa su richiamata, sia in corso di validità (e dunque non scaduto al momento della presentazione della richiesta di emissione del certificato); inoltre, è necessario che al predetto documento sia acclusa una fotografia chiara che consenta la riconducibilità diretta al soggetto che lo esibisce.

Al tal riguardo l'art. 1 lett. c) D.P.R. 445/2000 attribuisce la qualifica di "*Documento d'identità*" ad ogni documento *"…munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare"*.

Inoltre, ai sensi dell'art. 35 D.P.R. 445/2000: *"In tutti i casi in cui nel presente testo unico viene richiesto un documento di identità, esso può sempre essere sostituito dal documento di riconoscimento equipollente ai sensi del comma 2. Sono equipollenti alla carta di identità il passaporto, la patente di guida, la patente nautica, il libretto di pensione, il patentino di abilitazione alla conduzione di impianti termici, il porto d'armi, le tessere di riconoscimento, purché munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato"*.

Per l'elenco completo dei documenti di identità accettati da Uanataca si rimanda all'allegato "B" al presente Manuale.

#### *3.2.2.1. Procedura di identificazione De Visu*

Tale procedura di identificazione prevede la presenza fisica del Richiedente dinnanzi ad un Operatore o al personale autorizzato dalla R.A. di Uanataca, il quale provvede (avendo ricevuto apposita formazione in precedenza) ad accertare l'identità del Richiedente attraverso la verifica dei corrispondenti documenti di identità esibiti in originale.

È specifico onere dell'Operatore accertarsi che il documento di identità esibito risulti in corso di validità (e, dunque, che non sia scaduto al momento della presentazione della richiesta di emissione del certificato) e che quest'ultimo rechi in maniera chiara la fotografia del soggetto da identificare.

È necessario che il Richiedente sia in possesso del Codice Fiscale (Tessera Sanitaria, Tessera del Codice Fiscale, Certificato di attribuzione di Codice Fiscale ecc..) la cui esibizione può essere richiesta dai soggetti abilitati ad eseguire il riconoscimento; in mancanza sarà possibile utilizzare un analogo codice identificativo (es: codice di previdenza sociale) o il numero identificativo del passaporto.

Gli Uffici di Registrazione che operano in altri Stati membri dell'Unione Europea, così come quelli che procedono all'identificazione di Richiedenti che risiedono in altri Stati membri dell'Unione Europea, possono ricevere autorizzazione da Uanataca ad accettare documenti di identità emessi dalle autorità competenti nel Paese in questione. La lista di questi documenti è redatta da Uanataca e pubblicata ed aggiornata periodicamente sul suo sito internet.

Nel caso di persona fisica, il personale incaricato ed addetto all'identificazione provvederà all'accertamento delle seguenti tipologie di dati:

- Nome completo (prenome, nome e cognome);
- data e luogo di nascita;
- indirizzo di residenza e di domicilio;
- codice fiscale o altro codice identificativo univoco;
- indirizzo di posta elettronica o p.e.c.;
- tipo e numero del documento di identità esibito;
- Autorità che ha rilasciato il documento, data e luogo di rilascio, data di scadenza;
- ogni altro dato ritenuto utile ai fini dell'identificazione;

Nel caso in cui il soggetto da identificare sia una persona fisica identificata in associazione con una persona giuridica (della quale è dipendente o legata da rapporto di collaborazione) l'addetto provvederà ad acquisire le seguenti informazioni:

- Nome completo (prenome, nome e cognome);
- data e luogo di nascita;
- indirizzo di residenza e di domicilio;
- codice fiscale;
- indirizzo di posta elettronica o p.e.c.;
- tipo e numero del documento di identità esibito;
- Autorità che ha rilasciato il documento, data e luogo di rilascio, data di scadenza;
- nome completo e denominazione sociale della persona giuridica associata;
- qualsiasi informazione di registrazione esistente relativamente alla persona giuridica associata;
- tipo di affiliazione della persona fisica alla persona giuridica e documentazione comprovante tale rapporto.
- ogni altro dato ritenuto utile ai fini dell'identificazione;

Sarà onere del Richiedente fornire, al termine delle operazioni di identificazione, un indirizzo fisico o di domicilio dove poter essere contattato.

L'Ufficio di Registrazione verificherà, mediante la visualizzazione di documenti o attraverso le proprie fonti di informazione, il resto dei dati e degli attributi da includere nel certificato, conservando la documentazione che ne comprova la validità nei termini e per la durata previsti dalle normative applicabili.

La procedura di identificazione può essere svolta anche da un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività, ivi comprese le disposizioni di cui al D.L. 3 Maggio 1991, n. 143 e s.m.i..

Una volta terminata la procedura di identificazione da parte di un Operatore a ciò autorizzato, questi è tenuto a raccogliere e ad archiviare in maniera precisa ed ordinata, gli originali di tutta la documentazione inerente ogni singola richiesta di emissione dei Certificati nonché tutta la documentazione relativa all'identificazione dei Richiedenti che sarà preventivamente comunicata a Uanataca, anche in formato elettronico, al fine di attivare correttamente la procedura di emissione dei Certificati.

Uanataca si impegna a conservare e ad archiviare tutte le informazioni relative ai Dati Personali dei Richiedenti, in conformità con il Regolamento (UE) n. 679/2016 e la propria Politica sulla Privacy.

#### *3.2.2.2. Procedura di identificazione da remoto*

In alternativa alla procedura di identificazione "*de visu*", Uanataca, in armonia con gli obiettivi di cui al Regolamento eIDAS tesi a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini e imprese, ha previsto una procedura di identificazione dei richiedenti da remoto, tramite utilizzo di una apposita piattaforma telematica di video-identificazione.

Uanataca garantisce l'utilizzo di procedure e strumenti in grado di garantire, sul piano giuridico, l'identificazione "*certa*" del Richiedente il certificato qualificato, in piena conformità a quanto richiesto dall'art. 19 del CAD secondo cui il certificatore che *"rilascia […] certificati qualificati deve […] provvedere con certezza alla identificazione della persona che fa richiesta della certificazione" e dal successivo art. 32 co. 3 lett. a).*

Gli Uffici di Registrazione che operano in altri Stati membri dell'Unione Europea, così come quelli che procedono all'identificazione di Richiedenti che risiedono in altri Stati membri dell'Unione Europea, possono ricevere autorizzazione da Uanataca ad accettare documenti di identità emessi dalle autorità competenti nel Paese in questione. La lista di questi documenti e le relative caratteristiche (in grado di fornire certezza dell'identità) viene analizzata da Uanataca, che procede alle comunicazioni opportune ad AgID prima di effettuare la pubblicazione della lista dei documenti accettati sul proprio sito internet.

Una volta effettuata la richiesta di emissione di un certificato digitale qualificato da parte del Richiedente, Uanataca o un suo Ufficio di Registrazione (RA) autorizzato, provvederà alla fissazione della data e dell'ora del primo appuntamento disponibile, la quale sarà comunicata al Richiedente tramite i canali di comunicazione da quest'ultimo indicati in fase di richiesta.

Prima di procedere con tale modalità di identificazione il Richiedente viene informato che dovrà disporre di un Personal Computer, di uno smartphone o di un Tablet dotato di *webcam* (ovvero di videocamera che consenta la visualizzazione e l'ascolto di tutto ciò che avviene nel suo campo

visuale) e, successivamente, gli verranno fornite le opportune indicazioni in relazione alla piattaforma da utilizzare per la video-identificazione

Il sistema per la video-identificazione è messo a disposizione direttamente da Uanataca o anche da terzi e comunque deve essere in grado di garantire che le modalità di registrazione delle immagini e dei video assicurino la non alterabilità e/o sostituibilità del soggetto ripreso e di tutte le immagini e/o suoni che vengono rilevati nel corso della sessione di ripresa tramite *webcam*.

Inoltre, è necessario che, durante la sessione di ripresa, l'immagine video sia a colori e consenta una chiara visualizzazione dell'interlocutore.

L'operatore, al fine di assicurare quanto sopra, potrà non avviare o sospendere in qualsiasi momento la procedura di identificazione qualora la qualità audio/video risulti tale da non garantire i requisiti sopra indicati nonché quelli di cui all'art. 32 comma 3 lett. a) del CAD.

Scegliendo di proseguire nella procedura di identificazione da remoto il Richiedente sarà informato sulle modalità e sul Trattamento dei Dati Personali, in conformità alla Privacy Policy prevista da Uanataca e che la sessione di identificazione tramite *webcam* sarà registrata; in questo modo il Richiedente potrà così scegliere se fornire o meno il consenso al Trattamento: resta inteso che, in caso di mancato consenso circa il Trattamento dei Dati Personali da parte del Richiedente, Uanataca non potrà procedere alla successiva identificazione.

In caso di manifestazione espressa del consenso, che potrà avvenire anche a seguito di esplicita richiesta dell'operatore incaricato all'inizio di ogni sessione, Uanataca o uno degli operatori a ciò autorizzati, potrà procedere con l'identificazione da remoto.

A questo punto, avviata la sessione tramite *webcam*, l'operatore incaricato, ai fini di una corretta identificazione personale tramite il documento di identità, provvederà, innanzitutto a verificare se:

a. il documento è stato rilasciato da un'Amministrazione dello Stato;
b. il documento reca la fotografia del soggetto;
c. nel documento sono presenti i dati anagrafici del soggetto;
d. il documento presenta il seriale identificativo;
e. il documento presenta idonei segni di anticontraffazione;

Uanataca garantisce che gli operatori incaricati di effettuare le operazioni sopra descritte sono adeguatamente formati; è facoltà dell'incaricato, dunque, escludere l'ammissibilità dei documenti esibiti dai Richiedenti, se carenti di una delle caratteristiche sopra elencate.

Una volta completata e chiusa la sessione di identificazione da remoto, il video così realizzato sarà conservato e protetto in modo adeguato, in conformità al Trattamento dei dati personali di cui alla Privacy Policy adottata da Uanataca.

#### *3.2.2.3. Procedura di identificazione tramite AML (Anti-money Laundering)*

Con il Decreto legislativo 21 novembre 2007, n. 231, di recepimento della Direttiva 2005/60/CE in materia di AML (*Anti-money Laundering*), come modificato dal Decreto Legislativo 25 maggio 2017, n. 90, di recepimento della direttiva (UE) 2015/849 (poi sostituita dalla Direttiva (UE)

2018/843) relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo è stata data attuazione in Italia alle disposizioni europee in tema di AML nonché di organizzazione, procedure e controlli interni in materia di comunicazioni oggettive ed in materia di adeguata verifica della clientela previsti dal D.Lgs. n. 90/2017 (di seguito anche solo "*Normativa AML*").

Importante menzione sul tema meritano anche gli Orientamenti emanati congiuntamente dalle Autorità di Vigilanza europee (*EBA*, *ESMA* e *EIOPA*) sulle misure semplificate e rafforzate di adeguata verifica della clientela e sui fattori di rischio, pubblicati il 4 gennaio 2018 nonché le "*Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo*" emesse dalla Banca d'Italia (30/07/2019).

Allo scopo di semplificare e snellire le procedure di identificazione ed evitare che uno stesso soggetto, già identificato presso altra organizzazione o organismo, debba nuovamente effettuare la procedura di identificazione Uanataca, in accordo con la normativa italiana ed Europea sopra richiamata, ha adottato la seguente "*procedura di identificazione tramite AML (Anti-money laundering)*".

La predetta procedura può essere applicata unicamente nell'ipotesi in cui vi sia già stata la previa identificazione del Richiedente da parte di un soggetto a ciò autorizzato (Intermediario Finanziario o Soggetto Esercente Attività Finanziaria) che, in ossequio alla normativa su richiamata in materia di *AML* (o Antiriciclaggio) ha assolto precisi obblighi e osservato specifiche procedure nella fase di identificazione dei propri clienti.

I soggetti che, ai sensi della Normativa AML, identificano i Richiedenti sono tenuti ad accettare le disposizioni del presente Manuale e a stipulare appositi accordi con Uanataca al fine di operare quali Uffici di Registrazione (R.A.).

L'acquisizione dei dati identificativi dei Richiedenti, da parte dei soggetti abilitati ai sensi della Normativa AML, comporta che Uanataca potrà emettere certificati digitali qualificati a favore dei Richiedenti già identificati; tuttavia è necessario, al fine di completare correttamente la procedura di riconoscimento e di emissione del certificato in conformità alle disposizioni del presente Manuale, che il Richiedente sottoscriva le Condizioni Generali di Contratto per la fornitura dei servizi fiduciari qualificati predisposte da Uanataca e confermi i dati identificativi già precedentemente acquisiti.

#### *3.2.2.4. Procedura di identificazione tramite CIE/Passaporto Elettronico*

Uanataca ha previsto, quale ulteriore modalità di identificazione, la possibilità di utilizzare la CIE "*Carta di Identità Elettronica*" o il Passaporto Elettronico per l'acquisizione certa dei dati identificativi dei Richiedenti.

Per *CIE*, ai sensi dell'art. 1 del D.M. 23 dicembre 2015 si intende: "*il documento di identità personale rilasciato dal Ministero dell'Interno denominato "Carta di Identità Elettronica*".

Com'è noto la CIE, così come il Passaporto Elettronico sono documenti idonei a certificare l'identità fisica e digitale del possessore/intestatario e consentono l'attivazione di servizi basati sull'utilizzo del microprocessore a radio frequenza di cui sono dotati.
Ai fini dell'identificazione tramite uno di questi due documenti è necessario che il Richiedente sia dotato, in alternativa, di un lettore di smart-card e/o lettore smart-card con NFC, che consenta di accedere ai servizi di Uanataca con il più alto livello di sicurezza.
Nello specifico, le componenti software predisposte a tal scopo, elaborano la richiesta di autenticazione confermandone la correttezza e l'autenticità: il processo di autenticazione è garantito mediante la verifica di validità (autenticità e scadenza) del certificato digitale presente a bordo della CIE o del Passaporto Elettronico che viene letto dal microprocessore della carta ed inviato presso la C.A. Uanataca (cfr. DM del 23 dicembre 2015).
A seguito della corretta esecuzione della procedura di identificazione sopra descritta sarà possibile, per Uanataca, emettere il certificato digitale qualificato richiesto dal Richiedente, previa sottoscrizione, da parte di quest'ultimo, delle Condizioni Generali di Contratto per la fornitura dei servizi fiduciari qualificati.

#### *3.2.2.5. Procedura di identificazione tramite firma digitale rilasciata da altro QTSP*

La seguente procedura di identificazione consente al Richiedente di identificarsi in maniera certa mediante l'utilizzo di certificati qualificati rilasciati da altri prestatori di servizi, in conformità al Regolamento eIDAS.
In questo caso, il Richiedente è stato già previamente identificato da un prestatore di servizi fiduciari qualificato, che ha rilasciato il certificato digitale e utilizzerà quest'ultimo, se ancora in corso di validità, per firmare il modulo di richiesta di emissione del certificato qualificato da parte di Uanataca.
Ricevuta la richiesta di emissione, sottoscritta digitalmente da parte del Richiedente, Uanataca effettuerà adeguati controlli al fine di verificare la validità del certificato utilizzato per la firma riservandosi di rifiutare la richiesta di emissione in caso di esito negativo di questa.

#### *3.2.2.6. Procedura di identificazione tramite identità SPID*

Ai sensi dell'art. 64 co. 2-bis del Codice dell'Amministrazione Digitale "*per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)*".
Il Richiedente, che sia in possesso di credenziali di autenticazione tramite SPID (di livello 2 o superiore), potrà richiedere a Uanataca previa accettazione, da parte di quest'ultimo, delle Condizioni Generali di Contratto, l'emissione di certificati digitali qualificati senza effettuare una nuova procedura di identificazione secondo le norme del presente Manuale.

In tali casi, infatti, l'identità del Richiedente è già stata previamente accertata da uno dei Fornitori dell'Identità Digitale SPID accreditato dall'Agenzia per l'Italia Digitale, per la gestione dell'identità digitale dei propri utenti.

In ogni caso, Uanataca, si riserva la facoltà di rifiutare le richieste di emissione qualora, a seguito di adeguate verifiche, risultino incongruenze tra i dati identificativi forniti dal Richiedente al momento della richiesta di emissione del certificato e quelli risultanti dall'identità digitale SPID da questo utilizzata.

### *3.2.3. 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 3.2.2. 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.

(N.B. le disposizioni di cui al presente paragrafo non si applicano con riferimento al riconoscimento dei Richiedenti finalizzata all'emissione dei certificati di CNS i quali, in conformità con la normativa applicabile, possono essere rilasciati solo alle persone fisiche).

### *3.2.4. Misure anticontraffazione*

Al fine di prevenire il verificarsi di ogni possibile furto di identità (mediante impersonificazione *totale* o *parziale*) Uanataca 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. 3.2.2.1. e ss.).

In particolare, la verifica dell'identità dei Richiedenti è attuata mediante:

a) adeguata formazione degli operatori deputati allo svolgimento delle attività di identificazione dei Richiedenti (con particolare riferimento alla verifica della genuinità dei documenti di identità presentati in occasione delle operazioni di riconoscimento);
b) utilizzo di piattaforme e portali di fonti autoritative per il riscontro dei dati contenuti all'interno dei documenti di identità e delle tessere sanitarie utilizzate dai Richiedenti nella fase di identificazione. A titolo esemplificativo e non esaustivo:
    1. verifica dell'esattezza del codice fiscale (e/o della Partita Iva in caso di persona giuridica) dei Richiedenti attraverso l'interrogazione del servizio on-line messo a disposizione dall'Agenzia delle Entrate;
    2. verifica dei dati contenuti all'interno dei documenti di identità presentati dai Richiedenti attraverso l'utilizzo della piattaforma *SCIPAFI* ("*Sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con*

*specifico riferimento al furto di identità*") gestita da Consap S.p.a. e di titolarità del Ministero dell'Economia e delle Finanze.

Uanataca si riserva il diritto di adottare ulteriori e più adeguate misure di verifica dell'identità dei Richiedenti con l'esclusivo fine di prevenire il cd. *furto di identità* inteso nelle seguenti duplici accezioni:

- **Impersonificazione totale**: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità di un altro soggetto;
- **Impersonificazione parziale**: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto.

### 3.2.5. Informazioni non verificate

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

### 3.2.6. Autorizzazione di un Ufficio di Registrazione e dei suoi Operatori

Per la costituzione di un nuovo Ufficio di Registrazione (RA), Uanataca effettua le necessarie verifiche per confermare l'esistenza dell'entità o dell'organizzazione in questione. A tal fine, Uanataca potrà utilizzare i documenti presentati o le proprie fonti di informazione.

Allo stesso modo, Uanataca verifica e convalida l'identità degli Operatori delle R.A., per i quali, queste ultime, inviano a Uanataca la documentazione di identificazione, unitamente alla loro autorizzazione ad agire come tale. Uanataca garantisce che gli Operatori delle R.A. ricevano una formazione adeguata al corretto svolgimento delle loro attività, formazione che verrà confermata attraverso una corrispondente valutazione. Tale formazione e valutazione possono essere eseguite anche dalla R.A. precedentemente autorizzata da Uanataca.

Per la prestazione dei servizi oggetto del presente Manuale, Uanataca garantisce che gli operatori delle R.A. accedano al sistema tramite un'autenticazione sicura con certificati digitali.

## 3.3. Identificazione e autenticazione per le richieste di rinnovo

### 3.3.1. Rinnovo periodico dei certificati

La procedura di identificazione ed autenticazione nei casi in cui sia richiesto il rinnovo dei certificati qualificati si svolge in maniera più semplice rispetto a quella relativa alla richiesta di prima emissione.

Prima di rinnovare un certificato, l'Operatore o gli Operatori autorizzati dalla R.A. di Uanataca verificano che le informazioni utilizzate per l'identificazione del Richiedente e/o del Titolare continuino ad essere valide e non abbiano subito cambiamenti.

I metodi per effettuare tale verifica sono:

- l'utilizzo del codice riservato di emergenza ("*codice utente*") relativo al certificato precedente, o di altri mezzi di autenticazione personale, che consistono in informazioni note solo alla persona fisica identificata nel certificato e che consentono di riemettere automaticamente il certificato, a condizione che il periodo massimo stabilito dalla legge non sia stato superato;
- l'uso dell'attuale certificato, purché quest'ultimo non abbia superato il periodo massimo stabilito dalla legge per il rinnovo.

Se le informazioni del Richiedente o del Titolare identificato nel certificato hanno subito variazioni, le nuove informazioni verranno correttamente registrate e sarà effettuata un'identificazione completa, conformemente alle disposizioni della sezione 3.

### *3.3.2. Richieste di rinnovo dopo la revoca*

Nel caso in cui sia richiesto un rinnovo del certificato dopo la sua revoca è necessario, per il Richiedente, ripetere la procedura di validazione dell'identità di cui al par. 3.2.2.

Prima di generare un certificato per un Titolare il cui certificato precedente sia stato revocato, l'operatore o il personale autorizzato da una R.A. di Uanataca verificherà che le informazioni utilizzate per validare l'identità e le ulteriori informazioni del Richiedente e/o del Titolare siano valide, in quel caso si applicheranno le disposizioni della sezione precedente.

Dopo la revoca del certificato non sarà possibile procedere alla sua riattivazione ma sarà possibile unicamente procedere alla ri-emissione di un nuovo certificato (intesa quale nuova emissione).

Se le informazioni del Richiedente (o del Titolare) identificato nel certificato hanno subito variazioni, le nuove informazioni verranno correttamente registrate e sarà effettuata un'identificazione completa, conformemente alle disposizioni della sezione 3.

## *3.4. Identificazione e autenticazione per le richieste di revoca*

Uanataca o il personale autorizzato dalla R.A., 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 dei certificati può essere effettuata:

- dal Richiedente e/o il Titolare:
  - tramite l'uso del codice di revoca ERC attraverso il sito Web di Uanataca https://www.uanataca.com/lcm/ disponibile 7 giorni su 7 e 24 ore su 24;
  - con altri mezzi di comunicazione, come il telefono, l'e-mail, ecc. quando vi sono ragionevoli garanzie sull'identità del Richiedente in merito alla revoca, secondo il giudizio di Uanataca e/o delle R.A.
- dalle R.A.: queste devono identificare il Titolare prima di approvare una richiesta di revoca in base ai mezzi che ritengono necessari.

In tutte le ipotesi in cui sussistano dei dubi sull'identità del Richiedente il certificato entrerà in stato di sospensione.

# 4. REQUISITI OPERATIVI RELATIVI AL CICLO DI VITA DEI CERTIFICATI

## 4.1. Domanda di emissione del certificato

### 4.1.1. Legittimazione della richiesta

Il Richiedente è tenuto ad accettare e sottoscrivere la documentazione contrattuale predisposta da Uanataca.

### 4.1.2. Procedure e responsabilità

Uanataca riceve le richieste di certificati: tali richieste vengono inoltrate tramite un modulo, in formato cartaceo o digitale, singolarmente o in lotti, o collegandosi a database esterni o tramite appositi servizi Web predisposti da Uanataca.

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 allegare un indirizzo fisico o altri dati che consentano di contattare la persona fisica/giuridica identificata nel certificato.

## 4.2. Elaborazione della richiesta

### 4.2.1. Svolgimento delle funzioni di identificazione ed autenticazione

Ricevuta una richiesta di emissione di un certificato qualificato, Uanataca verifica che quest'ultima sia completa, accurata e debitamente autorizzata, prima di elaborarla.

In caso di esito positivo, Uanataca analizza le informazioni fornite, verificandone la compatibilità con gli aspetti descritti nella sezione 3.

Nel caso di un certificato qualificato, la documentazione comprovante l'approvazione della richiesta deve essere conservata e debitamente registrata e con garanzie di sicurezza e integrità per un periodo di 20 anni dalla data di scadenza del certificato, anche in caso di perdita anticipata della validità del certificato dovuta alla sua revoca.

### 4.2.2. Approvazione o rifiuto della richiesta

Nel caso in cui la verifica dei dati forniti abbia esito positivo, Uanataca approverà la richiesta di certificato e procederà alla sua emissione e consegna.

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, Uanataca rigetterà la richiesta o interromperà la sua approvazione fino a quando non avrà effettuato i controlli che riterrà necessari.

Se, a seguito dell'ulteriore verifica, dovesse risultare che le informazioni fornite non sono corrette, Uanataca rifiuterà definitivamente la richiesta.
Uanataca notificherà al Richiedente l'approvazione o il rifiuto della richiesta.
Uanataca sarà in grado di automatizzare le procedure che permettono di verificare la correttezza delle informazioni contenute nei certificati e i processi di approvazione delle domande.

### 4.2.3. Termine per l'elaborazione della richiesta

Uanataca 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.

## 4.3. Emissione del certificato

### 4.3.1. Processo di emissione

A seguito dell'approvazione della richiesta, il certificato viene generato in modo sicuro e reso disponibile al Titolare per l'accettazione.
Le procedure stabilite in questa sezione si applicano anche in caso di rinnovo dei certificati, poiché quest'ultimo implica, comunque, l'emissione di un nuovo certificato.
Durante il processo di emissione Uanataca:

- garantisce la riservatezza e l'integrità dei dati di registrazione forniti;
- 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;
- produce una coppia di chiavi, tramite una procedura sicura di generazione;
- implementa un processo di generazione di certificati che collega in modo sicuro il certificato alle informazioni di registrazione, inclusa la chiave pubblica certificata;
- 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;
- indica la data e l'ora in cui è stato emesso un certificato;
- garantisce il controllo esclusivo delle chiavi da parte dell'utente, di modo che terzi non possano detrarle o utilizzarle in alcun modo.

### 4.3.2. Emissione del certificato di TSU

La richiesta di certificato viene eseguita manualmente da due operatori di sistema che operano per conto di Uanataca e sono coinvolti nel processo di conduzione tecnica dei sistemi.

- Un operatore di sistema provvede alla generazione di una coppia di chiavi sulla partizione dell'HSM preposta al servizio di marcatura temporale. A seguire, genera il CSR (*Certificate Signing Request*) in formato PKCS#10 e la salva su un dispositivo fisico (es. CD-ROM, Pen

Drive). Detto dispositivo viene in fine passato ad un altro operatore di sistema preposto all'emissione del certificato.

- Quest'ultimo operatore, ricevuto il supporto fisico, procede all'emissione del certificato di TSU utilizzando un apposito software di CA che permette la firma del certificato con le chiavi di TSA. Il certificato così generato viene infine salvato su un supporto fisico (ove possibile, lo stesso del punto precedente) e restituito al primo operatore che finalizza il processo con l'installazione del certificato sull'HSM e con la configurazione opportuna del servizio di marca temporale.

In conformità alle disposizioni di cui all'art. 49 co. 3 del DPCM 22 febbraio 2013, una volta emesso il certificato di marcatura temporale, le chiavi di marcatura temporale sono sostituite ed emesso un nuovo certificato entro il termine massimo di n 3 (tre) mesi dall'emissione, al fine di limitare il numero di marche temporali generate con la medesima coppia: tale procedura è seguita da Uanataca indipendentemente dal periodo di validità del certificato di TSU.

### *4.3.3. Notifica di emissione del certificato*

Uanataca notifica l'emissione del certificato al Richiedente agli indirizzi da quest'ultimo forniti.

## *4.4. Consegna e accettazione del certificato*

### *4.4.1. Responsabilità della R.A.*

Il personale autorizzato dalla R.A. di Uanataca è tenuto a:

- verificare correttamente l'identità della persona fisica/giuridica identificata nel certificato, in conformità con le disposizioni delle sezioni 3;
- notificare l'emissione del certificato al Titolare, rendendo noto a quest'ultimo, almeno le seguenti informazioni:
  a) le informazioni di base sull'uso del certificato, il Manuale Operativo applicabile, i dati relativi alla CA, così come i suoi obblighi, facoltà e responsabilità;
  b) le informazioni sul certificato;
  c) evidenza della ricezione e accettazione da parte del Titolare dei dati associati all'uso del certificato;
  d) gli obblighi e responsabilità del Titolare;
  e) il metodo con cui viene garantito il controllo esclusivo, da parte del Titolare, della propria chiave privata o dei dati di attivazione della stessa secondo quanto stabilito nella sezione 6;
  f) la data dell'atto di consegna e accettazione del certificato.
- ottenere la firma del Richiedente così come identificato nel certificato.

Le R.A. sono responsabili dell'esecuzione di tali processi, sono tenute a conservare i documenti originali (fogli di consegna e accettazione), per le ipotesi in cui Uanataca abbia bisogno di accedervi e ad inviare una copia in formato digitale all'Organismo di vigilanza.
Tutti di documenti sopra indicati saranno conservati e archiviati, anche in formato elettronico, da Uanataca con garanzie di sicurezza e integrità per un periodo di almeno 20 anni decorrenti dalla data di scadenza del certificato di firma (ex art. 28 co. 4-bis D.Lgs. 7 marzo 2005 n. 82 e s.m.i.), anche al fine di fornire prova della certificazione in eventuali procedimenti dell'Autorità Giudiziaria e, comunque, non oltre il periodo stabilito dalla legge.

### *4.4.2. Processo di accettazione del certificato*

L'accettazione del certificato da parte della persona fisica o della persona giuridica identificata nel certificato viene effettuata firmando il modulo di consegna e accettazione.

### *4.4.3. Notifica dell'emissione a terzi*

Uanataca non notificherà alcuna emissione del certificato a favore di terzi diversi dal titolare.

## *4.5. Uso della coppia di chiavi e del certificato*

### *4.5.1. Utilizzo da parte del Richiedente e/o Titolare*

Il Titolare del certificato 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 ricevuti dalla CA;
- 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, controllare attentamente che il corrispondente certificato ottenuto da Uanataca abbia il profilo previsto e contenga informazioni corrette, incluse le eventuali limitazioni d'uso;
- fino alla data di scadenza o di eventuale revoca del proprio certificato, informare prontamente la CA o la RA nel caso in cui: il proprio dispositivo di firma sia andato perso, sia stato sottratto o si sia danneggiato; abbia perso il controllo esclusivo della propria

chiave privata, per esempio a causa della compromissione dei dati di attivazione (PIN o password) della propria chiave privata di firma; alcune informazioni contenute nel certificato siano inesatte o non più valide;

- nel caso di compromissione della propria chiave privata (per esempio, a causa dello smarrimento del PIN o della sua rivelazione a terzi non autorizzata), cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata: in tale situazione la C.A. revoca immediatamente il certificato.

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;
- 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.

### *4.5.2. Utilizzo da parte delle Relying Parties*

#### *4.5.2.1. 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;
- prendere qualsiasi precauzione così come prescritto negli accordi o altrove;

All'interno dell'Allegato "A" al presente Manuale è presente il link, insieme al relativo manuale, dell'applicativo messo a disposizione da Uanataca 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.

#### 4.5.2.2. 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.

## 4.6. Rinnovo di chiavi e certificati

### 4.6.1. Cause di rinnovo di chiavi e certificati

I certificati di firma o di sigillo elettronico non ancora scaduti e non revocati possono essere rinnovati attraverso una procedura specifica e semplificata.

Questa consiste nella generazione di una nuova coppia di chiavi (da parte del Richiedente attraverso appositi strumenti messi a disposizione da Uanataca) ed emissione di un nuovo certificato con

- periodo di validità uguale al periodo di validità del certificato in scadenza
- con gli stessi dati identificativi del Titolare.

Il rinnovo non richiede una nuova identificazione del Titolare e pertanto può essere condotto in autonomia anche da quest'ultimo attraverso l'utilizzo di appositi software messi a disposizione da Uanataca.

### 4.6.2. Procedura di rinnovo

Il Richiedente può richiedere un rinnovo del certificato nel caso in cui i dati identificativi non siano cambiati o, comunque, nel caso in cui il ciclo di vita del certificato è prossimo alla scadenza.

La procedura di rinnovo consta dei seguenti passaggi:

- il Richiedente invia alla CA richiesta di rinnovo autenticata con firma elettronica avanzata, generata con la chiave privata della coppia di chiavi da rinnovare, così da consentire a quest'ultima la verifica dell'identità del Richiedente;
- l'Operatore o gli Operatori autorizzati dalla R.A. di Uanataca verificano che le informazioni fornite durante l'identificazione del Richiedente e/o del Titolare continuino ad essere valide e non abbiano subito cambiamenti.

Qualora, nel Certificato qualificato, dovessero essere presenti anche informazioni relative al Ruolo e all'Organizzazione cui il Richiedente fa parte, la CA provvederà ad inserirle nel nuovo certificato verificando, al momento del rinnovo, che non sia pervenuta la revoca del certificato dal Terzo Interessato.

In questi casi la CA, oltre a verificare eventuali casi di revoca del certificato a causa di violazioni della sicurezza, è tenuta a verificare l'esistenza e la validità del certificato da rinnovare nonché la validità delle informazioni utilizzate per l'identificazione del titolare.
L'avvenuto rinnovo del certificato sarà notificato a cura della CA al Richiedente mediante posta elettronica all'ultimo indirizzo e-mail comunicato.
Il Richiedente che abbia ricevuto il nuovo certificato non potrà più utilizzare la Chiave privata relativa al vecchio certificato.
Una volta scaduto o revocato, il certificato non può più essere riemesso ma è necessaria una emissione *ex novo* del certificato con le medesime modalità descritte per l'emissione del primo (v. par. 4.1, 4.2 e 4.3).

## 4.7. Key Changeover (re-key dei certificati)

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

## 4.8. Modifica dei certificati

La modifica dei certificati, 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 ex novo, applicando quanto descritto nella sezione 4.

## 4.9. Revoca e sospensione di un certificato

La revoca e la sospensione di un certificato 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 revoca o sospensione del certificato si materializzano 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 Uanataca per consentire agli interessati la consultazione necessaria alla determinazione dello stato di validità dei certificati emessi da Uanataca.
Con la stessa finalità, Uanataca rende disponibile la stessa informazione mediante il protocollo OCSP.

### 4.9.1. Ipotesi di revoca di un certificato

Uanataca revoca un certificato 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.

3. **circostanze che riguardino 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) 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 Uanataca;
   b) utilizzo del certificato non conforme e pregiudizievole per Uanataca, specie in modo continuativo;
   c) provvedimento dell'Autorità giudiziaria.

In questo caso, 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.

### 4.9.2. Chi può richiedere la revoca

Può domandare la revoca del certificato il Richiedente e i soggetti indicati al Par. 4.9.1., n. 3 lett. f) attraverso l'intervento dell'Operatore di registrazione con le modalità appresso indicate, oltre che da Uanataca 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.

### 4.9.3. Procedura di revoca

Il soggetto che richiede la revoca di un certificato può farlo rivolgendosi direttamente a Uanataca ovvero alla R.A. ovvero, in prima persona, attraverso il servizio online disponibile sulla pagina web di Uanataca. La richiesta di revoca dovrà includere le informazioni seguenti:

- data della richiesta di revoca;
- dati identificativi del Richiedente;
- recapiti della persona che chiede la revoca;
- motivazione dettagliata relativa alla richiesta di revoca.

Prima di procedere alla revoca, la richiesta deve essere validata da Uanataca, in accordo con i requisiti stabiliti nel paragrafo 3 di questo Manuale.
Il servizio di revoca è disponibile al sito web di Uanataca all'indirizzo https://www.uanataca.com/lcm/.
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 Uanataca.

### 4.9.4. Periodo di grazia della richiesta di revoca

Uanataca 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.

### 4.9.5. Durata dell'elaborazione della richiesta di revoca

Se effettuata per mezzo di un Operatore, la richiesta di revoca sarà elaborata entro il consueto orario d'ufficio di Uanataca o laddove applicabile dalla R.A. che ha proceduto all'emissione del certificato. Se effettuata online, avrà effetto immediato.
In caso di ricezione da parte di Uanataca 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.

### 4.9.6. 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 Uanataca.

Le Liste di Revoca dei Certificati sono pubblicate ai seguenti indirizzi (URL):

- http://crl1.uanataca.com/public/pki/crl/uanataca_it.crl
- http://crl2.uanataca.com/public/pki/crl/uanataca_it.crl

I suddetti indirizzi sono riportati in ciascuno dei certificati emessi da Uanataca, nella sezione "CRL Distribution Point".

La verifica, inoltre, può essere compiuta mediante interrogazione del servizio OCSP erogato da Uanataca ai seguenti indirizzi:

- http://ocsp1.uanataca.com/public/pki/ocsp/;
- http://ocsp2.uanataca.com/public/pki/ocsp/.

### 4.9.7. Frequenza di emissione della CRL

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

### 4.9.8. 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.

### 4.9.9. Disponibilità dei servizi di verifica on-line della revoca

Uanataca 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, Uanataca 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.

### 4.9.10. Altre forme disponibili di pubblicazione della revoca

Non è prevista nessuna ulteriore modalità di pubblicazione della revoca a parte di quelle previste nella sezione 4.9.

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

Non previste.

### 4.9.12. Circostanze per la sospensione

La sospensione del certificato di firma elettronica qualificata 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.

### 4.9.13. Chi può richiedere la sospensione

Può domandare la sospensione del certificato il Richiedente e i soggetti indicati al Par. 4.9.1., n. 3 lett. f) attraverso l'intervento dell'Operatore di registrazione con le modalità appresso indicate, oltre che da Uanataca laddove venisse ravvisata detta necessità.

### 4.9.14. 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, Uanataca 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, Uanataca 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 4.9.3.

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. 5.4.2. e ss.)

## 4.10. Servizi informativi sullo stato del certificato

Lo stato dei certificati qualificati è messo a disposizione attraverso la pubblicazione della CRL mediante protocollo HTTP 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.

## 4.11. Cessazione del contratto

Il contratto tra la CA e il Titolare si intende cessato alla scadenza o alla revoca del certificato, salvo il caso di eventuali condizioni diverse previste nei contratti stipulati con alcuni clienti.
Il rinnovo del certificato determina la continuità della prestazione contrattuale da parte della CA.

## 4.12. Key escrow e recupero della chiave privata

### 4.12.1. 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.

### 4.12.2. Politica e servizi sui contenuti e recupero chiavi di sessione

Nessuna disposizione

# 5. MISURE DI SICUREZZA FISICA E OPERATIVA

## 5.1. Sicurezza fisica

Uanataca 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.

Uanataca si avvale dei servizi di data center e servizi di comunicazione associati (quali *housing*, connettività alla rete Internet, sicurezza fisica) offerti dalla società ADAM con la quale ha stipulato apposito contratto di servizio.

Detti servizi sono certificati secondo le norme:

- ISO/IEC 27001:2017

- ISO 9001:2015

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

### 5.1.1. 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.
Uanataca dispone di strutture che proteggono fisicamente gli ambienti in cui vengono effettuate le operazioni proprie dell'erogazione di servizi fiduciari.

### 5.1.2. Accesso fisico

I Fornitori 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 Uanataca ovvero del Responsabile della Sicurezza.
Uanataca 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.

### 5.1.3. 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.

### 5.1.4. 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.

### 5.1.5. Prevenzione e protezione antincendio

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

### 5.1.6. 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.

### 5.1.7. 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.

### 5.1.8. Copia di riserva esterna alle strutture

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

## 5.2. Controlli sulle procedure e sicurezza operativa

Uanataca 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 Uanataca esegue le procedure amministrative e di gestione in accordo con la politica di sicurezza stabilita da Uanataca.

### 5.2.1. 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, Uanataca ha stabilito i seguenti incarichi o ruoli di fiducia:

- **Responsabile della sicurezza**: incaricato di coordinare, controllare e far applicare le misure di sicurezza definite nella politica sulla sicurezza di Uanataca. Questi deve incaricarsi degli aspetti relativi alla sicurezza dell'informazione: logistica, fisica, di rete, organizzativa, etc.;
- **Responsabile delle verifiche e delle ispezioni (auditing)**: responsabile dello svolgimento delle procedure operative. È inoltre responsabile della verifica degli archivi e dei log di audit dei sistemi di CA;

- **Responsabile della conduzione tecnica dei sistemi**: responsabile dell''installazione, della configurazione, della manutenzione e del corretto funzionamento dei sistemi preposti all'erogazione dei servizi fiduciari;
- **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;

**Operatore di registrazione**: responsabile dell'approvazione delle richieste di emissione di un certificato inoltrate dal Richiedente e/o Titolare; responsabile della verifica delle informazioni necessarie e dell'applicazione delle procedure definite da Uanataca per l'emissione di certificati digitali ovvero per l'erogazione di 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 Uanataca, costituisce una misura atta a prevenire la commissione di attività fraudolente.

### *5.2.2. Numero di persone per attività*

Uanataca, 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.

### *5.2.3. 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.

### *5.2.4. 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.

### *5.2.5. 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.

## *5.3. Sicurezza del personale*

### *5.3.1. Qualifica, esperienza ed autorizzazioni richieste*

Il personale di Uanataca, analogamente a quello di propri partner tecnologici, 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.

Uanataca 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 Uanataca 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.

Uanataca 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.

In ogni caso, le R.A., essendo responsabili delle persone da esse autorizzate allo svolgimento delle attività che gli sono normalmente proprie, potranno stabilire procedure ulteriori per l'accertamento dei requisiti di cui sopra, sempre nel rispetto della politica di Uanataca.

### 5.3.2. Procedure di verifica delle informazioni relative al personale

Uanataca, 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.

Uanataca ottiene, preliminarmente allo svolgimento di tali accertamenti, il consenso espresso dell'interessato, impegnandosi a trattare e proteggere 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.

### 5.3.3. Requisiti di formazione

Uanataca 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 Uanataca;
- 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.

### 5.3.4. Requisiti e frequenza dei corsi di aggiornamento

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

### 5.3.5. Rotazione delle mansioni

Non applicabile.

### 5.3.6. Sanzioni per azioni non autorizzate

Uanataca 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.

### 5.3.7. 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 Uanataca. 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.

### 5.3.8. 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.

## 5.4. Procedure di controllo per la sicurezza

### 5.4.1. Tipi di incidente registrati

Uanataca 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;
- 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 databases 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.

### 5.4.2. Frequenza di elaborazione del giornale di controllo

Uanataca 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.

Uanataca 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.

### 5.4.3. Periodo di conservazione del giornale di controllo

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

### 5.4.4. 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.

### 5.4.5. Procedure di backup

Uanataca 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.
Uanataca 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.

### 5.4.6. 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 da Uanataca.
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).

### 5.4.7. Notifica in caso di evento sospetto

Nessuna disposizione.

### 5.4.8. Analisi di vulnerabilità

Le analisi di potenziali vulnerabilità dell'infrastruttura di Uanataca 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.

## 5.5. Archiviazione delle informazioni

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

### 5.5.1. Tipologie di documenti archiviati

I seguenti documenti coinvolti nel ciclo di vita del certificato sono archiviati da Uanataca (o dalle R.A.):

- tutti i dati di controllo del sistema;
- tutti i dati relativi ai certificati, compresi i contratti con i Titolari e i dati relativi alla loro identificazione e localizzazione;
- richieste di emissione e revoca dei certificati;
- tipologia di documento presentato al momento della richiesta di certificato;
- identità della R.A. che accetta la richiesta di certificato;
- tutti i certificati emessi o pubblicati;
- CRL emesse;
- log inerenti lo stato dei certificati;
- storico delle chiavi generate;
- comunicazioni tra gli elementi della PKI;
- politiche e pratiche di certificazione;
- informazioni sulle richieste di certificazione;
- documentazione fornita per giustificare le richieste di certificazione;
- informazioni sul ciclo di vita del certificato.

Uanataca e/o le R.A., a seconda dei casi, saranno responsabili della corretta archiviazione del materiale sopra indicato.

### 5.5.2. Periodo di archiviazione dei registri

Uanataca 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 o per il periodo stabilito dalla legislazione in vigore al momento della revoca.

### 5.5.3. Protezione degli archivi

Uanataca 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.

Uanataca garantisce la corretta protezione degli archivi grazie al personale qualificato che si occupa del trattamento e dell'archiviazione in strutture esterne sicure.

### 5.5.4. Procedure di back-up

Uanataca 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.

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

### *5.5.5. 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.

### *5.5.6. Localizzazione del sistema di archiviazione*

Uanataca dispone di un sistema centralizzato per raccogliere informazioni sull'attività del team coinvolto nel servizio di gestione dei certificati.

### *5.5.7. Procedure per ottenere e verificare le informazioni di archiviazione*

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

## *5.6. 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 Uanataca 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, Uanataca 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).

## 5.7. Compromissione delle chiavi e disaster recovery

### 5.7.1. Procedure di gestione degli incidenti e delle compromissioni

Uanataca, 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.

### 5.7.2. 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 Uanataca, che includono escalation, ricerca e risposta alla criticità. Se necessario, verrà avviata la procedura di compromissione della chiave o di disaster recovery di Uanataca.

### 5.7.3. Compromissione della chiave privata della CA

In caso di sospetto o accertamento della compromissione da parte di Uanataca, 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.

### 5.7.4. Continuità operativa dopo una criticità

Uanataca 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 Uanataca, 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.

Uanataca 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.

Uanataca 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 dell'azienda Bit4id S.r.l in Napoli alla via Diocleziano n. 107.

## 5.8. Cessazione del servizio

Uanataca assicura ai Richiedenti e/o Titolari 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, Uanataca garantisce una manutenzione continua dei registri per il tempo stabilito nella sezione 5 del presente Manuale Operativo.

Tuttavia, Uanataca 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, Uanataca ha sviluppato un piano di cessazione dell'attività, con le seguenti disposizioni:

- fornirà 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 ad Autorità subordinate 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 Uanataca, nonché qualsiasi altra circostanza rilevante che possa impedire il proseguimento dell'attività.

# 6. MISURE DI SICUREZZA TECNICA

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

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

## 6.1. Generazione e installazione della coppia di chiavi

### 6.1.1. Generazione della coppia di chiavi

#### 6.1.1.1. 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 Uanataca.

Per la generazione delle chiavi sono stati utilizzati dispositivi HSM conformi FIPS 140-2 livello 3 e Common Criteria EAL4 +.

| **UANATACA Qualified eIDAS CA 2020** | **4.096 bits** | **20 anni** |
|---|---|---|
| - Certificati di entità finale | 2.048 bits | Fino a 3 anni |
| **UANATACA Qualified TSA 2020** | **4.096 bits** | **20 anni** |
| Certificati di Time Stamping Unit | 2.048 bits | Fino a 8 anni |
| **UANATACA CNS CA 2020** | **4.096 bits** | **20 anni** |
| - Certificati di entità finale | 2.048 bits | Fino a 6 anni |

#### 6.1.1.2. 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 ETSI TS 119 312.
In particolare, le chiavi vengono generate utilizzando l'algoritmo a chiave pubblica RSA, con una lunghezza minima di 2048 bit, in ottemperanza a quanto previsto dall'art. 24, paragrafo 2, lettera e) del Regolamento eIDAS.

#### *6.1.1.3. Chiavi di TSU*

Le chiavi di TSU sono generate in un ambiente fisicamente protetto, in conformità con le procedure interne di Uanataca relative ai sistemi di marcatura temporale.
L'esecuzione di tali attività avviene in presenza dell'auditor interno ed è documentata in un 'apposito verbale.
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+.

### *6.1.2. 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.

### *6.1.3. Distruzione della chiave pubblica della CA*

Le chiavi pubbliche di Uanataca 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 https://web.uanataca.com/it/certificati-della-ca e attraverso la pubblicazione sulla Trust-service Status List (TSL) effettuata dall'Organismo di Supervisione Nazionale (AgID).

### *6.1.4. 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.

### 6.1.5. 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.

### 6.1.6. Controllo di qualità dei parametri della chiave pubblica

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

### 6.1.7. Generazione delle chiavi in applicazioni informatiche o in beni strumentali

Tutte le chiavi si generano con strumenti e procedure, in conformità con quanto indicato nella sezione 6.

### 6.1.8. 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*).

## 6.2. Protezione delle chiavi private e sicurezza moduli

### 6.2.1. Standard e sicurezza dei moduli crittografici

In relazione ai moduli che gestiscono le chiavi di Uanataca, 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.

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

È richiesto un controllo composto da più persone per l'attivazione della chiave privata della CA e della TSA.

Nel caso della chiave privata della CA e della TSA di Uanataca, 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.

### 6.2.3. Ripristino della chiave privata

Non consentito.

### 6.2.4. Backup della chiave privata

Uanataca 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.

### 6.2.5. 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 Uanataca S.A.
Uanataca 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.

### 6.2.6. Trasferimento della chiave privata tra moduli crittografici

Le chiavi private vengono generate direttamente nei moduli crittografici di produzione di Uanataca.
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.

### 6.2.7. 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.

### 6.2.8. Modalità di attivazione della chiave privata

La chiave privata di Uanataca 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.

### 6.2.9. 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 Uanataca 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.

#### *6.2.10. Modalità di disattivazione della chiave privata*

Non prevista.

#### *6.2.11. Classificazione dei moduli crittografici*

Vedere il paragrafo 6.1.

### *6.3. Altri aspetti della gestione della coppia di chiavi*

#### *6.3.1. Archiviazione della chiave pubblica*

Secondo quanto stabilito nel paragrafo 5 del presente Manuale.

#### *6.3.2. 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.

### *6.4. Dati di attivazione*

#### *6.4.1. Generazione dei dati di attivazione*

I dati di attivazione dei dispositivi che proteggono le chiavi private di CA e di TSA di Uanataca 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, Uanataca genera i dati di attivazione in modo sicuro.

#### *6.4.2. 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.

## 6.5. Controlli di sicurezza informatica

Uanataca utilizza sistemi affidabili per offrire i servizi di certificazione.

Uanataca 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, Uanataca 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.

### 6.5.1. Requisiti tecnici specifici per la sicurezza informatica

Ogni server impiegato da Uanataca 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.

### 6.5.2. Valutazione del livello di sicurezza informatica

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

## 6.6. Controlli tecnici del ciclo di vita

### 6.6.1. 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.

### 6.6.2. Controlli di gestione della sicurezza

Uanataca 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.
Uanataca 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.

## 6.7. 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.

## 6.8. 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 Uanataca sono realizzate in moduli con certificazioni FIPS 140-2 livello 3.

## 6.9. Riferimento temporale

Uanataca 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.

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

Uanataca 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 (UE) n. 910/2014.

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), Uanataca procederà come descritto di seguito:

1. Uanataca 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, Uanataca 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, Uanataca 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, Uanataca 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.

# 7. PROFILO DEI CERTIFICATI, CRL, OCSP

## 7.1. 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 Uanataca.

### 7.1.1. 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 Uanataca (https://web.uanataca.com/it/politiche-di-certificazione).

### 7.1.2. 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.

### 7.1.3. 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.

### 7.1.4. OID (Object Identifier)

Come previsto nel par. 1.2.1., ciascun profilo di certificato, emesso secondo questo Manuale, è identificato da uno specifico OID (*Object Identifier*).

## 7.2. Profilo delle CLR

Le CLR emesse da Uanataca sono conformi alla specifica pubblica RFC 5280.

### 7.2.1. Numero di versione

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

## 7.3. Profilo OCSP

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

# 8. AUDIT DI CONFORMITÀ

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

## 8.1. Frequenza degli audit

Con frequenza annuale, un Organismo di Valutazione accreditato (Conformity Assessment Body, CAB) provvede a verificare la conformità dei servizi CA di Uanataca al presente Manuale, al Regolamento (UE) n. 910/2014 e agli standard ETSI applicabili.

Sempre su base annuale, relativamente ai servizi di certificazione digitale, Uanataca 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.

## 8.2. 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.

## 8.3. Relazione tra la CA e gli auditor

Tra l'Organismo di Valutazione (CAB) e Uanataca 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 Uanataca.

## 8.4. 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 Uanataca 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 e delle RA;
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 norma ETSI EN 19 401 (REQ-7.13-03), è anche l'accessibilità dei servizi fiduciari da parte di persone con disabilità.

Considerando il contesto dell'Organizzazione ed il fatto che i servizi fiduciari emessi da Uanataca sono destinati principalmente a personale sanitario e amministrativo, il requisito di accessibilità dei servizi non è considerato strettamente necessario per l'erogazione degli stessi ai soggetti interessati.

## 8.5. Azioni successive alle non-conformità

Ricevuto il report, la Direzione Aziendale provvede ad esaminare, con la collaborazione dell'OdV, 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.

## 8.6. Comunicazione dei risultati

L'Organismo di Valutazione (OdV) comunica il risultato dell'attività di auditing alla Direzione Aziendale di Uanataca.

Il report prodotto dall'OdV, inoltre, viene trasmesso all'Organismo nazionale di Supervisione.

# 9. CONDIZIONI ECONOMICHE E LEGALI

## 9.1. Tariffe

### 9.1.1. Tariffe per l'emissione o rinnovo del certificato

Uanataca ha stabilito tariffe specifiche per l'emissione e il rinnovo dei certificati richiesti dagli utenti: le tariffe massime sono indicate sul sito web di Uanataca https://web.uanataca.com/it/.
Tuttavia Uanataca si riserva la facoltà di modificare le tariffe per i servizi di certificazione erogati senza previa notifica agli utenti e di rinegoziare le condizioni economiche con i singoli clienti in ragione del volume richiesto.

### 9.1.2. Tariffa per l'accesso ai certificati

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

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

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

### 9.1.4. Tariffa per altri servizi

Nessuna condizione.

### 9.1.5. 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 Uanataca, della sua decisione di recedere dal contratto tramite una dichiarazione esplicita, ai recapiti di seguito forniti:

- Indirizzo sede secondaria:
  Uanataca S.A. unipersonale
  Via Diocleziano, 107
  80125 – Napoli

Per ulteriori contatti è possibile consultare il sito all'indirizzo https://web.uanataca.com/it/

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.

## 9.2. Capacità finanziaria

In relazione alla gestione dei servizi di CA e al piano di cessazione delle attività, Uanataca 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.

### 9.2.1. 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, Uanataca 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 €. 3.000.000,00 (tremilioni,00//).

### 9.2.2. Altri asset

Nessuna condizione.

### 9.2.3. Copertura assicurativa per gli utenti finali

Si rinvia al precedente paragrafo 9.2.1.

## 9.3. Tutela delle informazioni trattate

### 9.3.1. Informazioni confidenziali

Uanataca 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;
- contratti con le RA;

- 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 Uanataca nel rispetto delle norme applicabili, in particolare del D.lgs. 196/03 e s.m.i. e del 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).

### 9.3.2. 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.

### 9.3.3. Ipotesi di divulgazione delle informazioni

Uanataca non divulga le informazioni confidenziali di cui al paragrafo 9.3.1., salvo che tale circostanza non gli sia imposta da un obbligo giuridico/normativo di divulgazione dello Stato.

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.

Le circostanze che legittimano la divulgazione, da parte di Uanataca, delle informazioni confidenziali e, in particolare, dei dati personali dei soggetti richiedenti e/o titolari, verranno debitamente indicate nell'informativa sul trattamento dei dati personali predisposta e rilasciata dalla CA.

## 9.4. Trattamento e protezione dei dati personali

### 9.4.1. Informativa sulla Privacy

Il Regolamento Europeo (UE) n.679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) ha introdotto requisiti normativi innovativi per la protezione dei dati personali, con ricadute organizzative, operative e tecnologiche che riguardano i principali processi di gestione dei Dati all'interno delle strutture organizzative aziendali.

Il predetto Regolamento impone ai Titolari e Responsabili del trattamento un obbligo generale di adozione di misure tecnico-organizzative adeguate al rischio associato al trattamento dei dati (cfr. art. 32 del GDPR).

In conformità alle disposizioni di cui al GDPR in materia di tutela dei dati personali, Uanataca illustra, nel presente paragrafo, quali sono i Dati personali che acquisice, in che modo vengono trattati e per quale finalità nonché le procedure organizzative e di sicurezza che ha adottato al fine di garantire i dati personali trattati dal rischio di perdita, distruzione, falsificazione e trattamento illecito e/o non autorizzato.

Di seguito si esplica l'informativa ai sensi dell'art. 13 del GDPR:

**a) TITOLARE DEL TRATTAMENTO**

Uanataca S.A. unipersonale, società del gruppo Bit4 Group S.r.l., è il Titolare del Trattamento, ai sensi dell'art. 4, n. 7 del GDPR, di tutti i Dati Personali forniti dai Richiedenti relativamente alle finalità di cui al presente Manuale Operativo.

Per qualunque informazione inerente al Trattamento dei Dati Personali da parte di Uanataca S.A. unipersonale è possibile scrivere ai seguenti contatti:

**Uanataca S.A. unipersonale**

**Sede legale:** Calle Riera de Can Toda n. 24-26 (08024) Barcellona – Spagna

**Sede secondaria:** Via Diocleziano n. 107 (80125) Napoli - Italia

**Indirizzo di posta elettronica:** info.it@uanataca.com

**Numero di telefono:**

(IT) +39 081 7625600

(ES)+34 935 272290

Con riferimento alle sole attività di trattamento finalizzate all'emissione dei certificati di CNS, in conformità al Manuale Operativo, Uanataca opera, ai sensi dell'art. 26 del GDPR, in regime di contitolarità con il seguente soggetto:

**Università degli Studi di Napoli Parthenope**

**Sede Legale**: Via Amm. F. Acton 38 (80133) Napoli – Italia

**C.F./P.I.**: 01877320638

**b) RESPONSABILE/I DEL TRATTAMENTO**

Ai fini dell'espletamento delle attività inerenti il Trattamento dei Dati Personali, in conformità alla presente Informativa, Uanataca può avvalersi ai sensi dell'art. 28 co. 1 del GDPR, di soggetti terzi che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento GDPR e garantisca la tutela dei diritti dell'interessato.

Una lista completa dei Responsabili del Trattamento, ove presenti, nominati da Uanataca può essere richiesta a quest'ultima in qualsiasi momento, tramite contatto ad uno dei recapiti indicati al paragrafo precedente.

**c) RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD O DPO)**

Uanataca ha designato, ai sensi dell'art. 37 del GDPR un Responsabile della Protezione dei Dati Personali (R.P.D. o D.P.O. "*Data Protection Officer*") individuandolo tra quei soggetti che, ai sensi dell'art. 37 n. 5 della citata norma, posseggono le qualità professionali, i requisiti di conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati.

Il Responsabile della Protezione dei Dati di Uanataca, che è la figura incaricata della sorveglianza dell'osservanza del Regolamento GDPR, è disponibile per rispondere a tutte le richieste degli interessati su come i dati vengono trattati e può essere contattato presso la sede di Uanataca o direttamente al seguente indirizzo:

- Indirizzo di posta elettronica del DPO: dpo@uanataca.com.

Per l'individuazione dei ruoli e dei compiti del DPO si rimanda a quanto previsto dall'art. 39 del GDPR.

**d) MODALITÀ DI TRATTAMENTO DEI DATI**

I Dati Personali sono trattati in formato cartaceo ed elettronico nel rispetto delle misure organizzative e di sicurezza previste dalla legge applicabile e il relativo Trattamento sarà improntato al rispetto dei principi di correttezza, liceità, trasparenza, completezza limitazione delle finalità e della conservazione, non eccedenza, minimizzazione ed esattezza, integrità e riservatezza, nonché al principio di responsabilizzazione di cui all'art. 5 del GDPR così da garantire le più adeguate misure di sicurezza e ridurre i rischi di distruzione/perdita, accessi non autorizzati o trattamenti non conformi alle finalità descritte nel presente documento.

Tali trattamenti hanno luogo presso la sede di Uanataca e/o presso i Responsabili esterni che effettuano il trattamento secondo le istruzioni impartite da Uanataca.

**e) DATI PERSONALI TRATTATI**

Ai sensi dell'art. 4 n. 1 del GDPR s'intende per "*dato personale*": "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale* ".

Per "*Dati Personali*", dunque, devono intendersi tutte quelle informazioni o frammenti di informazioni che permettono l'identificazione di una persona fisica.

Al fine di dare esecuzione alle richieste di emissione di certificati digitali qualificati (di firma, sigillo), di Carta Nazionale dei Servizi e di Marche Temporali qualificate da parte dei Richiedenti nonché, nell'ambito del rapporto contrattuale con gli stessi, Uanataca tratterà le seguenti categorie di Dati Personali:

- **Dati anagrafici:** ovvero, tutti i dati personali che consentano l'identificazione certa di una persona fisica o giuridica, forniti al momento della richiesta di emissione del certificato comprendenti: nome, cognome, sesso, data e luogo di nascita, codice fiscale, indirizzo di residenza/domicilio, recapito di telefonia fissa/mobile, partita iva, estremi e copia di un documento di identità in corso di validità, o altre informazioni come, per esempio, l'azienda presso la quale la persona opera o presta servizio, il ruolo ricoperto e il settore di attività;
- **Dati informatici**: indirizzo IP di provenienza, *log*; all'interno di tale categoria vi rientrano anche le immagini e i video, acquisiti nel corso della sessione di video-riconoscimento da remoto (tramite webcam), in caso di identificazione tramite l'utilizzo di questa procedura, dei soggetti da identificare;
- **Dati biometrici**: costituiti da quei frammenti di immagini e/o di video che, tramite l'elaborazione automatica per mezzo di appositi strumenti *hardware/software*, consentono di verificare l'identità di una persona fisica. Tale tipologia di dati viene trattata unicamente ove l'interessato richieda di essere riconosciuto con modalità di riconoscimento che utilizzano l'impiego di biometria per l'accertamento dell'identità dichiarata e purché vi presti esplicito ed informato consenso.
- **Informazioni per la fatturazione e dati di pagamento**: eventuale partita IVA, codice fiscale, indirizzo, codice IBAN e dati bancari/postali del Richiedente;
- **Dati di utilizzo**: generati nel contesto del prodotto/servizio acquistato;
- **Altri dati**: comprendenti dati e documenti utilizzati dal Richiedente per la richiesta di rilascio del certificato digitale o trattati da Uanataca nell'ambito delle attività di verifica dell'identità del Richiedente o al fine di accertare la presenza dei presupposti per l'aggiornamento o revoca del certificato rilasciato al Titolare, nonché informazioni di cui Uanataca possa entrare in possesso in occasione delle attività di manutenzione e/o assistenza tecnica o trattate da Uanataca nell'ambito delle finalità di supporto e *caring* svolte a favore dell'utente.

**f) FINALITÀ DEL TRATTAMENTO**

Il Trattamento delle categorie di Dati Personali elencate al capo precedente è effettuato da Uanataca, nello svolgimento delle sue attività, per specifiche finalità, come meglio descritto di seguito:

- **Finalità Contrattuali e di Legge**

a) Esecuzione delle attività necessarie alla conclusione ed esecuzione del contratto ai fini dell'emissione del certificato digitale richiesto e delle attività connesse alla sua gestione e utilizzazione;
b) attività di *customer assistance* e supporto all'utilizzo del servizio;
c) gestione di eventuali comunicazioni necessarie alla corretta gestione del rapporto tra Uanataca e gli interessati, nonché gestione di eventuali reclami e/o contenziosi;
d) adempimento degli obblighi di identificazione dei soggetti richiedenti di cui all'art. 24 co. 1 del 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/CA (anche solo "Regolamento eIDAS") e all'art. 32 co. 3 lett. a) del D.Lgs. 7 marzo 2005 n. 82 e s.m.i. (CAD);
e) adempimento degli ulteriori obblighi in capo ai prestatori di servizi fiduciari qualificati ai sensi degli artt. 24 e ss. del Regolamento eIDAS e artt. 30 e ss. del D.Lgs. 7 marzo 2005 n. 82 e s.m.i. (CAD);
f) adempimento di altri obblighi di legge (ivi compresi adempimenti fiscali e contabili), regolamenti, normative comunitarie, ovvero gestione e risposta a richieste provenienti dalle competenti autorità fiscali e amministrative, ivi compresa l'autorità di vigilanza (Agenzia per l'Italia digitale), oltre che dall'autorità giudiziaria.

La fornitura dei Dati Personali per le Finalità Contrattuali e di Legge sopra descritte è necessaria e obbligatoria sicché, in caso di diniego, Uanataca non può dare seguito al rapporto contrattuale e alla relativa fornitura del servizio richiesto.

- **Finalità di Marketing**

g) per inviare aggiornamenti su novità e offerte commerciali di prodotti e servizi di Uanataca, anche previa interconnessione dei dati di utilizzo e analisi del comportamento dell'utente rispetto all'utilizzo dei servizi e prodotti di Uanataca ovvero per l'invito a partecipare a eventi, condurre ricerche di mercato o altre iniziative commerciali e di *customer satisfaction* sia tramite canali di comunicazione tradizionali quali la posta cartacea o la telefonata da parte di un operatore che tramite strumenti di comunicazione automatizzati quali e-mail, chat, messaggi (SMS e altri messaggi istantanei), *chatbot* e altri strumenti di comunicazione a distanza;
h) per comunicare i Dati Personali ad altre società del gruppo Uanataca e/o di partner commerciali appartenenti alla propria rete vendite, per l'invio di comunicazioni di marketing e per altre iniziative commerciali come quelle indicate alla lettera precedente.

Il trattamento dei Dati Personali per le "*Finalità di Marketing*" non è obbligatorio e rimane facoltativo a seguito della prestazione del consenso dell'Interessato.

Inoltre, Uanataca potrà trattare i Dati Personali acquisiti per effettuare controlli sulla qualità del servizio e sulla sicurezza del sistema.

I Dati Personali acquisiti da Uanataca non saranno trattati per finalità diverse da quelle sopra descritte o in modo incompatibile con le stesse.

Uanataca informa gli interessati che i propri Dati Personali potranno essere comunicati a soggetti pubblici ed autorità giudiziarie su esplicita richiesta di queste ultime, nel rispetto delle disposizioni di legge applicabili e al fine di prevenzione delle frodi ed attività illecite.

**g) BASE GIURIDICA DEL TRATTAMENTO**

La base giuridica del trattamento, ai sensi dell'art. 6 del GDPR, è individuata:

- con riferimento alla Finalità Contrattuali di cui alle lett. a), b), c) la base giuridica che legittima il trattamento dei Dati Personali è l'adempimento delle attività necessarie alla fornitura dei certificati digitali richiesti dai clienti (esecuzione contrattuale);
- con riferimento alla Finalità di Legge, di cui alle lett. d), e), f) la base giuridica che legittima il trattamento dei Dati Personali è l'adempimento degli obblighi normativi posti in capo a Uanataca (adempimento di un obbligo di legge) mentre con riferimento alle Finalità di Legge di cui alla lett. d) nell'ambito del trattamento del dato biometrico (in caso di scelta di modalità di identificazione che prevede tale tipologia di trattamento da parte del Richiedente) la base giuridica che legittima il trattamento è il preventivo consenso dell'interessato;
- con riferimento alle Finalità di Marketing, di cui alle lett. g) e h), la base giuridica che legittima il trattamento dei Dati Personali è il preventivo consenso dell'Interessato, che Uanataca raccoglierà all'atto di richiesta di rilascio del certificato digitale. Il consenso espresso è sempre revocabile senza alcuna conseguenza rispetto ai rapporti contrattuali intercorrenti con Uanataca e all'erogazione del servizio richiesto.

La manifestazione del consenso da parte dell'interessato deve essere sempre liberamente espressa: i Richiedenti/Titolari sono sempre adeguatamente messi a conoscenza dell'Informativa sulla Privacy e di tutti i diritti alla stessa connessi, compreso il diritto di revocare il consenso già prestato ovvero di opporsi al Trattamento in qualunque momento.

Detto consenso può essere ritirato in qualsiasi momento contattando la direzione di Uanataca S.A. o il DPO ad uno dei contatti sopra indicati.

**h) CONSERVAZIONE E CANCELLAZIONE DEI DATI PERSONALI**

I Dati Personali saranno trattati per il tempo necessario al perseguimento delle finalità per cui sono raccolti. In ogni caso, si applicheranno i seguenti termini di conservazione con riferimento ai trattamenti dei Dati per le finalità riportate di seguito:

- per le Finalità Contrattuali e di Legge i Dati Personali acquisiti nell'ambito delle richieste di rilascio di certificati digitali vengono conservati, in conformità a quanto disposto dall'art. 7 co. 8 del D.P.C.M. 24 ottobre 2014, per un periodo pari a 20 (venti) anni decorrenti cessazione del contratto ovvero dalla scadenza o dalla revoca del certificato, conformemente a quanto stabilito dall'art. 28, co.4 bis del D. Lgs. 82/2005 e s.m.i., fatti salvi i casi in cui la conservazione per un periodo successivo sia richiesta dalla legge o in caso di

eventuali contenziosi, richieste delle autorità competenti e comunque della normativa applicabile;

- per le Finalità di Marketing i dati vengono conservati per un periodo pari a 24 mesi dalla data in cui il consenso viene prestato ovvero rinnovato in occasione dell'acquisto di un nuovo prodotto o servizio a marchio Uanataca oppure data dell'ultimo contatto da intendersi, tra gli altri, la partecipazione ad un evento di Uanataca, la fruizione di un prodotto o servizio fornito da Uanataca o l'apertura di una *newsletter*;

I *log* di servizio relativi ai Certificati verranno conservati per un periodo pari a 6 (sei) mesi al fine di garantire la corretta individuazione dei flussi dei servizi.

Decorsi tali periodi, Uanataca provvederà alla cancellazione dei Dati Personali così acquisiti.

**i) EVENTUALI DESTINATARI O CATEGORIE DI DESTINATARI DEI DATI PERSONALI**

Nel rispetto del principio di finalità e di minimizzazione, i Dati Personali acquisiti da Uanataca possono essere comunicati alle seguenti categorie di soggetti terzi che svolgono attività funzionali a quelle specifiche del Fornitore di Servizi Fiduciari, quali (a) personale incaricato del trattamento (ad es. il personale degli Uffici CRM, IT, Retail); (b) terzi fornitori di servizi di assistenza e consulenza per Uanataca con riferimento alle attività dei settori (a titolo meramente esemplificativo) tecnologico, contabile, amministrativo, legale, assicurativo; (c) società appartenenti al gruppo Bit4 Group S.r.l.; (d) banche e istituti di credito; (e) società di recupero crediti; (f) soggetti ed autorità pubbliche il cui diritto di accesso ai tuoi dati personali è espressamente riconosciuto dalla legge, da regolamenti o da provvedimenti emanati dalle autorità competenti; (g) potenziali acquirenti della società ed entità risultati dalla fusione o ogni altra forma di trasformazione riguardante la società; (h) banche dati pubbliche e sistemi informativi di informazioni creditizie.

Per le Finalità di Marketing, e solo previo consenso espresso, i Dati Personali potranno essere comunicati anche a soggetti terzi e partner commerciali incaricati delle campagne di marketing svolte per conto di Uanataca o delle altre società del gruppo Uanataca.

Tali destinatari, a seconda dei casi, tratteranno i Dati Personali in qualità di autonomi titolari, responsabili o incaricati del trattamento. La lista completa e aggiornata dei soggetti che trattano i dati in qualità di responsabili del trattamento è disponibile su richiesta al Responsabile della Protezione dei Dati, secondo le modalità di contatto indicate nella presente Informativa.

**j) TRASFERIMENTO DEI DATI IN AMBITO COMUNITARIO/EXTRA COMUNITARIO**

I Dati Personali acquisiti da Uanataca potranno essere liberamente trasferiti all'interno dell'Unione Europea. Uanataca non trasferisce né prevede il trasferimento di dati personali nei confronti di soggetti situati al di fuori dell'Unione Europea.

Tuttavia, laddove, per le finalità indicate, Uanataca avesse necessità di trasferire tali dati fuori dall'Unione europea, verso Paesi non considerati adeguati dalla Commissione europea (es. Stati Uniti), questa adotterà le misure necessarie a proteggere i Dati Personali trasferiti, nel rispetto delle garanzie di legge, ai sensi della normativa applicabile e in particolare degli articoli 45 e 46 del GDPR.

Gli interessati hanno il diritto di ottenere una copia dei Dati eventualmente detenuti all'estero, al di fuori dello Spazio Economico Europeo, e di ottenere informazioni circa il luogo dove tali Dati sono conservati facendone espressa richiesta a Uanataca ai contatti indicati nella presente informativa.

**k) DIRITTI DEGLI INTERESSATI**

In relazione al trattamento dei dati di cui alla presente Informativa, gli interessati possono esercitare in ogni momento i diritti previsti dal Regolamento GDPR (artt. 15 e ss.) ivi inclusi:

1. **DIRITTO DI ACCESSO AI DATI PERSONALI:** ai sensi dell'art. 15 del GDPR (rubricato "*Diritto di accesso dell'interessato*") l'Interessato ha diritto di ottenere dal Titolare del Trattamento la conferma che sia o meno in corso Trattamenti di Dati Personali che lo riguardano e in tal caso, di ottenere l'accesso ai Dati Personali in possesso del Titolare. L'interessato può contattare direttamente il DPO che prenderà in carico la richiesta e fornirà copia di tutti i Dati Personali oggetto del Trattamento. Si applicano, per quanto non espressamente qui richiamate, le disposizioni di cui all'art. 15 del GDPR.
2. **DIRITTO DI RETTIFICA DEI DATI PERSONALI:** ai sensi dell'art. 16 del GDPR (rubricato "*Diritto di rettifica*") l'Interessato ha diritto di ottenere dal Titolare del Trattamento la rettifica dei Dati Personali inesatti che lo riguardano; L'interessato ha diritto di ottenere l'integrazione dei dai personali incompleti, anche fornendo una dichiarazione integrativa, tenuto conto delle finalità del Trattamento.
3. **DIRITTO DI CANCELLAZIONE DEI DATI PERSONALI:** ai sensi dell'art. 17 del GDPR (rubricato "*Diritto di cancellazione («diritto all'oblio»)*") l'Interessato ha diritto di ottenere la cancellazione dei Dati Personali che lo riguardano dal Titolare del Trattamento; sarà quindi onere di Uanataca di cancellare, senza ingiustificato ritardo, i Dati Personali oggetto del Trattamento, sempre che sussistano le motivazioni di cui all'art. 17 co. 1 sopra citato e salva l'applicazione dei commi 2 e 3.
4. **DIRITTO DI RICHIEDERE UNA LIMITAZIONE DEL TRATTAMENTO:** ai sensi dell'art. 18 del GDPR (rubricato "*Diritto di limitazione del Trattamento*") l'interessato ha diritto di ottenere dal Titolare del Trattamento la limitazione del Trattamento in tutti i casi previsti dall'art. 18 co. 1 appena citato. Nel caso in cui abbia luogo la limitazione del Trattamento, i Dati Personali oggetto della limitazione potranno essere trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato Membro.
5. **DIRITTO DI OPPOSIZIONE AL TRATTAMENTO:** ai sensi dell'art. 21 del GDPR (rubricato "Diritto di opposizione al Trattamento") l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al Trattamento dei Dati Personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. A seguito della manifestazione dell'interessato

di voler esercitare il diritto di opposizione, il Titolare del Trattamento si astiene dal trattare ulteriormente i Dati Personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al Trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i Dati Personali siano trattati per finalità di *marketing* diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al Trattamento dei Dati Personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale *marketing* diretto. Qualora l'interessato si opponga al Trattamento per finalità di marketing diretto, i Dati Personali non sono più oggetto di Trattamento per tali finalità. Si applicano, per quanto non espressamente qui richiamate, le disposizioni di cui all'art. 21 del GDPR.

6. **DIRITTO ALLA PORTABILITA' DEI DATI:** ai sensi dell'art. 20 del GDPR (rubricato "Diritto alla portabilità dei Dati") l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati Personali che lo riguardano forniti a un Titolare del Trattamento e ha il diritto di trasmettere tali Dati a un altro Titolare del Trattamento senza impedimenti da parte del Titolare del Trattamento cui li ha forniti nei casi previsti dal co. 1 lett. a) e b) del predetto articolo. Tale diritto non trova applicazione nel caso in cui il Trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento.
7. **DIRITTO DI REVOCA DEL CONSENSO GIA' PRESTATO:** ai sensi degli artt. 7 co. 3 e 13 co. 2 lett. c) del GDPR l'interessato ha il diritto di revocare il proprio consenso già prestato in qualsiasi momento. La revoca del consenso non pregiudica la liceità del Trattamento basata sul consenso prima della revoca.
8. **DIRITTO DI OPPOSIZIONE ALLA PROFILAZIONE E AL TRATTAMENTO AUTOMATIZZATO:** ai sensi dell'art. 22 l'interessato ha diritto a non essere sottoposto a decisioni basate sul trattamento automatizzato, compresa la profilazione, che producano effetti giuridici nei loro confronti o che incidano in modo analogo sulla loro persona.
9. **DIRITTO DI PROPORRE RECLAMO ALL'AUTORITA' DI CONTROLLO**: ai sensi dell'art. 77 del GDPR l'interessato, il quale ritenga che il trattamento che lo riguarda violi il Regolamento, può proporre reclamo ad un'autorità di controllo situata all'interno dello Stato membro in cui risiede.

Ai sensi dell'articolo 2-*terdecies* del Codice Privacy, in caso di decesso i diritti anzidetti riferiti ai dati personali degli Interessati possono essere esercitati da chi ha un interesse proprio, o agisce a sua tutela in qualità di mandatario, o per ragioni familiari meritevoli di protezione. L'Interessato può vietare espressamente l'esercizio di alcuni dei diritti sopraelencati da parte degli aventi causa inviando una dichiarazione scritta a Uanataca all'indirizzo di posta elettronica indicato sotto. La dichiarazione potrà essere revocata o modificata in seguito nelle medesime modalità.

Per esercitare i diritti in materia di protezione dei dati personali in ogni momento e gratuitamente è possibile rivolgersi al Responsabile della Protezione dei Dati, che è contattabile inviando una richiesta all'indirizzo dpo@uanataca.com, oppure indirizzando la comunicazione via posta a:

Uanataca S.A. unipersonale
Via Diocleziano n. 107
(80125) - Napoli
c.a.: Responsabile della Protezione dei Dati

Nel contattare Uanataca, è necessario che l'Interessato includa nome, e-mail/indirizzo postale e/o numero/i di telefono per essere sicuro che la sua richiesta possa essere gestita correttamente.

### *9.4.2. Trattamento dei dati personali – Emissione dei Certificati di CNS*

Con riferimento al Trattamento dei dati personali trattati nell'ambito del ciclo di vita dei certificati di CNS, Uanataca opera in regime di contitolarità, ai sensi dell'art. 26 del GDPR, con l'Ente Emettitore.

## *9.5. Diritti di proprietà intellettuale*

### *9.5.1. Proprietà dei certificati*

Uanataca gode di tutti i diritti di proprietà intellettuale e sfruttamento economico, riconosciuti dalla legge, su tutti i certificati emessi in esecuzione dei rapporti contrattuali con i Richiedenti e applicazione del presente Manuale Operativo.

### *9.5.2. Proprietà del Manuale Operativo – Servizi di Certificazione digitale*

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

### *9.5.3. Proprietà dei marchi*

Il nome "Uanataca" è un marchio registrato di proprietà esclusiva della Bit4 Group S.r.l. cui spettano tutti i diritti di proprietà intellettuale e di utilizzazione economica 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 e i Richiedenti del certificato saranno tenuti a manlevare e indennizzare Uanataca 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.

## 9.6. Obblighi, Garanzie e responsabilità

### 9.6.1. Garanzie offerte da Uanataca

Fermo il rispetto degli obblighi di garanzia di cui al paragrafo 9.2, Uanataca si impegna a:

- erogare il servizio di certificazione in conformità alle disposizioni del Manuale Operativo;
- fornire un efficiente servizio di revoca dei certificati;
- fornire un servizio informativo efficiente ed affidabile 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, Uanataca 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 senza l'espresso consenso della persona alla quale si riferiscono.

### 9.6.2. Esclusione di garanzie

Uanataca 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 Fornitura relative ai servizi di certificazione digitale.

### 9.6.3. Limitazioni di responsabilità

Uanataca 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 Uanataca sono circoscritte, esclusivamente, a quelle dettati dal presente Manuale e dal Contratto di fornitura relativo ai servizi di certificazione.

In nessun altro caso, per nessun titolo e/o ragione, Uanataca 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 Uanataca.

In particolare, ai sensi dell'art. 13 della normativa eIDAS richiamata dalla normativa ETSI EN 319 401 punto 7.1.1., Uanataca 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 cit.

Va precisato, tuttavia, che ai sensi dell'art. 13 co. 2 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.

### *9.6.4. Obblighi relativi al ciclo di vita dei certificati di CNS*

#### *9.6.4.1. Obblighi dei Titolari*

Con riferimento agli obblighi dei titolari si applicano le disposizioni di cui al Par. 4.5.1. del presente Manuale, qui da intendersi come riportate e trascritte.

#### *9.6.4.2. Obblighi delle Relying Parties*

Con riferimento agli obblighi delle Relying Parties si applicano le disposizioni di cui al Par. 4.5.2. del presente Manuale, qui da intendersi come riportate e trascritte.

#### *9.6.4.3. Obblighi dell'Ente Emettitore*

Ai sensi del Decreto Interministeriale 9 dicembre 2004 recante regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi, l'Ente Emettitore è responsabile della formazione e del rilascio della CNS; si tratta della Pubblica

Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS.

L'Ente Emettitore è, quindi, responsabile:

a) della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione,
b) della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione,
c) della sicurezza delle fasi di produzione, inizializzazione, distribuzione ed aggiornamento/ritiro della carta.

### *9.6.4.4. Obblighi del Certificatore*

Il Certificatore Uanataca è l'ente che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche, abilitato ai sensi dell'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002, per conto dell'Ente Emettitore.

L'Ente Emettitore ha delegato al Certificatore lo svolgimento di parte delle attività relative al ciclo di vita del certificato di CNS a Uanataca.

In particolare, il Certificatore è responsabile della generazione del certificato di autenticazione e di firma di CNS.

Ulteriori informazioni in merito ai ruoli delle parti coinvolte è rinvenibile nel Manuale Operativo adottato da parte dell'Ente Emettitore cui si rinvia per ulteriori dettagli.

### *9.6.4.5. 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** | 24x7 | - Servizio di assistenza dalle ore 9 alle ore 18 (lun.-ven), esclusi i festivi.<br>- Presso gli Uffici di registrazione secondo gli orari da essi indicati. |
| **Rilascio** | Orario di ufficio | Presso gli Uffici di registrazione secondo gli orari da essi indicati. |

Con riferimento alle modalità di contatto del Centro Assistenza di Uanataca è possibile inoltrare tutte le richieste al seguente indirizzo di posta elettronica: assistenza@uanataca.com.

### 9.6.5. Indennizzi a favore di Uanataca

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 Uanataca, 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.

### 9.6.6. Indennizzi ai contraenti

Fermo quanto previsto dalle Condizioni Generali di Contratto relative ai servizi di certificazione, Uanataca dispone di un'apposita assicurazione a copertura dei rischi dell'attività associata all'erogazione dei servizi di certificazione (si veda il par. 9.2.1).

In ogni caso, il risarcimento di danni a terzi non potrà superare l'importo massimo annuo complessivo di €. 3.000.000,00 (tremilioni,00//) escluso una franchigia di €. 500,00 (cinquecento,00//) per ogni reclamo.

In caso di danno derivante dalle attività oggetto del Contratto, il Contraente dovrà, a pena di decadenza:

- farne denuncia a Uanataca entro 24 ore dal suo verificarsi, ovvero da quando ne abbia avuta conoscenza (facendo seguire conferma per lettera raccomandata A.R. oppure Posta Elettronica Certificata entro le 24 ore successive);
- entro sei mesi dall'inoltro della denuncia di cui al punto precedente, quantificare l'eventuale danno subìto e formulare la relativa richiesta di risarcimento.

### 9.6.7. Durata e risoluzione del contratto

Le disposizioni di cui al presente documento trovano applicazione dalla data dell'adesione da parte dell'Utente che usufruisca dei servizi fiduciari qualificati messi a disposizione di Uanataca e che si intendono dunque come integralmente accettati 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 presente contratto.

Analoga conseguenza deriva dalla risoluzione del contratto che determina la revoca del certificato da parte della CA emittente.

### 9.6.8. Cessione del contratto

Non è consentito al Richiedente la cessione di tutto o parte degli obblighi e dei diritti nascenti dal presente contratto.

### 9.6.9. 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, servizi di certificazione erogati da Uanataca sono sottoposti alle norme vigenti.

### 9.6.10. Foro competente

Per tutte le controversie nascenti dal presente Manuale Operativo, dai Termini e le Condizioni accettati dal Richiedente o da ulteriori eventuali contratti stipulati per la fruizione dei servizi messi a disposizione da Uanataca, compresi quelle inerenti alla loro esistenza, validità, estinzione, interpretazione, esecuzione e risoluzione sarà, competente in via esclusiva il Foro di Napoli, con espressa esclusione di ogni altro Foro concorrente.

## 9.7. Disposizioni finali

### 9.7.1. Modifiche al presente accordo

Il presente Manuale 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.

### 9.7.2. 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.

### 9.7.3. Forza maggiore

Uanataca 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*

Uanataca, 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.uanataca.com/it

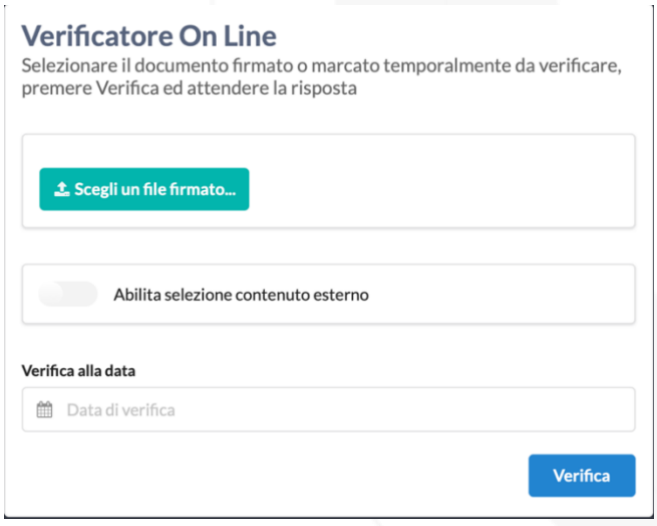
Il predetto software consente, nello specifico, di verificare:

a. l'identità 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.

uanataca
trust service provider

*Bringing trust and simplicity into the digital future*

www.uanataca.com