Manuale Operativo

Certification Practice Statement e

Certificate Policy

REGIONE DEL VENETO

AZIENDA ZERO

Firmato da:
AgID
Email: it_tsl@agid.gov.it
Codice fiscale: VATIT-97735020584
Valido da: 27-04-2016 10:53:42 a: 12-01-2021 10:53:42
Certificato emesso da: AgID, Agenzia per l'Italia Digitale, IT
Riferimento temporale 'SigningTime': 12-05-2020 10:50:43
Approvo il documento

Firmato da:
AgID
Email: it_tsl@agid.gov.it
Codice fiscale: VATIT-9773502058
Valido da: 01-12-2020 10:34:41 a: 14-01-2026 10:34:41
Certificato emesso da: AgID, Agenzia per l'Italia Digitale, IT
Riferimento temporale 'SigningTime': 13-01-2021 17:18:54
Approvo il documento

Informazioni generali

Controllo documentale

Livello di sicurezza:	Pubblico
Ente di emissione:	AZIENDA ZERO
Versione:	2.1
Data di edizione:	23.03.2020
Codice documento:	ManualeOperativo_AziendaZero_v.2.1

Controllo formale

Redatto da:	Approvato da:
UOC Sistemi Informativi – Responsabile IT Data: 23.03.2020	UOC Sistemi Informativi - Direzione Data: 23.03.2020

Controllo delle versioni

Versione	Parti modificate	Descrizione delle modifiche	Data
1	Originale	Prima versione del documento	14.01.2019
1.1	Individuazione dettagliata dei ruoli dei diversi soggetti coinvolti nel servizio in outsourcing Parag. 8.4 – Considerazioni sull'accessibilità dei servizi	Seconda versione del documento	15.02.2019
1.1 rev. 1	Revisione link esterni. Aggiornamento sez. "Approvato da".	Revisione	27.02.2019
2.0	Nuova versione del documento	Nuova versione	15.01.2020
2.1	- Aggiornamento Par. 9.1.1. - Allegato A – Sistema di verifica dei certificati elettronici qualificati (nuovo)	Revisione e aggiornamento	23.03.2020

Indice

1. Introduzione

1.1. Presentazione

Questo documento pubblico, chiamato anche "Certification Practice Statement" (CPS), descrive le procedure operative seguite da AZIENDA ZERO nell'erogazione dei seguenti Servizi Fiduciari:

- emissione di certificati di firma qualificata;
- emissione certificati di marcatura temporale qualificata;
- generazione marche temporali.

I certificati emessi secondo questo CPS sono i seguenti:

- **Certificato qualificato di sottoscrizione**
  - *Certificato qualificato di sottoscrizione in QSCD remoto*
- **Certificato di Time Stamping Unit**
  - *Certificato di Time Stamping Unit per l'emissione di marche temporali qualificate*

I Servizi Fiduciari qualificati erogato da AZIENDA ZERO 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 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.

La struttura del presente documento CPS 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 - Certification Practice Statement / CPS" di AZIENDA ZERO.

La versione vigente del presente Manuale è indicata nell'intestazione del documento e nella sezione "Controllo delle versioni".

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 AZIENDA ZERO e sono specificate all'interno di ciascun certificato.

OID	Tipo di certificato
	Servizio di firma elettronica
1.3.6.1.4.1.52658.1.1.1	Certificato qualificato di sottoscrizione in QSCD remoto
	Servizio di Marca Temporale
1.3.6.1.4.1.52658.1.2.1	*Certificato di Time Stamping Unit*

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 AZIENDA ZERO, prevarrà quanto stabilito nel presente Manuale Operativo.

Azienda Zero 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 sarà premura di Azienda Zero notificare ad AGID la versione aggiornata del Manuale Operativo che sarà pubblicata sui relativi siti web istituzionali.

Questo documento è pubblicato sul sito web di AZIENDA ZERO https://www.azero.veneto.it/ .

1.3. Partecipanti ai servizi di certificazione

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

AZIENDA ZERO, attraverso la collaborazione dei partner tecnologici Bit4id S.r.l. e Uanataca S.A., opera in qualità di Qualified Trust Service Provider (QTSP).
I dati identificativi dell'Organizzazione sono i seguenti:

AZIENDA ZERO
SEDE LEGALE: PASSAGGIO LUIGI GAUDENZIO, 1 - 35131 PADOVA
TELEFONO: 049/8778178, 049/8778236, 049/8778249
EMAIL: SUPPORTO.CA@AZERO.VENETO.IT

AZIENDA ZERO eroga i seguenti servizi fiduciari:

- rilascio e gestione dei certificati qualificati, 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 319 411-1" e "EN 319 411-2".

- 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".

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

1.3.1.1. Azienda Zero CA Qualificata eIDAS 1

Si tratta della CA che rilascia i certificati agli utenti finali e il cui certificato di chiave pubblica è autofirmato (self-signed).

Dati identificativi:

CN:	Azienda Zero CA Qualificata eIDAS 1
Fingeprint:	fb6b79978e7d9062322acbe431d24cc92c278001
Valido da:	11 gennaio 2019
Valido fino a:	11 gennaio 2044
Lunghezza chiave RSA:	4.096 bits

1.3.1.2. Azienda Zero TSA Qualificata eIDAS 1

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

Dati identificativi:

CN:	Azienda Zero TSA Qualificata eIDAS 1
Fingeprint:	97217b8d2bccd5cacb6dbe61619c421412dbf266
Valido da:	11 gennaio 2019
Valido fino a:	11 gennaio 2044
Lunghezza chiave RSA:	4.096 bits

1.3.2. Uffici di Registrazione (Registration Authorities - R.A.)

Gli Uffici di Registrazione (R.A.) costituiscono terze parti delegate da AZIENDA ZERO che, attraverso la stipula di appositi accordi, sono deputati a svolgere le attività di

identificazione ed autenticazione dei soggetti che richiedono i certificati.

Nello specifico, una R.A. compie le seguenti attività:

- identificazione e autenticazione (I&A) del soggetto Richiedente il certificato di firma
- verifica dei requisiti necessari per lo svolgimento della richiesta di certificato da parte del Richiedente;
- verifica dei dati identificativi di colui che figurerà come Titolare del certificato;
- registrazione dei Richiedenti (futuri Titolari) e dei relativi dati;
- autorizzazione all'emissione di certificati digitali attraverso appositi strumenti messi a disposizione da Azienda Zero;
- custodia della documentazione relativa: a) all'identificazione del Richiedente; b) alla registrazione del Richiedente; c) alla gestione del ciclo di vita dei certificati.

Potranno agire in qualità di R.A. di AZIENDA ZERO:

- qualunque persona, fisica o giuridica, esterna a AZIENDA ZERO, espressamente autorizzata da quest'ultima;
- AZIENDA ZERO, direttamente, per il tramite del suo personale.

AZIENDA ZERO formalizzerà contrattualmente i rapporti intercorrenti tra la medesima e ciascun soggetto che agirà come Ufficio di Registrazione.

La R.A., a sua volta, potrà autorizzare una o più persone ad agire come "Operatore 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.

Il suddetto accordo dovrà essere espressamente autorizzato da AZIENDA ZERO.

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

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

1.3.3. Utenti finali

Gli utenti finali si identificano nelle persone fisiche destinatarie del servizio di emissione, gestione ed utilizzo dei certificati qualificati emessi da AZIENDA ZERO.

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

1. Richiedenti: persone fisiche che domandano alla CA il rilascio di un certificato digitale;
2. Titolari: persone fisiche 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 digitale ivi presente) per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

1.3.3.1. Richiedente il certificato

È la persona fisica che richiede il rilascio di certificati digitali, rivolgendosi direttamente alla CA o ad una sua RA.

Il Richiedente, pertanto, può anche qualificarsi come "Cliente" della CA: 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 CA 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.

1.3.3.2. Titolare del certificato

Il Titolare del certificato è il soggetto che possiede ed utilizza la chiave privata relativa ad un certificato 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 chiarimenti identificativi del Titolare del certificato, senza che sia possibile, in genere, l'utilizzo di pseudonimi.

La chiave privata di un Titolare non può essere recuperata o ricavata dalla CA, in quanto i Titolari identificati nei rispettivi certificati sono gli unici responsabili della sua protezione. Essi, pertanto, sono tenuti a tenere in debita considerazione le conseguenze derivanti dallo smarrimento della chiave privata.

1.3.3.3. Relying parties (R.P.)

Le Relying Parties si identificano nei soggetti che fanno affidamento sulle informazioni contenute nei certificati emessi da AZIENDA ZERO.

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 questo 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 AZIENDA ZERO

1.3.4. Outsourcee

Azienda ZERO offre il servizio di certificazione di chiavi pubbliche avvalendosi della partnership tecnologica di

- Bit4id S.r.l., azienda fondata nel 2004 con comprovata esperienza nell'ambito dell'infrastruttura a chiave pubblica (tecnologia PKI) e con numerose esperienze di successo in ambito italiano e internazionale.
- Uanataca S.A., QTSP fondato nel 2015 e con sede legale a Barcellona (Spagna).

Dette società sono responsabili della conduzione tecnica dei sistemi e dei servizi tecnici e logistici, erogati in outsourcing.

In particolare, viene demandata l'erogazione in outsourcing di determinati servizi della CA con particolare riferimento a:

- Definizione degli obiettivi di sicurezza;
- Individuazione dei requisiti contrattuali e normativi;
- Risk assessment per l'analisi, la valutazione, la pianificazione del trattamento dei rischi e la selezione delle contromisure rilevanti.

Tramite l'affidamento in outsourcing dei servizi erogati dalla CA a Fornitori qualificati, Azienda Zero intende garantire la riservatezza, l'integrità e la diponibilità delle informazioni.

1.3.5. Autorità

1.3.5.1. 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 sui Prestatori di servizi fiduciari qualificati stabiliti nel territorio italiano allo scopo di garantirne la rispondenza ai requisiti stabiliti dal Regolamento.

1.3.5.2. Organismo di valutazione della conformità – Conformity Assessment Body

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 AZIENDA ZERO e i limiti caratterizzanti l'utilizzo di alcune tipologie di certificati.

1.4.1. Uso previsto dei certificati

I certificati emessi da AZIENDA ZERO, secondo le modalità indicate dal presente Manuale operativo, sono Certificati Qualificati ai sensi del CAD e del Regolamento eIDAS.
Il certificato emesso dalla CA sarà usato per verificare la firma qualificata 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 Manuale Operativo, nella documentazione contrattuale nonché in violazione dei limiti d'uso e di valore (key usage, extended key usage, user notice) indicati nel certificato.
AZIENDA ZERO si riserva la facoltà di revocare i certificati qualora venga a conoscenza che tali certificati siano stati utilizzati in modo improprio.

1.4.1.1. Certificato qualificato di sottoscrizione in QSCD remoto

Questo certificato è contrassegnato da OID 1.3.6.1.4.1.52658.1.1.1. 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 fima (QSCD), nel rispetto degli articoli 29 e 51 del Regolamento (UE) 910/2014, e in accordo a quanto disposto dalla regolamentazione tecnica rilasciata dall'Instituto Europeo per gli Standard nelle Telecomunicazioni, identificata con il riferimento EN 319 411-2.
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 Time Stamping Unit

Questo certificato è contrassegnato dall' OID 1.3.6.1.4.1.52658.1.2.1 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 AZIENDA ZERO si effettua attraverso il protocollo NTP, puntando a un server con un livello di sincronizzazione Stratum 3.

1.4.2. Limiti e divieti nell'utilizzo dei certificati

I certificati emessi da AZIENDA ZERO 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 e in violazione dei limiti d'uso e di valore (key usage, extended key usage, user notice) riportati all'interno del certificato stesso.
Allo stesso modo, i certificati emessi da AZIENDA ZERO devono essere impiegati unicamente nel rispetto della normativa vigente.

1.5. Amministrazione del Manuale Operativo

1.5.1. Organizzazione responsabile

Questo documento è la CPS di AZIENDA ZERO e viene redatto, pubblicato ed aggiornato da AZIENDA ZERO.
I dati di contatto del TSP sono i seguenti:

Azienda Zero
Passaggio Luigi Gaudenzio, 1 - 35131 Padova (PD)
Padova (Italia)
protocollo.azero@pecveneto.it
Codice Fiscale 05018720283
https://azero.veneto.it/ca

1.5.2. Procedura di approvazione e gestione

AZIENDA ZERO, con il supporto dell'Outsourcee, 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

CA: Certification Authority

CAB: Conformity Assessment Body

CAD: Codice dell'Amministrazione Digitale (D.lgs. n.82/2005)

CP: Certificate Policy

CRL: Certificate Revocation List

CSP: Certification Practice Statement

ETSI: European Telecommunications Standards Institute

FQDN: Fully-Qualified Domain Name

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

RA: Registration Authority

TLS: Transport Layer Security

TSL: Trust-service Status List

TSP: Trust Service Provider

2. Pubblicazione delle informazioni sui certificati e Repository

2.1. Repository

AZIENDA ZERO 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 al link: https://azero.veneto.it/ca/.
Il "repository" è accessibile in modo continuo (7x24).
Nell'ipotesi in cui si verifichi un arresto del sistema, al di fuori del controllo di AZIENDA ZERO, quest'ultima si impegnerà 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.

AZIENDA ZERO pubblica sul proprio sito internet:

- 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 nella pubblicazione

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 nelle sezione 4 del presente Manuale Operativo.

2.4. Controllo nell'accesso

AZIENDA ZERO 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 dette informazioni, allo scopo di tutelarne l'integrità e l'autenticità.

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 e le specifiche contenute nella RFC 5280.
In particolare, i certificati emessi secondo questo documento CPS sono conformi ai seguenti standard:

- 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 soggetti dei certificati e dei certificati di Time Stamp Unit.

3.1.2.1. Emissione di certificati di prova

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 AZIENDA ZERO.

I suddetti certificati vengono emessi al fine di realizzare prove tecniche di interoperabilità e permettere all'Organismo supervisore competente 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. Allo stesso modo, in nessun caso verranno emessi certificati anonimi.

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) contiene attributi identificativi specifici in base alla natura del Titolare stesso.

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

- il SerialNumber (OID 2.5.4.44) contenente il codice fiscale del soggetto 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).
- il Givenname (OID 2.5.4.44) contenente il nome del soggetto
- il Surname (OID 2.5.4.44) contenente il cognome del soggetto

L'unicità per i certificate di TSU viene parimenti assicurata dalle procedure di Azienda Zero.

3.1.6. Soluzione dei conflitti relativi ai nominativi

AZIENDA ZERO non sarà obbligata a verificare previamente che un Richiedente il certificato sia titolare del diritto all'uso del nome che compare in una richiesta di certificato ma, in linea di principio, provvederà al rilascio del certificato.
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.

Tuttavia, nel caso in cui AZIENDA ZERO 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. 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; prima di procedere al rilascio del certificato richiesto, dunque, la C.A. dovrà svolgere tutte le attività necessarie all'identificazione dei Richiedenti.

L'identità del Richiedente il certificato viene verificata tramite il suo documento d'identità nonché tramite specifici attributi che possono essere: l'associazione con l'Organizzazione di appartenenza e, possibilmente, il ruolo posseduto all'interno dell'organizzazione.

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) 2016/279 – 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 è possibile fare riferimento al par. 3.2.2. di seguito.

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.

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".

3.2.2.1. Nei certificati

L'identità delle persone fisiche titolari, 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 o altro documento idoneo riconosciuto dalla legge per l'identificazione).

3.2.2.2. Validazione dell'identità

Il procedimento di identificazione prevede la presenza fisica del Richiedente, avente almeno 18 (diciotto) anni di età, dinnanzi ad un Operatore o al personale autorizzato dalla R.A. di AZIENDA ZERO, i quali provvedono ad accertare l'identità del Richiedente attraverso la verifica dei corrispondenti documenti di identità esibiti in originale.

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.

Nel caso di persona fisica, per l'appunto, il personale incaricato ed addetto alla verifica 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;
- 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;

Questo processo consente una verifica ed un accertamento rigoroso dell'identità della persona fisica nel certificato. Per questo motivo, in tutti i casi in cui viene emesso un certificato, l'identità della persona fisica Titolare viene sempre precedentemente validata da un Operatore di Registrazione autorizzato.

Sarà onere del Richiedente fornire, al termine delle operazioni di identificazione fisica, fornire un indirizzo fisico o di domicilio dove quest'ultimo può essere sempre 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.

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 ad Azienda Zero, anche in formato elettronico, al fine di attivare correttamente la procedura di emissione dei Certificati.

3.2.3. Informazioni non verificate

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

3.2.4. Autenticazione di un Ufficio di Registrazione e dei suoi Operatori

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

Allo stesso modo, AZIENDA ZERO, direttamente o attraverso la propria R.A., verifica e convalida l'identità degli Operatori delle R.A., per i quali, queste ultime, inviano a AZIENDA ZERO la documentazione di identificazione, unitamente alla loro autorizzazione ad agire come tale.

AZIENDA ZERO garantisce che gli Operatori delle R.A. ricevano una formazione adeguata per il corretto svolgimento delle loro attività, formazione che verrà confermata attraverso una corrispondente valutazione. Tale formazione e valutazione possono essere eseguite dalla R.A. precedentemente autorizzata da AZIENDA ZERO.

Per la prestazione dei servizi oggetto del presente Manuale, AZIENDA ZERO 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. Identificazione e autenticazione per il rinnovo periodica 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 AZIENDA ZERO 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. Identificazione e autenticazione per le 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. 3.2.2.2.

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 AZIENDA ZERO 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 la riemissione dei certificati, qualora ricorra uno dei seguenti casi:

- il certificato è stato revocato in quanto erroneamente emesso per una persona diversa da quella identificata nel certificato;
- il certificato è stato revocato in quanto emesso senza l'autorizzazione del soggetto identificato nel certificato;
- il certificato revocato contiene informazioni errate o false.

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 la richiesta di revoca

AZIENDA ZERO 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 da:

• Il Richiedente e/o il Titolare:

- tramite l'uso del codice di revoca ERC attraverso il sito Web di AZIENDA ZERO (https://azero.veneto.it/ca) disponibile 7 giorni su 7 e 24 ore su 24;
- o 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 AZIENDA ZERO e / o delle R.A.

• Le R.A.: queste devono identificare il Titolare prima di approvare una richiesta di revoca in base ai mezzi che ritengono necessari.

Nell'ipotesi in cui il Richiedente inoltri una richiesta di revoca durante l'orario d'ufficio ma vi siano dubbi sulla sua identificazione 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 alla richiesta

Il Richiedente del certificato è tenuto a sottoscrivere la documentazione contrattuale predisposta da AZIENDA ZERO.

4.1.2. Procedure e responsabilità

AZIENDA ZERO riceve richieste di certificati: le richieste vengono inoltrate tramite un modulo, in formato cartaceo o digitale, singolarmente o in lotti, o collegandosi a database esterni o tramite un pacchetto di servizi Web il cui destinatario è AZIENDA ZERO.
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 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, AZIENDA ZERO garantisce che quest'ultima sia completa, accurata e debitamente autorizzata, prima di elaborarla.

In caso di esito positivo, AZIENDA ZERO 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, AZIENDA ZERO 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, AZIENDA ZERO 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, AZIENDA ZERO rifiuterà definitivamente la richiesta.
AZIENDA ZERO notificherà al Richiedente l'approvazione o il rifiuto della richiesta.

AZIENDA ZERO 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

AZIENDA ZERO elabora le richieste di certificati in ordine di arrivo, entro un termine di tempo ragionevole.

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 AZIENDA ZERO:

- 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 consto di Azienda Zero 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.

4.3.3. Notifica di emissione del certificato

AZIENDA ZERO notifica l'emissione del certificato al Richiedente.

4.4. Consegna e accettazione del certificato

4.4.1. Responsabilità della R.A.

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

- verificare correttamente l'identità della persona fisica 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: 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;
- le informazioni sul certificato;
- evidenza della ricezione e accettazione da parte del Titolare dei dati associati all'uso del certificato;
- gli obblighi e responsabilità del Titolare;
- 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;
- la data dell'atto di consegna e accettazione del certificato.

• ottenere la firma della persona identificata sul 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 AZIENDA ZERO 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 Azienda Zero 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 identificata nel certificato viene effettuata firmando il modulo di consegna e accettazione.

4.4.3. Notifica dell'emissione a terzi

AZIENDA ZERO non emette nessuna notifica di emissione del certificato a terzi.

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 AZIENDA ZERO 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.

AZIENDA ZERO obbliga il Titolare ad assumersi la responsabilità che:

• 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 319 411-1/411-2hanno 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;

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 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 Azienda Zero) 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 AZIENDA ZERO.

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 AZIENDA ZERO 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)

Il rekeying del certificato non è ammesso in nessuna circostanza da AZIENDA ZERO.

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 nelle sezioni 4.

4.9. Revoca di un certificato

La revoca di un certificato comporta la cessazione anticipata e definitiva della sua validità. La revoca, pertanto, è una condizione irreversibile.

4.9.1. Ipotesi di revoca di un certificato

AZIENDA ZERO revoca un certificato quando si presenta una delle seguenti cause:

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 riguardano il Richiedente e/o il Titolare:

a) cessazione del contratto tra la CA e il Richiedente e/o il Titolare;

b) modifica o risoluzione anticipata del contratto tra la CA e il Richiedente e/o il Titolare;

c) violazione da parte del Richiedente il certificato dei requisiti prestabiliti per la sua richiesta;

d) violazione da parte del Richiedente e/o del Titolare degli obblighi contrattuali;

e) incapacità sopravvenuta del Richiedente e/o Titolare;

f) 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 AZIENDA ZERO;

b) utilizzo del certificato non conforme e pregiudizievole per AZIENDA ZERO, specie in modo continuativo.

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.

4.9.3. Procedimento relativo alla richiesta di revoca

Il soggetto che richiede la revoca di un certificato può farlo rivolgendosi direttamente a AZIENDA ZERO ovvero alla R.A. ovvero, in prima persona, attraverso il servizio online disponibile sulla pagina web di AZIENDA ZERO. 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 AZIENDA ZERO, in accordo con i requisiti stabiliti nel paragrafo 3 di questo Manuale.

Il servizio di revoca è disponibile al sito web di AZIENDA ZERO all'indirizzo https://azero.veneto.it/ca/.

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 AZIENDA ZERO.

4.9.4. Periodo di grazia della richiesta di revoca

Le richieste di revoca saranno trattate nel momento stesso in cui la CA ne prende conoscenza.

AZIENDA ZERO esegue la revoca con la massima tempestività e attenzione, garantendo che il tempo necessario per l'elaborazione dell'operazione di revoca 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 AZIENDA ZERO 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 Azienda Zero 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. Obbligo di 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.

Un metodo per effettuare tale verifica è consultare la Lista di Revoca dei certificati (CRL) più recente emessa da AZIENDA ZERO.

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

- http://crl1.uanataca.com/public/pki/crl/azeroCA.crl;
- http://crl1.uanataca.com/public/pki/crl/azeroTSA.crl;
- http://crl2.uanataca.com/public/pki/crl/azeroCA.crl;
- http://crl2.uanataca.com/public/pki/crl/azeroTSA.crl.

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

La verifica, inoltre, può essere compiuta mediante interrogazione del servizio OCSP erogato da AZIENDA ZERO 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

AZIENDA ZERO emette una nuova CRL almeno ogni 24 ore, anche in assenza 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 online della revoca

AZIENDA ZERO rende disponibile, in aggiunta alla pubblicazione delle CRL, un servizio di verifica on-line dello stato dei certificati basato sul protocollo OCSP (RFC 6960).

Il servizio OCSP è accessibile 7x24.

In caso di malfunzionamento dei sistemi di verifica dei certificati, AZIENDA ZERO 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 disponibile

4.9.12. Circostanze per la sospensione

La sospensione del certificato di firma elettronica qualificata non è prevista in nessuna circostanza.

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

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 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 di chiavi di sessione

Nessuna disposizione.

5. Misure di sicurezza fisica ed operativa

5.1. Sicurezza fisica.

Il sistema di certificazione di AZIENDA ZERO si trova presso il QTSP Uanataca S.A.

Uanataca è un'azienda del gruppo Bit4id, outsourcee designato da AZIENDA ZERO per i servizi oggetto di questo documento

L'outsorcee 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.

AZIENDA ZERO, per il tramite dell'Outsourcee, si avvale dei servizi di data center e servizi di comunicazione associati (quali housing, connettività alla rete Internet, sicurezza fisica) offerti dalla società ADAM.

Detti servizi sono certificati secondo le norme:

- ISO/IEC 27001:2017
- ISO 9001:2018

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.

L'Outsourcee 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 dell'Outsorucee ovvero del Responsabile della Sicurezza.

Azienda Zero 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 e aria condizionata

Le strutture nell'ambito delle quali viene svolto, in outsorucing, 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 AZIENDA ZERO, 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

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

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, AZIENDA ZERO 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 AZIENDA ZERO. Questi deve incaricarsi degli aspetti relativi alla sicurezza dell'informazione: logistica, fisica, di rete, organizzativa, etc.;
- **Auditor interno**: responsabile dello svolgimento delle procedure operative. E' inoltre responsabile della verifica degli archivi e dei log di audit dei sistemi di CA;
- **Amministratore di sistema**: responsabile dell''installazione, della configurazione, della manutenzione e del corretto funzionamento dei sistemi preposti all'erogazione dei servizi fiduciari;
- **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 Azienda Zero per l'emissione di certificati digitali ovvero per l'erogazione di servizi fiduciari;
- **Operatore di revoca**: responsabile dell'aggiornamento dello stato di validità un certificato (es. revoca).

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 AZIENDA ZERO, costituisce una misura atta a prevenire la commissione di attività fraudolente.

5.2.2. Numero di persone per attività

AZIENDA ZERO, 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.

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 e autorizzazioni richieste

Il personale di AZIENDA ZERO, 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.

AZIENDA ZERO 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 AZIENDA ZERO 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.

AZIENDA ZERO 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 precedentemete 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 AZIENDA ZERO.

5.3.2. Procedure di verifica delle informazioni relative al personale

AZIENDA ZERO, prima di assumere una persona o consentirgli l'accesso al posto di lavoro, compie accertamenti relativi a:

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

AZIENDA ZERO 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 n° 2016/679 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

AZIENDA ZERO 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.

La formazione include 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 AZIENDA ZERO;
- 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, AZIENDA ZERO 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

AZIENDA ZERO 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 AZIENDA ZERO. 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, affinchè quest'ultimo possa adempiere alle proprie attività in maniera competente e efficace.

5.4. Procedure di controllo per la sicurezza

5.4.1. Tipi di incidenti registrati

AZIENDA ZERO 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

AZIENDA ZERO 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.

AZIENDA ZERO 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

AZIENDA ZERO conserva le informazioni del giornale di controllo per un periodo di 20 anni.

5.4.4. Protezione dei registri di verifica

I Log dei sistemi:

- Sono protetti da eventuale manipolazione mediante firma digitale;
- Sonno 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

AZIENDA ZERO 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.

AZIENDA ZERO 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 AZIENDA ZERO.

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 stipula.

5.4.8. Analisi di vulnerabilità

Le analisi di potenziali vulnerabilità dell'infrastruttura di AZIENDA ZERO 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 periodocamente 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

AZIENDA ZERO 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 AZIENDA ZERO (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.

AZIENDA ZERO 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

AZIENDA ZERO 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

AZIENDA ZERO 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.
AZIENDA ZERO 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

AZIENDA ZERO 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.
AZIENDA ZERO esegue ogni giorno backup incrementali di tutti i dati elettronici e ogni settimana svolge backup completi in caso di recupero dei dati.
Inoltre, AZIENDA ZERO (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

AZIENDA ZERO 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

AZIENDA ZERO dispone di una procedura che descrive il processo per verificare che le informazioni archiviate siano corrette e accessibili. AZIENDA ZERO 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 AZIENDA ZERO la generazione di una nuova coppia di chiavi di CA.

Il certificato selfsigned 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, AZIENDA ZERO 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

AZIENDA ZERO, con il supporto degli Outsourcers, 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 AZIENDA ZERO, che includono escalation, ricerca e risposta alla criticità. Se necessario, verrà avviata la procedura di compromissione della chiave o di disaster recovery di

AZIENDA ZERO.

5.7.3. Compromissione della chiave privata della CA

In caso di sospetto o accertamento della compromissione da parte di AZIENDA ZERO, 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

AZIENDA ZERO 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 Azienda Zero, 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.

AZIENDA ZERO 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.

AZIENDA ZERO 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 datacenter dell'azienda outsourcee Bit4id s.r.l in via Diocleziano n. 107 – Napoli.

5.8. Cessazione del servizio

AZIENDA ZERO 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, AZIENDA ZERO garantisce una manutenzione continua dei registri per il tempo stabilito nella sezione 5 del presente Manuale Operativo.

Tuttavia, AZIENDA ZERO 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, AZIENDA ZERO sviluppa 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 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 AZIENDA ZERO, nonché qualsiasi altra circostanza rilevante che possa impedire il proseguimento dell'attività.

6. Misure di sicurezza tecnica

AZIENDA ZERO utilizza sistemi e tecniche affidabili atte a garantire la sicurezza tecnica dei processi implementati. Tutte le misure di sicurezza tecnica impiegate da AZIENDA ZERO

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

Azienda Zero CA Qualificata eIDAS 1	4.096 bits	25 anni
- Certificati di entità finale	2.048 bits	Fino a 3 anni
Azienda Zero TSA Qualificata eIDAS 1	4.096 bits	25 anni
- Certificati di Time Stamping Unit	2.048 bits	Fino a 8

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

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 AZIENDA ZERO 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. Distribuzione della chiave pubblica della CA

Le chiavi pubbliche di AZIENDA ZERO 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://azero.veneto.it 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 4096 bit;
- La lunghezza delle chiavi dei Certificati degli utenti finali è di 2048 bit. La lunghezza delle chiavi dei Certificati di TSU è di 2048 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 della chiave private e sicurezza dei moduli crittografici

6.2.1. Standard e sicurezza dei moduli crittografici

In relazione ai moduli che gestiscono le chiavi di AZIENDA ZERO, 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 risiede all'interno di un dispositivo crittografico hardware certificato Common Criteria livello EAL4+ o superiore, appropriato per l'uso previsto delle chiavi, in accord 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 TSAdi AZIENDA ZERO, 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

AZIENDA ZERO 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 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., QTSP e partner tecnologico di Azienda Zero cui la stessa ha conferito apposito incarico per l'archiviazione e la conservazione di queste.

Azienda Zero garantisce il possesso in Uanataca S.A. 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 AZIENDA ZERO.

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 AZIENDA ZERO 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 AZIENDA ZERO 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 o in caso di

6.2.10. Modalità di disattivazione della chiave privata

Nessuna stipula.

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 di questo documento.

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 AZIENDA ZERO 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, AZIENDA ZERO 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

AZIENDA ZERO utilizza sistemi affidabili per offrire i servizi di certificazione, messi a disposizione del partner tecnologico e QTSP UANATACA S.A.

AZIENDA ZERO e UANATACA effettuano 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, AZIENDA ZERO si avvale dei controlli dello schema di certificazione sui sistemi di gestione delle informazioni conformi ISO 27001 operati per conto dell'Outsourcee.
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 AZIENDA ZERO 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 AZIENDA ZERO sono affidabili.

6.6. Controlli tecnici del ciclo di vita

6.6.1. Controlli di sviluppo dei sistemi

Le applicazioni e i sistemi sono sviluppatimplementati e gestiti secondo gli standard di sviluppo e le procedure interne di change management. eLe 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 nella procedure di qualità ISO 9001 e nelle policy di sicurezza ISO 27001 degli outsourcee indicati nei paragrafi 1.3 e 1.3.4 del presente documento,

6.6.2. Controlli di gestione della sicurezza

AZIENDA ZERO 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. AZIENDA ZERO 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'architetturain 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 AZIENDA ZERO sono realizzate in moduli con

certificazioni FIPS 140-2 livello 3.

6.9. Riferimento temporale

AZIENDA ZERO 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 (QSCD)

Azienda Zero 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 elettronica qualificata a norma dell'art. 30, par. 3, lett. a) del Regolamento (UE) n. 910/2014.

Le norme cui si fa riferimento sono indicate nell'allegato alla Decisione di Esecuzione (UE) n. 650/2016 della Commissione del 25 aprile 2016.

In particolare, caso di modifiche dello stato di certificazione dei dispositivi qualificati di creazione di firma (QSCD), AZIENDA ZERO procederà come descritto di seguito:

1. Azienda Zero 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, AZIENDA ZERO 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, Azienda Zero 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, Azienda Zero 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. La documentazione relativa al profilo dei certificati emessi in conformità alla norma europea ETSI EN 319 412 può essere richiesta a AZIENDA ZERO.

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 AZIENDA ZERO (https://azero.veneto.it/ca/).

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 CRL

Le CRL emesse da AZIENDA ZERO sono conformi alla specifica pubblica RFC 5280.

7.2.1. Numero di versione

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

7.3. Profilo OCSP

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

8. Audit di conformità

In qualità di Prestatore di Servizi Fiduciari, AZIENDA ZERO è soggetta a periodiche verifiche di conformità.

8.1. Frequenza degli audit

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

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

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 AZIENDA ZERO 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 Azienda Zero 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 AZIENDA ZERO.

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

9. Condizioni economiche e legali

9.1. Tariffe

9.1.1. Tariffa per l'emissione o rinnovo del certificato

AZIENDA ZERO non ha previsto tariffe per l'emissione o il rinnovo dei certificati: la ragione di tale circostanza è che il servizio di certificazione sarà erogato da quest'ultima inizialmente solo in favore dei dipendenti delle Aziende Sanitarie della Regione Veneto.

Attualmente non è prevista l'emissione o rinnovo dei certificati in favore di soggetti terzi rispetto a quelli innanzi indicati.

AZIENDA ZERO, tuttavia, si riserva la facoltà di estendere successivamente il servizio anche a persone fisiche/giuridiche diverse dai dipendenti delle Aziende Sanitarie Locali: in tal caso, procederà a stabilire compiutamente le condizioni economiche delle tariffe per i servizi di certificazione erogati, informandone opportunatamente i richiedenti, tramite pubblicazione delle stesse sul proprio sito web istituzionale, assicurandone la concorrenzialità.

9.1.2. Tariffa per l'accesso ai certificati

Non è prevista alcuna tariffa economica per l'accesso ai certificati pubblicati. Tale accesso è libero e gratuito.

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

AZIENDA ZERO 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

Nessuna condizione.

9.2. Capacità finanziaria

In conformità a quanto stabilito dalla normativa tecnica europea, in relazione alla gestione dei

servizi di CA e al piano di cessazione delle attività, AZIENDA ZERO dispone di sufficienti risorse economiche necessarie a garantire l'operatività dei propri servizi, ad assicurare l'adempimento dei propri obblighi e ad affrontare i rischi eventualmente derivanti dall'erogazione del servizio di certificazione.

9.2.1. Copertura assicurativa

In virtù del rapporto di Partnership strategico con gli Outsourcee di cui al punto 1.3.4 del presente Manuale AZIENDA ZERO può contare sulla presenza di apposita polizza assicurativa stipulata a nome dell'Outsourcee, con società di verificata importanza in campo assicurativo.

La predetta polizza assicurativa è stipulata per lo specifico esercizio delle 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 rimanda al par. 9.2.1.

9.3. Tutela delle informazioni trattate

9.3.1. Informazioni confidenziali

AZIENDA ZERO si impegna a trattare e gestire come confidenziali 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 AZIENDA ZERO nel rispetto delle norme applicabili, in particolare del D.lgs. 196/03 e ss.mm.ii.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

AZIENDA ZERO divulga le informazioni considerate confidenziali, ai sensi del par. 9.3.1., nei soli casi in cui ricorra un obbligo giuridico/normativo di divulgazione.

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 ss.mm., 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 AZIENDA ZERO, delle informazioni confidenziali ed, 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

Per quanto riguarda il trattamento e la protezione dei dati personali, AZIENDA ZERO rispetta la normativa vigente in materia, sia nazionale che comunitaria, con particolare riferimento al D.lgs. 196/03, e s.m.i., ed il Regolamento (UE) 2016/679 (di seguito anche solo "GDPR").

In conformità alle disposizioni normative in materia di tutela dei dati personali, AZIENDA ZERO ha illustrato, nel presente Manuale, quali procedure organizzative e di sicurezza 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 rendono, più nel dettaglio, le informazioni relative al trattamento dei dati personali realizzato da AZIENDA ZERO:

- Titolare del trattamento

Titolare del trattamento dei dati personali, ai sensi dell'art. 4, n. 7 del GDPR, è AZIENDA ZERO, Passaggio Luigi Gaudenzio, 1, 35131 Padova PEC: protocollo.azero@pecveneto.it.

AZIENDA ZERO è titolare dei dati personali raccolti in fase di identificazione e registrazione degli utenti che richiedono certificati e si obbliga quindi a trattare tali dati con la massima riservatezza e nel rispetto di quanto previsto dal D.lgs. 196/03, e s.m.i., nonché dal Regolamento (UE) 2016/679.

- Finalità del trattamento

Il trattamento dei dati personali da parte di AZIENDA ZERO si svolge per le seguenti finalità:

- fornitura di servizi fiduciari qualificati: i dati vengono raccolti attraverso il relativo contratto ed elaborati al fine di eseguire i servizi fiduciari richiesti ed accettati dal contraente, secondo le procedure indicate nel presente documento;
- inviare domande e richieste: i dati sono raccolti attraverso il modulo di contatto disponibile sul sito web di AZIENDA ZERO ed utilizzati esclusivamente per gestire le domande e le richieste ricevute.

I dati personali forniti non saranno trattati per finalità diverse da quelle sopra descritte né in modo incompatibile con le stesse.

- Base giuridca del trattamento

La base giuridica legittimante il trattamento dei dati personali degli utenti è la seguente:

a) il trattamento dei dati personali per la prestazione di servizi fiduciari qualificati deriva dall'esecuzione del contratto per i servizi richiesti, di cui l'utente è parte;
b) il trattamento per la gestione di domande e richieste si fonda sul consenso

dell'interessato, fornito espressamente ed inequivocabilmente da quest'ultimo, presa visione dell'informativa sul trattamento dei dati personali. Detto consenso può essere ritirato in qualsiasi momento inviando una e-mail a supporto.ca@azero.veneto.it .

- Tipologia di dati trattati

Per dati trattati, nel contesto della presente informativa, si intendono i cd. "Dati Personali" e cioè quelle informazioni o frammenti di informazioni che permettono l'identificazione del/dei Richiedente/i.
Solitamente queste includono informazioni come il nome, l'indirizzo di residenza o di domicilio, l'indirizzo di posta elettronica e il numero di telefono, o altre informazioni come, per esempio, l'Azienda presso la quale il Richiedente opera o presta servizio, il ruolo ricoperto e il settore di attività.

- Conservazione e cancellazione dei dati personali

AZIENDA ZERO conserverà i dati degli interessati in una forma che consenta l'identificazione degli stessi per un arco temporale non superiore al conseguimento delle finalità per le quali i dati sono stati raccolti. I dati relativi ai Certificati e/o all'Identità digitale verranno conservati per 20 (venti) anni dalla cessazione del contratto ovvero dalla scadenza o dalla revoca del Certificato o dell'Identità digitale, conformemente a quanto stabilito dall'art.28, co.4bis del D. Lgs. 82/2005 e s.m.i. Codice dell'Amministrazione Digitale) e dell'art. 7, co.8 del DPCM 24 ottobre 2014 e s.m.i.. I dati strettamente necessari per gli adempimenti fiscali e contabili, venuta meno la finalità per la quale erano stati raccolti, verranno conservati per un periodo di 10 (dieci) anni come richiesto dalle normative in materia. I log di servizio relativi ai Certificati e/o all'Identità digitale verranno conservati per un periodo pari a 6 (sei) mesi al fine di garantire la corretta individuazione dei flussi dei servizi.
Decorsi tali periodi, AZIENDA ZERO provvederà alla cancellazione dei dati degli interessati.

- Eventuali destinatari o categorie di destinatari dei dati personali

I Trattamenti connessi ai servizi forniti da Azienda saranno curati solo da personale incaricato del Trattamento, oppure da eventuali incaricati di occasionali operazioni di manutenzione per tutto il tempo necessario ad assicurare la regolare fruizione dei servizi richiesti.

I Dati acquisiti tramite le procedure di identificazione e registrazione saranno anche direttamente comunicati e trattati dai partner tecnologici e strumentali di cui la CA si avvale per l'erogazione dei servizi richiesti (tra Uanataca S.a., ADAM ecc...)

I servizi forniti dai predetti partner (o anche terzi) vengono utilizzati dalla CA per fornire i propri servizi.

I dati relativi al contratto e all'attività relativa ai servizi fiduciari qualificati possono essere comunicati, altresì, a consulenti commerciali per finalità amministrative e contabili, nonché a consulenti legali per eventuale gestione di contenziosi.
Inoltre, i dati possono essere comunicati anche a organi di polizia o all'autorità giudiziaria per finalità di accertamento o repressione di reati compiuti dagli utenti dei servizi telematici, ove necessario.
I dati potranno essere trattati anche da soggetti terzi in qualità di Autorità di Registrazione, Operatore di Registrazione, nonché da soggetti con funzione di gestione ed archiviazione cartacea e/o digitale, formalmente nominati da AZIENDA ZERO quali responsabili/sub responsabili esterni del trattamento dati.

- Diritti degli interessati

I Richiedenti e tutte le persone interessate hanno diritto di ottenere l'indicazione dell'origine dei Dati Personali, delle finalità e delle modalità con cui questi ultimi vengono trattati e della logica applicata in caso di Trattamento effettuato con l'ausilio di strumenti elettronici, così come degli estremi identificativi del Titolare del Trattamento dei Dati Personali, dei rappresentati di questi ultimi e dei soggetti o delle categorie di soggetti ai quali i Dati Personali possono essere comunicati o che possono venirne a conoscenza.
In particolare, il Richiedente o l'Interessato, ai sensi del GDPR possiede i seguenti diritti:

1) DIRITTO DI ACCESSO AI DATI PERSONALI: ai sensi dell'art. 15 del GDPR (rubricato "Diritto di accesso dell'interessato") il Richiedente o l'Interessato ha diritto di ottenere dal Titolare del Trattamento la conferma che sia o meno in corso un Trattamento di Dati Personali che lo riguardano e in tal caso, di ottenere l'accesso ai Dati Personali in possesso di questo. 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") il Richiedente o l'Interessato hanno diritto di ottenere dal Titolare del Trattamento la rettifica dei Dati Personali inesatti che li 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»)") il Richiedente o l'Interessato hanno diritto di ottenere la cancellazione dei Dati Personali che li riguardano dal Titolare del Trattamento; sarà quindi onere di Azienda Zero 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 alla portabilità dei Dati") 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. Con la lettura del presente Manuale Operativo, messo a disposizione del Richiedente, quest'ultimo si ritiene informato di tale diritto.
8) DIRITTO DI OPPOSIZIONE ALLA PROFILAZIONE E AL TRATTAMENTO AUTOMATIZZATO: ai senti dell'art. 22 il Richiedente o 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.

Per esercitare i propri diritti, gli interessati possono inviare una richiesta all'indirizzo email aagg.assicurativi@azero.veneto.it. In questa richiesta, bisognerà allegare una copia del proprio documento di identità ed indicare chiaramente quale diritto si desidera esercitare.

L'informativa sul trattamento dei dati personali è pubblicata sul sito web di AZIENDA ZERO.

La richiesta del certificato richiede la manifestazione del consenso, da parte del Richiedente, al trattamento dei propri dati personali da parte della CA.

9.5. Diritti di proprietà intellettuale

9.5.1. Proprietà dei certificati

Sui certificati emessi AZIENDA ZERO gode dei diritti di proprietà intellettuale.

9.5.2. Proprietà del Manuale Operativo – Servizi di Certificazione digitale

Questo Manuale Operativo è proprietà intellettuale di AZIENDA ZERO. Tutti i diritti sono riservati.

9.5.3. Proprietà dei marchi

I marchi e i marchi registrati, utilizzati dai Richiedenti del certificato, sono di proprietà esclusiva dei rispettivi titolari.

I Richiedenti del certificato 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 si obbligano a manlevare e indennizzare AZIENDA ZERO 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 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.

I Titolari e i Richiedenti del certificato si obbligano a manlevare e indennizzare AZIENDA ZERO contro qualunque perdita o danno derivanti da una tale interferenza o infrazione.

9.6. Garanzie e responsabilità

9.6.1. Garanzie offerte da AZIENDA ZERO

AZIENDA ZERO si impegna a:

- erogare il servizio di certificazione in conformità a questo 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 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, AZIENDA ZERO 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) fornisce l'informativa prevista dal Reg. europeo 2016/679;

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

AZIENDA ZERO non ha ulteriori obblighi e non garantisce nulla più di quanto espressamente previsto dalla normativa vigente in materia ovvero indicato nel presente Manuale e nelle Condizioni Generali di Fornitura relative ai servizi di certificazione digitale.

9.6.3. Limitazioni di responsabilità

Azienda Zero 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 ad Azienda Zero 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, AZIENDA ZERO potrà essere ritenuta responsabile nei confronti del Richiedente e/o Titolare, ovvero verso altri soggetti, direttamente o indirettamente, connessi o collegati a questi ultimi l, 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 AZIENDA ZERO.

In particolare, ai sensi dell'art. 13 della normativa eIDAS su richiamata AZIENDA ZERO 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. Indennizzi a favore di AZIENDA ZERO

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 AZIENDA ZERO, 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.

9.6.5. Indennizzi ai contraenti

Fermo quanto previsto dalle Condizioni Generali di Contratto relative ai servizi di certificazione, AZIENDA ZERO dispone, per mezzo dell'Outsourcee, 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 ad AZIENDA ZERO 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.

9.6.6. 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 Azienda Zero 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.

9.6.7. Cessione del contratto

Non è consentito all'Utente la cessione di tutto o parte degli obblighi e dei diritti nascenti da tale contratto.

9.6.8. Legge applicabile

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

9.6.5. Foro competente

Nel contratto concluso con il Richiedente e/o il Titolare sono contenute clausole relative alla risoluzione delle dispute che dovessero insorgere tra le Parti.

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

Azienda Zero 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 ad Azienda Zero, 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 dei certificati elettronici qualificati

Indicazione del Sistema di verifica della firma

AZIENDA ZERO, in conformità a quanto previsto dall'art. 14 co.1 del D.P.C.M. del 22 febbraio 2013, fornisce ed indica ai soggetti interessati un applicativo che permette la verifica dei certificati di firma elettronica qualificata e digitale apposta su documenti informatici (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

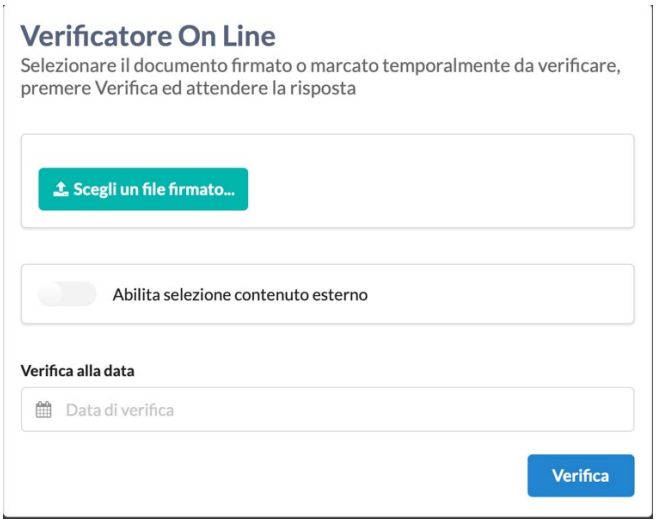
Il predetto software consente, nello specifico, di verificare:

a. l'identità del documento firmato e i dati del soggetto firmatario;
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 verificare il certificato di una firma qualificata o digitale 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.