CEDACRI

Manuale Operativo Firma Elettronica Qualificata Cedacri - CP e CPS

17-06-2025

Unrestricted

Legal Notices

Contenuti

Scopo e ambito di applicazione

Scopo

Lo scopo del presente documento è quello di delineare le politiche e le pratiche seguite nel processo di identificazione ed emissione di un certificato qualificato ("Certificato Qualificato") in conformità con la vigente normativa in materia di servizi fiduciari, firma elettronica qualificata e firma digitale.

Ambito di applicazione

Il presente documento ha validità per il Gruppo Cedacri.

1 Definizioni e abbreviazioni

Oltre a quanto riportato nel "Glossario" (rif. PR00018A2 – Glossario, allegato alla Procedura di Gestione della Documentazione) che contiene le definizioni e abbreviazioni applicabili a tutta la documentazione interna aziendale, si riportano qui di seguito le definizioni e abbreviazioni specifiche che troveranno applicazione solo per il presente documento.

Dal regolamento europeo 910/2014 eIDAS, Art 3:

- "identificazione elettronica": è il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;
- "mezzi di identificazione elettronica": è un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;
- "dati di identificazione personale": un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;
- "regime di identificazione elettronica": è un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche;
- "autenticazione": è un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica;
- "parte facente affidamento sulla certificazione": è una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario;
- "organismo del settore pubblico": è un'autorità statale, regionale o locale, un organismo di diritto pubblico o un'associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un'autorità, un organismo o un'associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato;
- "organismo di diritto pubblico": è un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio (1);
- "firmatario": una persona fisica che crea una firma elettronica;
- "firma elettronica": la firma elettronica è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti cartacei ;
- "firma elettronica avanzata": è una firma elettronica che soddisfi i requisiti di cui all'articolo 26;
- "firma elettronica qualificata": è una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;
- "dati per la creazione di una firma elettronica": si intende dati unici utilizzati dal firmatario per creare una firma elettronica;

- “certificato di firma elettronica”: si intende un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;
- “certificato qualificato di firma elettronica”: è un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all’allegato I;
- “servizio fiduciario”: è un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:
  - a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure
  - b) creazione, verifica e convalida di certificati di autenticazione di siti web; o
  - c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;
- “servizio fiduciario qualificato”: si intende un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;
- “organismo di valutazione della conformità”: è un organismo ai sensi dell’articolo 2, punto 13, del regolamento (CE) n. 765/2008, che è accreditato a norma di detto regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati;
- “prestatore di servizi fiduciari”: è una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;
- “prestatore di servizi fiduciari qualificato”: è un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l’organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;
- “prodotto”: è un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;
- “dispositivo per la creazione di una firma elettronica”: è un software o hardware configurato utilizzato per creare una firma elettronica;
- “dispositivo per la creazione di una firma elettronica qualificata”: è un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all’allegato II;
- “creatore di un sigillo”: è una persona giuridica che crea un sigillo elettronico;
- “sigillo elettronico”: si intende dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l’origine e l’integrità di questi ultimi;
- “sigillo elettronico avanzato”: si intende un sigillo elettronico che soddisfi i requisiti sanciti all’articolo 36;
- “sigillo elettronico qualificato”: si intende un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;
- “dati per la creazione di un sigillo elettronico”: i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

- “certificato di sigillo elettronico”: si intende un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;
- “certificato qualificato di sigillo elettronico”: si intende un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all’allegato III;
- “dispositivo per la creazione di un sigillo elettronico”: è un software o hardware configurato utilizzato per creare un sigillo elettronico;
- “dispositivo per la creazione di un sigillo elettronico qualificato”: è un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all’allegato II;
- “validazione temporale elettronica”: sono dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;
- “validazione temporale elettronica qualificata”: è una validazione temporale elettronica che soddisfa i requisiti di cui all’articolo 42;
- “documento elettronico”: si intende qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;
- “servizio elettronico di recapito certificato”: è un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell’avvenuto invio e dell’avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;
- “servizio elettronico di recapito qualificato certificato”: è un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all’articolo 44;
- “certificato di autenticazione di sito web”: è un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;
- “certificato qualificato di autenticazione di sito web”: è un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all’allegato IV;
- “dati di convalida”: sono dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;
- “convalida”: si intende il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.
- QTSP: Qualified Trust Service Provider – Prestatore di Servizi Fiduciari Qualificato
- CA: Certification Authority
- HSM: Hardware Security Module
- HA: High Availability (Alta affidabilità)
- CRL: Certificate Revocation List
- OCSP: Online Certificate Protocol Status
- TSA: Time Stamp Authority
- TSU: Time Stamp Unit

- QSCD: Qualified Signature Creation Device
- RAO: Registration Authority Operator
- RA: Registration Authority (Autorità di Registrazione)

2 Introduzione

2.1 Quadro generale

La firma digitale permette ad un soggetto di manifestare l'autenticità e l'integrità di un documento informatico attraverso l'impiego di una coppia di chiavi asimmetriche (una pubblica ed una privata) in modo che chiunque venga in possesso di tale documento possa sempre verificarne la piena validità.

Il presente documento costituisce il Manuale Operativo del Prestatore di Servizi Fiduciari Qualificato (Qualified Trust Service Provider – "QTSP"), nel seguito anche "Cedacri" quale fornitore dei servizi di firma elettronica qualificata.

Il manuale contiene le politiche e le pratiche seguite nel processo di identificazione ed emissione di un certificato qualificato ("Certificato Qualificato") in conformità con la vigente normativa in materia di servizi fiduciari, firma elettronica qualificata e firma digitale.

Pubblicando tale Manuale Operativo e inserendo i riferimenti a tale documento nei certificati, si consente agli utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione e quindi del legame tra chiave e Soggetto.

Il contenuto si basa sulle norme vigenti alla data di emissione.

2.2 Identificativo del documento

Al documento è associato l'object identifier (OID); quello che identifica Cedacri è 1.3.76.27 Questo documento è pubblicato in formato elettronico presso il sito Web del QTSP all'indirizzo: https://www.cedacricert.it/, sezione "Documentazione".

2.3 Partecipanti e responsabilità

2.3.1 Certification Authority – Autorità di Certificazione

La Certification Authority è il soggetto terzo e fidato che emette i certificati qualificati di firma digitale, firmandoli con la propria chiave privata, detta chiave di CA o chiave di root.

Cedacri è la Certification Authority ("CA") che emette, pubblica nel registro e revoca i Certificati Qualificati, operando in conformità alle regole tecniche emanate dall'Autorità di Vigilanza e secondo quanto prescritto dal Regolamento eIDAS e dal Codice dell'Amministrazione Digitale.

I dati completi dell'organizzazione che svolge la funzione di CA sono i seguenti:

Ragione Sociale	***Cedacri S.p.A.***
Sede legale	***Corso Monforte, 30*** ***20122 Milano (Milano)***

Legale Rappresentante ***nato a*** ***funzione***	***Luca Peyrano*** ***Milano (Milano), 09 gennaio 1971*** ***Legale Rappresentante***
N. Iscrizione al Registro delle Imprese di Milano Monza Brianza Lodi	***00432960342***
Partita IVA	***00432960342***
Gruppo IVA	***02952290340***
Codice ABI	***89002***
UNINFO Object Identifier (OID)	***1.3.76.27***
ISO-OID P.E.N.	***8414***
N° telefonico	***0521 8071 (centralino)***
N° di Fax	***0521 807373***
Indirizzo Internet	www.cedacricert.it
Indirizzo di posta elettronica	servizifiduciari-cedacri@iongroup.com
Indirizzo di posta elettronica certificata	servizifiduciari@postacert.cedacri.it

La CA adotta le misure tecniche e organizzative idonee per un tale servizio.

In particolare, il Certificatore:

- si accerta dell'identità della persona che fa richiesta di Certificato;
- rilascia il relativo Certificato qualificato nelle modalità previste;
- informa i titolari sulle caratteristiche del servizio;
- adotta le necessarie misure di sicurezza per il trattamento dei dati personali;
- garantisce che il dispositivo sicuro per la generazione della firma abbia le caratteristiche richieste dai regolamenti;
- garantisce che il soggetto titolare mantenga sempre in modo esclusivo il controllo delle proprie chiavi di firma;
- garantisce che le chiavi private di firma generate all'interno degli HSM non possano essere esportate;
- mantiene aggiornata la lista dei Certificati revocati;
- mantiene aggiornata la lista dei Certificati sospesi;
- gestisce tutte le procedure necessarie ai fini delle attività di cui sopra, secondo adeguate norme di sicurezza;
- mantiene le registrazioni di tutte le informazioni relative alla gestione del certificato qualificato per almeno venti anni.

2.3.2 Registration authority ("RA")

Il Certificatore può dare mandato a svolgere le funzioni di Ente di registrazione o Registration Authority verso banche, istituti di credito o altre entità che avranno sottoscritto con il Certificatore uno specifico contratto.

Il ruolo di Ente di registrazione o Registration Authority è svolto da personale esplicitamente autorizzato e formato dal QTSP.

L'operatore:

- identifica con certezza l'utente che richiede la Certificazione di una Chiave pubblica;
- invia al QTSP la domanda di Certificazione dell'utente;
- archivia copia del contratto firmato dall'utente con copia del documento d'identità allegata;
- fornisce all'utente il necessario per perfezionare la procedura di richiesta Certificato.

L'elenco degli Enti di registrazione verrà pubblicati sul sito web www.cedacricert.it.

Al momento la mansione di Ente di registrazione è svolta da Cedacri.

2.3.3 Soggetto

Il Soggetto (o "Titolare") è la persona fisica titolare del certificato qualificato, all'interno del quale sono inseriti i dati identificativi fondamentali. Il Soggetto è tenuto a:

- fornire al QTSP, tutte le informazioni necessarie all'atto della richiesta del Certificato;
- utilizzare la Chiave privata per i soli scopi per i quali la corrispondente Chiave pubblica è stata certificata;
- custodire diligentemente il Dispositivo di firma;
- custodire le informazioni di abilitazione all'uso della Chiave privata (P.I.N. del Dispositivo di firma) in un luogo diverso dal dispositivo contenente la chiave;
- richiedere immediatamente la revoca del Certificato in caso di smarrimento, furto, deterioramento o distruzione del Dispositivo di firma;
- richiedere immediatamente la revoca del Certificato in caso di certezza di compromissione della Chiave privata utilizzata;
- cessare l'utilizzo della coppia di chiavi una volta che il Certificato è scaduto;
- comunicare un indirizzo di e-mail valido;
- informare il QTSP di eventuali successive variazioni del proprio indirizzo e-mail, inviando un messaggio di posta elettronica firmato con il proprio Certificato all'indirizzo: servizifiduciari-cedacri@iongroup.com;
- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- comunicare tempestivamente al QTSP le variazioni dei propri dati identificativi e/o dei poteri di rappresentanza o di altri titoli relativi all'attività o a cariche rivestite (modifica, cessazione, revoca).

Il QTSP non è responsabile dei danni causati al Soggetto, agli Utenti Utilizzatori, ed ai terzi del mancato rispetto, da parte del Soggetto, degli obblighi in qualità di Titolare e degli obblighi di cui al presente Manuale Operativo.

Il QTSP, ferma restando la facoltà di revocare o sospendere il Certificato, potrà risolvere in qualsiasi momento, ai sensi dell'articolo 1456 del Codice Civile, il rapporto contrattuale in

essere con il Titolare, qualora questi non adempia anche ad uno solo degli obblighi previsti dal presente paragrafo.

2.3.4 Utente

L'Utente è la persona che riceve un documento informatico sottoscritto con il certificato digitale del Soggetto.

L'Utente è tenuto a svolgere almeno le seguenti verifiche:

- verificare che la tipologia del certificato utilizzato per la firma sia coerente a quanto indicato all'art. 5 comma 4 del DPCM;
- verificare le liste dei certificati revocati e sospesi pubblicata dal Certificatore per assicurarsi che il certificato fosse valido al momento della firma;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato;
- verificare che il certificato sia stato rilasciato da un certificatore pubblicato nelle liste reperibili presso Agenzia per l'Italia Digitale.

I dati dei Titolari non possono essere usati per comunicazioni non richieste, quali pubblicità o simili, anche se sono pubblicati.

2.3.5 Richiedente

Il Richiedente è la persona fisica o giuridica che richiede alla CA il rilascio di certificati digitali per un Soggetto, eventualmente sostenendone i costi e assumendo la facoltà di sospendere o revocare i certificati stessi. Tale ruolo, può eventualmente essere assunto anche dalla RA.

Il Richiedente:

- può coincidere con il Soggetto, se questi è una persona fisica;
- può essere la persona giuridica che richiede il certificato per persone fisiche a essa legate da rapporti commerciali ovvero nell'ambito di organizzazioni.

Il Richiedente può essere la persona fisica o giuridica da cui discendono i poteri di firma o il ruolo del Soggetto. In questo caso, dove il Richiedente viene anche definito Terzo Interessato, viene inserita nel certificato l'indicazione dell'Organizzazione a cui il Soggetto stesso è collegato, e/o del relativo ruolo.

Se non diversamente specificato nella documentazione contrattuale, il Richiedente coincide con il Soggetto.

2.3.6 RAO (Registration Authority Operator)

I RAO sono gli addetti alle attività di Identificazione, raccolta e trasmissione documentazione e alla registrazione di utenti.

I RAO vengono selezionati tra il personale del QTSP e vengono abilitati ad operare in seguito alla stipula di un mandato e solamente dopo avere seguito un corso di formazione.

Al termine di questo processo, agli operatori viene dato accesso agli strumenti telematici sicuri messi a disposizione dalla CA e necessari per consentire lo svolgimento delle attività RAO.

2.3.7 Autorità

Agenzia per l'Italia Digitale -AgID

L'Agenzia per l'Italia Digitale (AgID), è l'organismo di vigilanza sui prestatori di servizi fiduciari, ai sensi dell'articolo 17 del Regolamento eIDAS.

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, che è competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati alle normative e agli standard applicabili.

2.4 Utilizzo del certificato

2.4.1 Utilizzi consentiti

I certificati emessi dalla CA 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 Soggetto cui il certificato appartiene.

Le policy dei certificati per l'apposizione di firme contenute in questo Manuale Operativo sono identificate dai seguenti OID:

Cedacricert OID	ETSI OID	Agid OID	Descrizione
1.3.76.27.1.1.2.4	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD for Remote Signature.
1.3.76.27.1.1.2.3	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD for Remote Signature - Customer user notice.
1.3.76.27.1.1.2.1	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons with QSCD.

Tabella 1 – Policy dei certificati per l'apposizione delle firme

Cedacri mette a disposizione dei propri clienti un tool di firma e verifica che consente di apporre e verificare firme digitali in formato standard nonché di richiedere e verificare marche temporali.

Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.

2.4.2 Utilizzi non consentiti

È vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel Manuale Operativo e dai contratti, e comunque in violazione dei limiti d'uso e di valore (key usage, usernotice) previsti.

2.5 Amministrazione del Manuale Operativo

2.5.1 Contatti

È attivo un servizio di Call Center indirizzato all'utenza del servizio per qualsiasi tipo di informazione riguardo le procedure descritte nel presente manuale, Il servizio è attivo tutti i giorni, festivi compresi, con orario continuativo nelle **24 ore, al numero 840 033033**.

2.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

Il responsabile del presente documento è il CISO - Chief Information Security Officer di Cedacri.

2.5.3 Procedure di approvazione

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità ISO 9001.

Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

2.5.4 Revisione del Manuale Operativo

Ogni nuova versione del Manuale Operativo annulla e sostituisce la precedente; tuttavia, i certificati emessi durante la loro vigenza rimangono validi fino alla scadenza degli stessi.

Ogni modifica tecnica o procedurale che implica cambiamenti rilevanti, la CA deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (CAR – Conformity Assessment Report) e il manuale operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

È garantita almeno una revisione annuale del Manuale Operativo.

2.5.5 Pubblicazione

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito: https://www.cedacricert.it/cedacricert/it/documentazione/
- in formato elettronico nell'elenco pubblico dei certificatori tenuto da AgID;

può essere richiesto in formato cartaceo a: auditing-cedacri@iongroup.com

3 Pubblicazione e archiviazione

3.1 Archiviazione

I certificati pubblicati, le CRL e i manuali operativi sono pubblicati e disponibili 24 ore al giorno per 7 giorni alla settimana.

3.2 Pubblicazione delle informazioni sulla certificazione

3.2.1 Informazioni pubblicate

Attraverso il proprio sito web, viene pubblicata la seguente documentazione:

- Manuale Opertivo Firma Elettronica Qualificata – CP e CPS;
- PKI Disclosure statements;
- Termini e condizioni di contratto dei servizi;
- Certificati di CA;
- CRL – Liste di revoca dei certificati;
- Modulistica.

3.2.2 Pubblicazione del manuale operativo

Il presente Manuale Operativo è reperibile in formato elettronico presso il sito web del QTSP.

Il presente Manuale Operativo, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative alla CA previste dalla legge sono pubblicati presso l'elenco dei certificatori.

3.2.3 Pubblicazione dei certificati

Gli elenchi dei Certificati in vigore (previa autorizzazione del Soggetto alla pubblicazione), possono essere disponibili sul sito https://www.cedacricert.it.

3.2.4 Pubblicazione delle liste di revoca e sospensione

Le liste dei certificati revocati ("CRL") sono disponibili sul sito https://www.cedacricert.it/.

3.3 Periodo o frequenza di pubblicazione

3.3.1 Frequenza di pubblicazione del manuale operativo

Il Manuale Operativo viene pubblicato con frequenza variabile in caso di cambiamenti.

Se i cambiamenti sono importanti, il QTSP deve sottoporsi ad audit di un CAB accreditato, presentare il rapporto di certificazione (*CAR – Conformity Assessment Report*) e il manuale operativo all'Autorità di vigilanza (AgID) ed attendere il permesso per la pubblicazione.

3.3.2 Frequenza pubblicazione delle liste di revoca e sospensione

I Certificati revocati vengono inseriti nella CRL emessa dal QTSP, che viene marcata temporalmente e pubblicata.

La pubblicazione ordinaria della suddetta lista, con validità di 24 ore, avviene con cadenza giornaliera, ogni ora.

In caso di richiesta di revoca immediata, la lista CRL sarà prontamente pubblicata.

3.3.3 Controllo degli accessi agli archivi pubblici

Le informazioni relative ai certificati pubblicati, alle CRLs e i manuali operativi sono pubbliche, e opportunamente protette.

4 Identificazione e autenticazione

4.1 Denominazione

4.1.1 Tipologie di nomi

L'identificatore del Soggetto è il Distinguished Name ("DN"), che consiste in una stringa formattata estesa dei dati anagrafici del soggetto stesso, emesso secondo gli standard RFC 5280, ETSI e le indicazioni del DPCM.

L'attributo del certificato Il DN identifica in maniera univoca il soggetto al quale è rilasciato il certificato.

4.1.2 Anonimato e pseudonimia dei richiedenti

L'anonimato non è consentito, mentre lo pseudonimato è regolato da regolamento EIDAS secondo art. 5 Par.2 e CAD.

4.1.3 Regole di interpretazione dei tipi di nomi

Le regole di interpretazione dei tipi di nomi sono regolate dalle normative ETSI EN 319 412-2 Par 4.2.4.

4.1.4 Univocità dei nomi

Nel caso di persona fisica, per garantire l'univocità del Soggetto, nel certificato deve essere indicato il nome e cognome e un codice identificativo univoco:

- il Codice Fiscale per i cittadini italiani;
- il TIN – Tax Identification Number per i cittadini stranieri. Il TIN può essere stato assegnato dalle autorità del Paese di cui il Soggetto è cittadino ovvero dal Paese in cui ha la sede l'organizzazione in cui lo stesso lavora.

In assenza di Codice Fiscale o TIN, nel certificato potrà essere inserito un codice identificativo tratto da un documento di identità valido, utilizzato nell'ambito delle procedure di riconoscimento.

4.2 Convalida iniziale dell'identità

Questo paragrafo descrive le procedure utilizzate per l'identificazione del Soggetto o del Richiedente al momento della richiesta di rilascio del certificato qualificato.

La procedura di identificazione comporta che il Soggetto sia riconosciuto dalla CA, anche attraverso una eventuale RA o un suo Incaricato, che ne verificherà l'identità attraverso la modalità definita nel Manuale Operativo.

4.2.1 Possesso della chiave privata

Cedacri stabilisce che il richiedente possiede o controlla la chiave privata corrispondente alla chiave pubblica da certificare, verificando la firma con la chiave pubblica da certificare.

4.2.2 Autenticazione dell'identità delle organizzazioni

n/a

4.2.3 Identificazione della persona fisica

Prima di poter procedere all'effettivo rilascio del certificato, è necessario memorizzare negli archivi del Certificatore i dati del Soggetto. Tale processo viene portato a termine dal QTSP tramite l'operatore dedicato alla funzione di Ente di registrazione (RAO) e si svolge come segue:

- il Richiedente contatta Cedacri tramite i canali dedicati (servizifiduciari-cedacri@iongroup.com o sistema di trouble ticketing);
- il RAO effettua il riconoscimento dell'utente secondo la normativa vigente;
- il RAO produce la documentazione contrattuale a partire dal modulo di richiesta predefinito, su cui vengono inseriti i dati anagrafici dell'utente; la documentazione viene firmata per accettazione dall'utente;
- il RAO si collega al sistema Cedacricert ed effettua l'autenticazione al sistema;
- il RAO procede alla registrazione inserendo i dati anagrafici del Richiedente, oltre a tutte le informazioni necessarie alla sua gestione successiva.

Come definito nell'articolo 24 del regolamento EIDAS, il QTSP verifica, l'identità e, se del caso, eventuali attributi specifici della persona fisica a cui il certificato qualificato è rilasciato. Le informazioni sono verificate dal prestatore di servizi fiduciari qualificato direttamente mediante la presenza della persona fisica, attraverso la propria infrastruttura di riconoscimento remoto, attraverso la verifica di una firma digitale qualificata (emessa da un prestatore di servizi fiduciari qualificati) apposta sul modulo di richiesta di certificato. Alla ricezione del documento firmato, Cedacri verificherà la validità della firma e la corrispondenza dei dati dell'intestatario del certificato qualificato con i dati inseriti all'interno del modulo di richiesta.

Il RAO deve accertarsi che il Richiedente abbia fornito tutte informazioni necessarie alla identificazione, corredate dalla idonea documentazione.

I dati indispensabili per l'emissione del certificato che il Richiedente deve obbligatoriamente fornire, sono i seguenti:

- cognome e nome
- data e luogo di nascita
- codice fiscale
- indirizzo di residenza
- indirizzo e-mail

È inoltre indispensabile verificare la presenza di un documento di identità in corso di validità e del codice fiscale del Richiedente.

Nel caso in cui venga richiesto l'utilizzo dello pseudonimo in luogo dei propri dati reali all'interno del certificato, Cedacri in qualità di QTSP conserverà le informazioni relative alla reale identità del Richiedente per 20 anni.

Qualora venga richiesto, direttamente dal Richiedente, o con il consenso dell'eventuale Terzo Interessato, l'inserimento nel certificato di sottoscrizione di informazioni relative a Funzioni, Titoli e/o Abilitazioni Professionali e Poteri di Rappresentanza, il RAO deve accertarsi che il Richiedente, oltre alla documentazione e alle informazioni identificative necessarie, abbia prodotto anche la documentazione idonea a dimostrare l'effettiva sussistenza dello specifico Ruolo anche mediante Autocertificazione.

La ragione sociale o la denominazione e il codice identificativo dell'Organizzazione saranno invece riportate nel certificato se la stessa ha richiesto o autorizzato il rilascio del certificato al Soggetto, anche senza l'esplicita indicazione di un ruolo.

Per quanto concerne l'inserimento nel certificato di limiti di valore degli atti unilaterali e dei contratti per i quali il certificato stesso può essere utilizzato, rimane responsabilità del Richiedente verificare il rispetto dei limiti d'uso inseriti nel certificato.

La richiesta di inserire specifiche limitazioni d'uso deve essere valutata dal QTSP per gli aspetti legali, tecnici e di interoperabilità.

4.2.4 Identificazione della persona giuridica

n/a

4.2.5 Informazioni del Soggetto o del Richiedente non verificate

n/a

4.2.6 Validazione dell'autorità

Cedacri ovvero la RA verifica le informazioni richieste, definite nei paragrafi 4.2.3 e 4.2.4, per l'identificazione e valida la richiesta.

5 Operatività

5.1 Richiesta del certificato

5.1.1 Chi può richiedere un certificato

Il certificato qualificato per una persona fisica può essere richiesto da:

- il Soggetto rivolgendosi direttamente a Cedacri mediante i riferimenti reperibili sul sito www.cedacricert.it oppure rivolgendosi ad una Registration Authority (se presente);
- il Richiedente per conto del Soggetto rivolgendosi direttamente a Cedacri mediante i riferimenti reperibili sul sito www.cedacricert.it oppure rivolgendosi ad una Registration Authority (se presente).

5.1.2 Processo di iscrizione e responsabilità

Il processo di iscrizione comprende: la richiesta da parte del Soggetto, la generazione della coppia di chiavi, la richiesta di certificazione della chiave pubblica e la firma dei contratti. Di seguito i ruoli dei sei versi soggetti coinvolti nel processo:

- il Soggetto ha la responsabilità di fornire informazioni corrette e veritiere sulla propria identità, di leggere attentamente il materiale messo a disposizione da Cedacri, anche attraverso la RA, di seguire le istruzioni della CA e/o della RA nell'avanzare la richiesta del certificato qualificato. Quando il Soggetto è una persona giuridica, tali responsabilità ricadono sul legale rappresentante o soggetto munito di apposita procura, che richiede il certificato qualificato;
- il Richiedente, ove presente, ha la responsabilità di informare il Soggetto, per conto del quale sta richiedendo il certificato, sugli obblighi derivanti dal certificato, di fornire le informazioni corrette e veritiere sull'identità del Soggetto, di seguire i processi e le indicazioni della CA e/o della RA;
- la Registration Authority, dove presente e anche attraverso l'Incaricato alla Registrazione, ha la responsabilità di identificare con certezza il Soggetto e il Richiedente, informare i vari soggetti sugli obblighi derivanti dal certificato e seguire dettagliatamente i processi definiti della CA;
- la Certification Authority è il responsabile ultimo della identificazione del Soggetto e del buon esito del processo di iscrizione del certificato qualificato.

5.2 Elaborazione della richiesta

Ai fini del processo di iscrizione ed emissione, il Soggetto e/o il Richiedente deve:

- prendere visione del presente Manuale Operativo, della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dal QTSP descritte nel paragrafo 4.2.3;

- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione e certificazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio, sulla apposita modulistica analogica o elettronica predisposta dalla CA.

5.2.1 Informazioni sul Soggetto

Per la richiesta di un certificato qualificato di sottoscrizione il Soggetto o il Richiedente che richiede il certificato della persona fisica deve fornire obbligatoriamente le seguenti informazioni:

- cognome e nome;
- data e luogo di nascita;
- codice fiscale o analogo codice identificativo (TIN);
- indirizzo di residenza;
- estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso;
- e-mail per l'invio delle comunicazioni dalla CA al Soggetto.

Opzionalmente il Soggetto (o il Richiedente) può fornire un altro nome, con il quale è comunemente conosciuto, che sarà inserito in un apposito campo denominato Common Name (nome comune) del DN del certificato.

5.2.2 Approvazione o rifiuto della richiesta del certificato

Dopo la registrazione iniziale, Cedacri può rifiutarsi di portare a termine l'emissione del certificato di sottoscrizione in caso di assenza o incompletezza di informazioni, verifiche di coerenza e consistenza delle informazioni fornite, verifiche antifrode, dubbi sull'identità del Soggetto o del Richiedente, ecc.

5.2.3 Avvio della procedura di emissione

Terminata la fase di registrazione, l'operatore RAO avvia la procedura di generazione della coppia di chiavi e di emissione del certificato.

La procedura consiste nel consentire al Soggetto di personalizzare il codice segrete PIN del dispositivo, effettuare l'operatività necessaria alla creazione della coppia di chiavi, scaricare il relativo Certificato sul dispositivo di firma.

Cedacri prevede che il PIN di firma sia scelto in autonomia dal Soggetto ed è onere dello stesso (o del Richiedente) ricordare il PIN.

5.3 Emissione del certificato

5.3.1 Azioni della CA/RA durante l'emissione del certificato

Emissione del certificato su dispositivo di firma (smartcard o token)

La coppia di chiavi crittografiche viene generata dalla RA direttamente sui dispositivi sicuri di firma utilizzando le applicazioni messe a disposizione dalla CA, previa autenticazione sicura.

La RA invia alla CA la richiesta di certificazione della chiave pubblica in formato PKCS#10 firmata digitalmente con il certificato qualificato di sottoscrizione specificatamente autorizzato a tal fine.

La CA, verificata la validità della firma sul PKCS#10 e la titolarità del soggetto a inoltrare la richiesta, procede alla generazione del certificato qualificato, che è inviato su canale sicuro all'interno del dispositivo.

Emissione del certificato su dispositivo di firma remota (HSM) per sottoscrizione con procedura automatica

Il Soggetto o il Richiedente si autenticano ai servizi o alle applicazioni messe a disposizione dalla CA o RA.

La coppia di chiavi crittografiche viene generata dalla RA direttamente sull'HSM; la RA invia quindi alla CA la richiesta di certificazione della chiave pubblica in formato PKCS#10, che è firmata digitalmente con il certificato qualificato di sottoscrizione per procedura automatica specificatamente autorizzato a tal fine.

La CA, verificata la validità della firma sul PKCS#10 e la titolarità del soggetto a inoltrare la richiesta, procede alla generazione del certificato qualificato, che viene memorizzato sull'HSM stesso.

5.3.2 Attivazione

In entrambi i casi citati nel paragrafo 5.3.1. la fase di attivazione del Certificato avviene durante la fase di registrazione ad opera del RAO.

5.4 Accettazione del certificato

5.4.1 Comportamenti concludenti di accettazione del certificato

n/a

5.4.2 Pubblicazione del certificato da parte della Certification Authority

Il certificato è reso pubblico immediatamente dopo aver terminato la fase di registrazione ed emissione delle chiavi da parte del QTSP su dispositivo di firma.

5.4.3 Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato

n/a

5.5 Utilizzo delle chiavi e del certificato

5.5.1 Utilizzo della chiave privata e del certificato da parte del Soggetto

Il Soggetto deve custodire in maniera sicura il dispositivo di firma; in particolare nel caso del token:

- deve conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo;
- deve garantire la protezione della segretezza e la conservazione del codice di emergenza necessario alla sospensione del certificato, deve utilizzare il certificato per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi;
- non deve apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato o sospeso il certificato e non deve apporre firme elettroniche avvalendosi di certificato emesso da CA revocata.

5.5.2 Utilizzo della chiave pubblica e del certificato da parte degli Utenti Finali

L'Utente Finale deve conoscere l'ambito di utilizzo del certificato riportati nel Manuale Operativo e nel certificato stesso. Deve verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta e che il certificato non risulti sospeso o revocato controllando le relative liste nel registro dei certificati, deve inoltre verificare l'esistenza ed il contenuto di eventuali limitazioni d'uso della coppia di chiavi, poteri di rappresentanza ed abilitazioni professionali.

A tale proposito Cedacri mette a disposizione dei suoi clienti un tool di firma e verifica che consente di apporre e verificare firme digitali in formato standard nonché di richiedere e verificare marche temporali.

Le releases dei sistemi operativi compatibili con il servizio Cedacricert, nonché il documento in cui sono presenti le istruzioni per la generazione e la verifica della firma digitale, sono reperibili sul sito ufficiale Cedacricert.

5.5.3 Limiti d'uso e di valore

I certificati qualificati di sottoscrizione per procedura automatica contengono il limite d'uso previsto dall'Autorità di Vigilanza, come ulteriori Certificate Policy, identificati dai seguenti OID:

1.3.76.27.1.1.1.3	Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.
1.3.76.27.1.1.1.1	I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.
1.3.76.27.1.1.1.2	L'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto). The certificate may be used only for relations with the (declare the subject).

Tabella 2 – OID limite d'uso

È inoltre facoltà del Soggetto o del Richiedente richiedere al QTSP l'inserimento nel certificato di limiti d'uso personalizzati. La richiesta di inserire altre specifiche limitazioni d'uso sarà valutata dal QTSP sotto il profilo legale, tecnico e di interoperabilità e valorizzata di conseguenza.

È inoltre facoltà del Soggetto richiedere al QTSP l'inserimento nel certificato di limiti di valore specifico per gli atti unilaterali e dei contratti per i quali il certificato stesso può essere usato. I valori devono essere espressi come numeri interi positivi, senza indicazione di cifre decimali.

La QTSP non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Ferma restando la responsabilità del QTSP di cui al CAD (art.30 comma 3), è responsabilità del Soggetto verificare il rispetto dei limiti d'uso e di valore inseriti nel certificato.

Per la CA CEDACRICERT EU 2019, invece, il limite d'uso previsto dall'Autorità di Vigilanza, come ulteriori Certificate Policy, è identificato dai seguenti OID:

1.3.76.27.1.1.2.3	Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.
1.3.76.27.1.1.2.1	I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.

Tabella 3 – OID limite d'uso CEDACRICERT 2019

5.6 Rinnovo del certificato

5.6.1 Motivi per il rinnovo

Il rinnovo consente di ottenere un nuovo certificato di sottoscrizione da utilizzare per firmare documenti e transazioni.

5.6.2 Chi può richiedere il rinnovo

Il Soggetto può richiedere il rinnovo del certificato almeno 30 giorni prima della sua scadenza solo se non è stato revocato e se tutte le informazioni fornite all'atto della emissione precedente sono ancora valide; oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere alla richiesta di un nuovo certificato. La procedura di rinnovo si applica esclusivamente a certificati emessi da Cedacri.

Tale richiesta dovrà essere firmata con le chiavi in corso di validità, in modo che il QTSP sia in grado di verificare l'identità del Richiedente.

Il rinnovo di un certificato per firma automatica non è previsto e si dovrà procedere ad una nuova emissione.

Il rinnovo di un certificato emesso a una persona giuridica non è previsto, si dovrà procedere ad una nuova emissione.

5.6.3 Elaborazione della richiesta di rinnovo

Il rinnovo comporta comunque la riemissione del certificato da parte della CA, ma a delle condizioni agevolate per il cliente finale.

Una volta ricevuto il nuovo certificato, la Chiave privata relativa al vecchio Certificato non dovrà più essere utilizzata.

Il vecchio Certificato sarà conservato, a partire dalla data di scadenza, negli archivi del QTSP per 20 anni.

5.7 Riemissione del certificato

La riemissione del Certificato si verifica quando – a seguito di una revoca- il Soggetto o il Richiedente esprimono la richiesta di emissione.

5.8 Modifica del certificato

In caso di variazioni dei dati presenti all'interno del certificato, il certificato dev'essere revocato e riemesso con i dati corretti.

5.9 Revoca e sospensione del certificato

La sospensione può avvenire su richiesta del Soggetto oppure su iniziativa del QTSP o su richiesta di un Terzo interessato.

La revoca o la sospensione di un certificato ne tolgono la validità prima della scadenza stabilita e invalidano le firme apposte successivamente al momento della pubblicazione della revoca. I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione ("CRL") firmata dalla CA che li ha emessi e pubblicata nel registro dei certificati con periodicità stabilita dalla CA (1 ora). Inoltre, la CA può emettere una CRL non programmata in determinate circostanze. L'efficacia della revoca e della sospensione si verifica dal momento di pubblicazione della lista, prendendo come riferimento la data attestata nel Giornale di Controllo della CA.

5.9.1 Motivi per la revoca

Le condizioni per cui deve essere effettuata la richiesta di revoca sono le seguenti:

1) La chiave privata sia stata compromessa, oppure:
   a) sia stato smarrito il dispositivo sicuro di firma che contiene la chiave;
   b) sia venuta meno la segretezza della chiave o del suo codice d'attivazione (PIN);
   c) si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;
2) il Soggetto non riesce più ad utilizzare il dispositivo sicuro di firma in suo possesso, ad esempio per guasto o deterioramento;
3) si verifica un cambiamento dei dati del Soggetto presenti nel certificato, compresi quelli relativi al ruolo, in modo da rendere tali dati non più corretti;
4) termina il rapporto tra il Soggetto e la CA, ovvero tra il Richiedente e la CA;
5) vengono meno le condizioni riportate nel Manuale Operativo.

5.9.2 Chi può richiedere la revoca

La revoca può essere richiesta dal Soggetto in qualsiasi momento e per un qualunque motivo. Inoltre, la revoca del certificato può essere richiesta anche dal Richiedente, per i motivi e nelle modalità previsti dal presente Manuale Operativo. Infine, il certificato può essere revocato d'ufficio dalla CA.

5.9.3 Procedure per richiedere la revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del soggetto che la pone in essere.

Revoca richiesta dal Soggetto

Il Soggetto è tenuto a sottoscrivere la richiesta di revoca, utilizzando il modulo presente nel sito www.cedacricert.it consegnarla personalmente alla RA o inviarla direttamente per posta

raccomandata, PEC, o sistema di trouble ticketing, corredata di una fotocopia di un documento di identità in corso di validità.

Il QTSP verifica l'autenticità della richiesta, procede alla revoca del certificato, dandone immediata notizia al Soggetto o al Richiedente.

Il QTSP, qualora nel certificato oggetto della richiesta di revoca siano presenti informazioni relative al Ruolo del Soggetto, provvederà a comunicare l'avvenuta revoca all'eventuale Terzo Interessato con cui siano attive specifiche condizioni contrattuali.

Se invece nel certificato per il quale è stata richiesta la revoca è presente l'indicazione dell'Organizzazione, il QTSP provvederà a comunicare l'avvenuta revoca a tale Soggetto.

Revoca richiesta dal Richiedente o dal Terzo Interessato

Il Richiedente può richiedere la revoca del certificato del Soggetto compilando l'apposito modulo messo a disposizione sul sito www.cedacricert.it, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del Soggetto del certificato comunicati al QTSP al momento dell'emissione del certificato.

Il QTSP verificherà l'autenticità della richiesta, lo comunicherà al Soggetto attraverso i canali di comunicazione stabiliti all'atto della richiesta del certificato e procederà alla revoca del certificato.

Revoca su iniziativa della Certification Authority

Il QTSP, qualora ne riscontri la necessità ha facoltà di revocare il certificato, comunicandolo preventivamente al Soggetto, fornendo il motivo della revoca, nonché la data di decorrenza. I motivi per i quali il QTSP può autonomamente revocare un certificato non scaduto possono essere legati, a titolo esemplificativo e non esaustivo, al fatto che il certificato non è più conforme a CP per il quale è stato emesso o in generale quando il QTSP viene a conoscenza di cambiamenti che incidono sulla validità/sicurezza del certificato stesso.

Se nel certificato oggetto della revoca il QTSP rilevi la presenza di informazioni relative al Ruolo del Soggetto, provvederà a comunicare l'avvenuta revoca all'eventuale Terzo Interessato con cui siano state stipulate specifiche condizioni contrattuali.

Se nel certificato oggetto della richiesta di revoca è anche presente l'indicazione dell'Organizzazione, il QTSP provvederà a comunicare l'avvenuta revoca a tale Soggetto.

5.9.4 Grace period della richiesta di revoca

Il grace period della CRL è il periodo di tempo che intercorre tra il momento della pubblicazione della successiva CRL e il momento in cui scade la CRL corrente. Per non causare disservizi alle parti coinvolte, questo periodo è più lungo del tempo necessario alla CA per generare e pubblicare una nuova CRL. In questo modo la CRL corrente rimane valida almeno fino a quando non viene sostituita dalla nuova CRL. Tale grace period non supera comunque le 24 ore.

5.9.5 Tempo massimo di elaborazione della richiesta di revoca

La richiesta viene evasa entro 12 ore dalla presa in carico da parte dell'operatore a meno che non siano necessari ulteriori controlli sull'autenticità della stessa.

5.9.6 Frequenza di pubblicazione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dal QTSP che viene pubblicata nel Registro pubblico. La CRL viene pubblicata in modo programmato con cadenza 1 ora (emissione ordinaria), ma la CA può, in circostanze particolari, forzare un'emissione non programmata della CRL (emissione straordinaria immediata), nel caso in cui, ad esempio, la revoca o la sospensione di un certificato avvenga per la sospetta compromissione della segretezza della chiave privata (revoca o sospensione immediata).

Il momento della pubblicazione della CRL viene attestata utilizzando quale riferimento temporale la data fornita dal sistema di Time Stamping Authority Cedacri e tale registrazione viene riportata sul giornale di controllo. Ogni elemento della lista CRL contiene la data e l'ora di revoca o sospensione.

L'acquisizione e consultazione della CRL è a cura degli utenti che possono scaricarla andando sul sito Cedacricert. La CRL da consultare per lo specifico certificato è indicata nel certificato stesso secondo le norme vigenti.

5.9.7 Latenza massima della CRL

Il tempo di attesa tra la richiesta di revoca o di sospensione e la pubblicazione della CRL è di massimo 2 ore.

5.9.8 Servizio online di verifica dello stato di revoca del certificato

Cedacri mette a disposizione anche un servizio OCSP per la verifica dello stato del certificato. L'URL del servizio è indicato nel certificato. Il servizio è disponibile 24/7.

5.9.9 Motivi per la sospensione

La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

1) è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2) il Soggetto, Il Richiedente o Terzo Interessato, la RA o la CA hanno acquisito elementi di dubbio sulla validità del certificato;
3) sia stato rilevato un problema di sicurezza;
4) è necessaria un'interruzione temporanea della validità del certificato.

Nei casi citati si richiederà la sospensione del certificato specificando un periodo di tempo finito il quale la sospensione potrà essere seguita o da una revoca definitiva oppure dalla riattivazione del certificato.

5.9.10 Chi può richiedere la sospensione

La sospensione può essere richiesta dal Soggetto in qualsiasi momento e per un qualunque motivo. Inoltre, la sospensione del certificato può essere richiesta anche dal Richiedente o dal Terzo Interessato, per i motivi e nelle modalità previsti dal presente Manuale Operativo oppure in certificato può essere sospeso d'ufficio da Cedacri.

5.9.11 Procedure per richiedere la sospensione

La richiesta di sospensione viene effettuata con modalità diverse a seconda del soggetto che la pone in essere. La sospensione termina alla mezzanotte dell'ultimo giorno del periodo richiesto.

Sospensione richiesta dal Soggetto

Il Soggetto deve richiedere la sospensione con una delle seguenti modalità:

1) telefonando al Call Center e fornendo le informazioni richieste per identificare i dati del certificato;
2) il Soggetto è tenuto a sottoscrivere la richiesta di sospensione e consegnarla alla RA – Cedacri o inviarla direttamente alla CA per posta ordinaria o PEC, corredata di una fotocopia di un documento di identità in corso di validità e codice fiscale.

La CA, se nel certificato oggetto della sospensione rileva la presenza di informazioni relative al Ruolo del Soggetto, provvederà a comunicare l'avvenuta sospensione all' eventuale Terzo Interessato con cui siano state stipulate specifiche condizioni contrattuali. Se nel certificato oggetto della richiesta di sospensione è anche presente l'indicazione dell'Organizzazione, la CA provvederà a comunicare l'avvenuta sospensione a tale Soggetto.

La CA verificherà l'autenticità della richiesta, lo comunicherà al Soggetto attraverso i canali di comunicazione stabiliti all'atto della richiesta del certificato e procederà alla sospensione del certificato.

Sospensione richiesta dal Richiedente o dal Terzo Interessato

Il Richiedente o il Terzo Interessato possono richiedere la sospensione del certificato del Soggetto compilando l'apposito modulo messo a disposizione sul sito della CA e presso le RA, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando i dati del Soggetto comunicati alla CA al momento dell'emissione del certificato.

La CA verificherà l'autenticità della richiesta, lo comunicherà al Soggetto attraverso i canali di comunicazione stabiliti all'atto della richiesta del certificato e procederà alla revoca del certificato.

Sospensione su iniziativa della CA

Il QTSP salvo casi d'urgenza comunica preventivamente al Soggetto l'intenzione di sospendere il certificato, fornendo il motivo della sospensione, la data di decorrenza e la data di termine. Queste ultime informazioni saranno in ogni caso comunicate al più presto al Soggetto.

Il QTSP se nel certificato oggetto della sospensione rileva la presenza di informazioni relative al Ruolo del Soggetto, provvederà a comunicare l'avvenuta sospensione all' eventuale Terzo Interessato con cui siano state stipulate specifiche condizioni contrattuali.

Se nel certificato oggetto della richiesta di sospensione è anche presente l'indicazione dell'Organizzazione, la CA provvederà a comunicare l'avvenuta sospensione a tale Soggetto.

5.9.12 Limiti al periodo di sospensione

Alla scadenza del periodo di sospensione richiesto, la validità del certificato viene ripristinata tramite la rimozione del certificato dalla lista di revoca e sospensione (CRL). La riattivazione avviene nell'arco delle 24 ore successive alla data di termine della sospensione. Qualora il giorno di scadenza della sospensione coincida con il giorno di scadenza del certificato o sia a questa successivo, la sospensione viene invece tramutata in revoca, con effetto dall'inizio della sospensione.

È possibile richiedere la riattivazione del certificato prima della data del termine di sospensione inviando il modulo che si trova sul sito Cedacricert, firmato e accompagnato da un documento di identità in corso di validità.

5.10 Servizi riguardanti lo stato del certificato

5.10.1 Caratteristiche operative

Le informazioni sullo stato dei certificati sono disponibili tramite CRL e risponditore OCSP.

Il numero di serie di un certificato revocato rimane in CRL anche dopo la fine della validità del certificato.

Le informazioni dall'OCSP per i certificati sono aggiornate in tempo reale.

5.10.2 Disponibilità del servizio

Il servizio OCSP è disponibile 24/7.

5.11 Disdetta dai servizi della CA

Il rapporto del Soggetto e/o del Richiedente con la Certification Authority finisce quando il certificato scade o viene revocato, salvo casi particolari definiti secondo specifici accordi contrattuali tra le parti.

5.12 Deposito presso terzi e recovery della chiave

Cedacri non prevede nell'erogazione di questo servizio il deposito presso terzi della chiave.

6 Misure di sicurezza e controlli

Tutte le misure di salvaguardia di Cedacri sono inquadrate nel contesto generale del Manuale della Sicurezza di Cedacri stessa, che fornisce le prescrizioni fondamentali per la gestione dei sistemi ed il trattamento dei dati in ambiente sicuro, applicabili anche al servizio di Firma Elettronica Qualificata decritto dal presente Manuale Operativo.

Tale documento ì è disponibile facendone richiesta a auditing-cedacri@iongroup.com.

6.1 Sicurezza fisica

Sono messe in atto tutte le misure di natura tecnica e logistica di prevenzione degli incidenti fisici e di protezione delle risorse fisiche coinvolte nell'erogazione del Servizio, riguardanti i seguenti principali aspetti:

- sicurezza del perimetro;
- controllo degli accessi fisici;
- sicurezza degli uffici locali e strutture;
- protezione da minacce esterne e ambientali;
- alimentazione elettrica e condizionamento dell'aria;
- cablaggi e apparati di rete;
- protezione contro gli incendi;
- protezione contro gli allagamenti;
- modalità di archiviazione dei supporti magnetici;
- siti di archiviazione dei supporti magnetici.

6.1.1 Posizione e costruzione della struttura

Il data center Cedacri si trova a Collecchio (Parma) mentre il sito secondario è ubicato presso la sede di Castellazzo Bormida (Alessandria) ed è connesso al data center; i due siti sono interconnessi tra loro mediante connessioni dedicate a 10Gbps realizzate con diverso operatore.

6.1.2 Accesso fisico

L'accesso delle persone agli edifici dove Cedacri svolge la propria attività è soggetto a regole che definiscono controlli, modalità e responsabilità di gestione.

Il perimetro esterno degli edifici Cedacri è protetto da un sistema passivo di antintrusione mentre il perimetro degli edifici è protetto da un sistema attivo di antintrusione.

Il sistema di accesso del personale esterno prevede l'identificazione, la registrazione e il rilascio di un badge presso la Reception, presidiata h24 7X7.

Un impianto TV a circuito chiuso con monitor in reception consente la visione, anche notturna delle aree aperte del comprensorio.

Le porte che non sono adibite all'entrata negli edifici (ed in particolare quelle adibite ad uscite di sicurezza), sono dotate di sistema di allarme.

Le vie di accesso esterne sono protette da porte e tornelli con apertura mediante badge.

All'interno degli edifici sono attive zone di sicurezza soggette a particolari restrizioni di accesso con apertura porte tramite badge e pin (es. control room, sale macchine, gabbia CA, sala robot) all'interno dei quali sono presenti tutti i sistemi che concorrono all'erogazione del Servizio di Firma Digitale

Regole particolari, nel rispetto dei principi generali di protezione fisica, sono previste per le attività di consegna e ritiro di merci e materiali.

6.1.3 Impianto elettrico e di climatizzazione

I locali tecnici sono provvisti di un sistema di alimentazione elettrica progettato al fine di prevenire guasti e soprattutto disservizi. L'alimentazione dei sistemi include le più moderne tecnologie al fine di incrementare l'affidabilità e assicurare la ridondanza delle funzionalità più critiche ai fini dei servizi erogati.

L'alimentazione elettrica delle sale macchine è realizzata con doppia alimentazione tramite 2 sistemi di generazione distinti (Enel, gruppi elettrogeni di soccorso, inverter, batterie tampone, ecc.) che, in caso di guasto di una stazione, la restante è in grado di supportare completamente tutto il carico delle sale macchine.

Le principali caratteristiche impiantistiche e di dotazioni degli spazi sono:

- alimentazione ridondante derivata da:
  a. cabine indipendenti con disponibilità di supportare il carico completo della sala macchine;
  b. gruppi di continuità ridondati sulla singola cabina (in caso di guasto di un UPS i restanti gruppi supportano il carico completo);
  c. apparati alimentati in doppia alimentazione privilegiata completamente indipendente;
  d. apparati alimentati da una singola alimentazione privilegiata;
- alimentazioni con switch;
- gruppi di continuità monitorati H24 con sistema LIFE da centro specializzato;
- condizionamento realizzato con apparecchiature ad espansione diretta ridondante sia sull'alimentazione elettrica che sulla potenza termica della singola macchina;
- illuminazione primaria e di emergenza.

Ogni armadio tecnologico installato presso il data center fruisce di due linee elettriche che assicurano l'HA in caso di interruzione di una delle due linee disponibili.

L'armadio tecnologico è monitorato remotamente; vengono effettuati controlli costanti sullo stato della linea elettrica (on/off) e le potenze elettriche assorbite (ogni linea non deve superare il 50% del carico).

L'area tecnica è normalmente mantenuta fra 20° e 27° con un tasso di umidità relativo compreso fra il 30% ed il 60%. Gli impianti sono dotati di batterie condensanti con sistema di raccolta e scarico condensa sigillato e controllato da sonde antiallagamento. L'intero sistema di condizionamento è asservito ai generatori di emergenza in caso di assenza di energia elettrica. Si garantisce la capacità frigorifera per armadio con un carico massimo previsto di 10KW e massimo di 15 KW su due armadi affiancati.

6.1.4 Prevenzione e protezione contro gli allagamenti

Per quanto riguarda possibili allagamenti, sono presenti due pompe idrovore sommerse con alimentazione elettrica e collegamento ai gruppi di continuità e una pompa idrovora con alimentazione autonoma (diesel).

Il personale operativo è addestrato all'impiego dei mezzi di intervento contro gli incidenti, sulla base delle disposizioni DLGS 81/2008.

6.1.5 Supporti di memorizzazione

Per quanto concerne la piattaforma storage, la soluzione in essere prevede per la parte NAS l'utilizzo di sistemi NetApp. Per la parte SAN si è invece implementata un'infrastruttura basata su tecnologie HDS che comprendono VSP e G1000 senza nessun layer di virtualizzazione degli apparati storage.

6.1.6 Disposizioni sulla dismissione di apparati

Cedacri adotta una politica di raccolta differenziata e smaltimento sostenibile dei rifiuti. Per quel che riguarda il contenuto informativo dei rifiuti elettronici, Cedacri si avvale di società specializzate nello smaltimento dei rifiuti speciali, e garantisce che tutti i media vengono ripuliti secondo le procedure previste di sicurezza dei dati e delle informazioni, rendendoli completamente inutilizzabili e che tali supporti vengano smaltiti in maniera sostenibile.

6.2 Controlli procedurali

6.2.1 Ruoli chiave

Cedacri definisce, e mantiene aggiornate, procedure che rappresentano le modalità di gestione dei processi aziendali prevedendo ruoli e responsabilità e definendo adeguati controlli per la riduzione dei rischi di uso improprio accidentale o deliberato del sistema informativo e delle informazioni.

Cedacri, in osservanza al DPCM del 22 febbraio 2013, prevede almeno le seguenti fi gure professionali:

a) responsabile della sicurezza;

b) responsabile del servizio di certificazione e validazione temporale;

c) responsabile della conduzione tecnica dei sistemi;

d) responsabile dei servizi tecnici e logistici;

e) responsabile delle verifiche e delle ispezioni (auditing).

Cedacri ha assegnato i suddetti ruoli a personale interno che ha maturato un'esperienza professionale e una competenza tecnica elevata ed inoltre, in conformità al DPCM del 22 febbraio 2013 Art.38, garantisce che i ruoli a) ed e) sono assegnati a soggetti differenti.

6.3 Controllo del personale

Cedacri considera le risorse umane componente fondamentale e imprescindibile del proprio business.

A tutti i livelli dell'organizzazione, è inserito in un processo di valutazione e sviluppo delle competenze; informazione, addestramento e sensibilizzazione relativamente alla sicurezza delle informazioni.

Sono inoltre definiti i termini delle responsabilità in materia di sicurezza e/o legale, che si protraggono per il periodo successivo al termine del contratto di lavoro (ad esempio vincoli di riservatezza e proprietà intellettuale).

6.3.1 Qualifiche, esperienze e autorizzazioni richieste

Effettuata la pianificazione annuale delle risorse umane, il responsabile funzione/struttura organizzativa identifica le caratteristiche e le skills della risorsa da inserire. Successivamente, di concerto con il responsabile selezione, viene attivato il processo di ricerca e selezione.

6.3.2 Procedure di controllo delle esperienze pregresse

I candidati vengono valutati in modo preliminare mediante colloqui effettuati dalla Direzione Human Resources & Organization e dal responsabile richiedente, acquisendo la documentazione che attesti il curriculum vitae ed eventuali referenze che permettono all'azienda di effettuare una serie di controlli evidenziati nel paragrafo 6.3.8.

Infatti, vengono effettuate tutte le verifiche necessarie in accordo con la legislazione, regolamenti e principi etici, atte a garantire i requisiti di sicurezza previsti dalle politiche aziendali, proporzionalmente all'importanza del ruolo che devono ricoprire e alle tipologie di informazioni a cui hanno accesso.

Viene inoltre richiesto ai candidati di effettuare un "test attitudinale" i cui risultati vengono elaborati e valutati. Le registrazioni relative ai colloqui effettuati, le risultanze dei test e le valutazioni effettuate dalla Direzione Risorse Umane e dal responsabile richiedente sono raccolte in appositi documenti di registrazione del profilo professionale del candidato.

6.3.3 Requisiti di formazione

Tutto il personale che deve operare dispone di una documentazione adeguata ed ha seguito appositi corsi di formazione o dispone di una pluriennale esperienza.

La formazione del personale al fine della sicurezza è stata impostata da Cedacri a seguito dei dettami del Manuale della Sicurezza. I principali riferimenti normativi in questo ambito sono le Leggi 81 (Sicurezza fisica), 196 (Privacy) e il Regolamento UE 2016/679. La formazione viene inoltre ricalibrata sulle necessità del Servizio di Posta Elettronica Certificata e del Servizio di Firma Digitale per il personale direttamente coinvolto da questi.

Il piano di formazione è stato finalizzato a rendere edotto il personale dei rischi individuati e dei modi per prevenire i danni. A tal fine il piano è stato suddiviso sulla base delle specifiche esigenze di ciascuna area aziendale in relazione alla natura dei dati trattati e dei rischi generici o specifici incombenti sui dati e sui criteri e modalità di evitare tali rischi.

Per le risorse umane che svolgono trattamenti di dati, ed in particolare per quelle operanti nell'ambito del Servizio di Firma Digitale, è stata pianificata e via via svolta un'attività formativa i cui contenuti essenziali sono:

- informazioni sulla legge 196/03 e decreti successivi e connessi;
- informazioni sulla legge 81/2008 e decreti successivi e connessi;
- principi legislativi e comunitari;
- informazioni sulla 231/01;
- comportamenti aziendali;
- rischi possibili cui sono sottoposti i dati;
- misure di sicurezza tecniche, organizzative e comportamentali deputate alla prevenzione dei rischi;
- comportamenti e modalità di lavoro per prevenire i rischi.

Tale formazione viene erogata mediante supporti informativi cartacei, elettronici e/o telematici.

I contenuti sono quelli previsti nella formazione di base, con l'aggiunta di contenuti particolarmente specializzati sulle attività specifiche di ciascuna area aziendale e coordinati per gruppi di incaricati che svolgono attività omogenee. La didattica è mista e comprende momenti di aula tradizionale e partecipazioni a formazione specialistica interaziendale.

6.3.4 Frequenza di aggiornamento della formazione

Con cadenza almeno annuale, è redatto il Piano di Formazione nel quale sono riassunti gli interventi che devono essere attuati per rendere disponibili le competenze necessarie per gestire i processi aziendali ed erogare i servizi ai clienti.

Tale Piano è redatto dalla Direzione Human Resources & Organization in collaborazione con le aree aziendali ed è approvato dall'Executive Chairman. Al verificarsi di eventi nuovi o non previsti, tali da influire in modo significativo su organizzazione, conformità legislativa, e capacità di rispondere alle esigenze operative, il Piano di Formazione viene aggiornato a cura

della Direzione Human Resources & Organization per recepire ed attuare nuovi interventi di addestramento necessari.

6.3.5 Frequenza nella rotazione dei turni di lavoro

Per garantire che il servizio erogato sia conforme ai requisiti di qualità e ai livelli di servizio, Cedacri si è dotata di una struttura (Control Room) che lavora H24 7/7 su turni.

A seguito di questa necessità di assicurare la presenza di personale qualificato e competente l'articolazione dell'orario di lavoro del personale turnista di Contro Room garantisce la copertura delle 24 ore giornaliere dal lunedì alla domenica utilizzando le seguenti fasce orarie:

- mattina;
- pomeriggio;
- notte.

Le altre strutture Cedacri lavorano invece seguendo l'orario di lavoro spezzato senza turni.

6.3.6 Sanzioni per azioni non autorizzate

Al momento dell'assunzione i dipendenti Cedacri vengono informati circa le condizioni contrattuali di impiego e di particolare circa le regole aziendali in materia di sicurezza etica e privacy e sottoscrivono per accettazione il "Codice di Comportamento" aziendale.

Le clausole e gli impegni di riservatezza dei dipendenti sono anche specificati nel Contratto Nazionale di Lavoro di settore.

Cedacri ha adottato norme di sicurezza per la specifica attività dalla stessa svolta, necessita che tutto il personale si attenga scrupolosamente a quanto definito in materia; qualora si verificassero violazioni, Cedacri si riserva di applicare sanzioni disciplinari secondo le modalità e nel rispetto di quanto definito dai contratti nazionali e di integrativi di impiego in vigore.

Le violazioni delle regole di sicurezza delle informazioni e dei dati sono sanzionate con modalità di differente natura ed estensione a seconda della tipologia di illecito che determinano, in conformità alla legislazione in vigore.

6.3.7 Controlli sul personale non dipendente

Detto che Cedacri assegna i ruoli chiave per l'erogazione del Servizio di Firma Digitale Qualificata al personale interno, l'azienda intrattiene relazioni con fornitori costituiti da primarie aziende che operano nel settore delle forniture ICT quali hardware, software, apparati di TLC, trasmissione dati ed energia, impianti tecnologici, tecnologie e servizi per la sicurezza. Cedacri, inoltre, ha definito e applica precise procedure per l'acquisizione, la gestione, l'accettazione e la valutazione delle forniture esterne che hanno un impatto sulla qualità e sulla sicurezza sui servizi erogati.

In particolare, sono definiti accordi di riservatezza con fornitori, mediante la sottoscrizione dei contratti di fornitura, delle "Condizioni generali di fornitura" e NDA (Non Disclosure Agreement).

6.3.8 Documentazione che il personale deve fornire

Le verifiche della risorsa entrante devono essere effettuate tutte con esito positivo; diversamente qualora non sia possibile effettuare il controllo o l'esito del controllo sia negativo, verrà coinvolta la Direzione del Personale per la decisione finale (accettazione in deroga oppure rifiuto).

Sono definite e applicate policies aziendali che garantiscono appropriate check list in funzione della risorsa entrante. I controlli minimi prevedono la seguente documentazione fornita dal candidato:

- documento di identità con foto e nome del richiedente, il certificato di nascita, il certificato di cittadinanza, il certificato di stato di famiglia, il codice fiscale;
- certificato di residenza;
- certificato di godimento dei diritti politici;
- copia del titolo di studio;
- curriculum vitae firmato.

Nel caso in cui la risorsa abbia svolto precedenti attività lavorative

- busta paga fornita e/o TFR compilato dal precedente datore di lavoro. Nel caso in cui la documentazione fornita non copra i 3 anni antecedenti la selezione, l'ufficio personale consulterà le visure camerali;
- se disponibile vengono fornite le cartelle delle visite mediche svolte presso i precedenti datori di lavoro (consegnate dal dipendente in busta chiusa e consegna al medico del lavoro).

6.4 Audit logging

In conformità a ETSI EN 319 411-2 e alla normativa vigente, sono registrati I principali eventi relativi alla gestione del ciclo di vita dei certificati e anche relativi agli accessi logici ai sistemi, le operazioni svolte dal personale, l'entrata e l'uscita di visitatori nei locali in cui si svolge l'attività di certificazione.

Di ogni evento viene registrata la tipologia, la data e l'ora di occorrenza e, se disponibili, altre informazioni utili ad individuare gli attori coinvolti nell'evento e l'esito delle operazioni.

L'insieme delle registrazioni costituisce il "giornale di controllo" (audit log). I file che lo compongono vengono trasferiti periodicamente su supporto permanente.

L 'integrità del giornale di controllo viene garantita trasferendo e conservando lo stesso nel sistema aziendale di log management (Splunk). Lo stesso viene archiviato e conservato per un periodo non inferiore ai 20 anni.

La data/ora inserita come riferimento temporale in ogni registrazione appartenente al giornale di controllo, viene mantenuta allineata con l'ora esatta UTC (Tempo Universale Coordinato).

6.4.1 Frequenza di trattamento e di memorizzazione del giornale di controllo

Il trattamento e raggruppamento dei dati nonché memorizzazione sul sistema di conservazione avviene mensilmente.

6.4.2 Periodo di conservazione del giornale di controllo

Il giornale di controllo viene conservato per 20 anni.

6.4.3 Protezione del giornale di controllo

Il giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti. L'accesso logico è strettamente limitato agli addetti ai lavori, secondo le politiche del business to Know.

6.4.4 Procedure di backup del giornale di controllo

Sono predisposte opportune copie del giornale di controllo secondo le policies aziendali in essere.

6.4.5 Sistema di memorizzazione del giornale di controllo

La raccolta dei log degli eventi avviene attraverso procedure automatiche ad hoc e viene periodicamente trasferito al sistema di log management aziendale che ne garantisce, tra gli altri aspetti, l'integrità.

6.4.6 Valutazioni di vulnerabilità

Cedacri implementa e mantiene un processo di vulnerability management che permette di:

- gestire le vulnerabilità rilevate dalle scansioni periodiche dei sistemi in modo efficace;
- assegnare la priorità dell'azione di remediation rapportando la gravità della vulnerabilità alla criticità di business del sistema sul quale è stata identificata la minaccia e la reale esposizione;
- monitorare lo stato di esposizione al rischio dei sistemi interni/esterni rispetto alle vulnerabilità attualmente note;
- migliorare la sicurezza dei sistemi;
- operare un controllo sull'implementazione del piano di remediation;
- garantire che le informazioni utili siano gestite e conservate in modo opportuno;
- produrre reportistica idonea a sostenere audit di terze parti.

6.4.7 Notifica in caso di incidenti di sicurezza

Si applica il processo aziendale di gestione degli incidenti di sicurezza (si veda paragrafo 6.7.1).

6.5 Archiviazione dei dati

In conformità alle normative ETSI EN 401 cap. 7.10, il QTSP conserva le seguenti informazioni relative ai processi di emissione e gestione dei certificati:

- le richieste di emissione;
- la documentazione fornita dai richiedenti;
- le CSR (Certificate Signing Request) fornite dai richiedenti;
- i dati anagrafici dei richiedenti e dei titolari (ove siano soggetti diversi);
- le richieste di sospensione o revoca;
- tutti i certificati emessi.

I dati sopra elencati sono conservati almeno per 20 anni oltre la data di scadenza dei certificati.

6.6 Sostituzione della chiave privata della CA

Almeno 90 giorni prima della scadenza del certificato relativo alla coppia di chiavi di certificazione il Certificatore avvia la procedura di sostituzione, generando una nuova coppia di chiavi, rispettando le modalità previste dal suddetto DPCM.

Ogni sostituzione comporterà una modifica al presente manuale e comunicazione ad Autorità di vigilanza (AgID).

6.7 Gestione Incidenti e Disaster Recovery

6.7.1 Procedure per la gestione degli incidenti

Cedacri pur avendo messo a disposizione tutte le misure di salvaguardia e sicurezza delle informazioni relativo al servizio di Firma Digitale (es back up, alta affidabilità server e dr su sito secondario) ha attivato procedure che descrivono le modalità di segnalazione degli eventi relativi alla sicurezza delle informazioni, la loro classificazione, l'avviamento del piano di risposta all'incidente e la raccolta delle evidenze.

Il processo prevede le seguenti macro-fasi:

- segnalazione degli eventi;
- presa in carico;
- classificazione della severity (da 1 a 5) in base alle linee Guida pubblicate a marzo 2017 (cfr. ENISA- "Article 19 Incident Reporting – Incident reporting framework for eIDAS Article

19" – December 2016 https://www.enisa.europa.eu/publications/article19-incident-reporting-framework);

- trattamento mediante eventuale processo di escalation;
- risoluzione;
- notifica presso l'Autorità di Vigilanza (AgiD) secondo i tempi e le modalità stabiliti dal livello di severity da ENISA.

6.7.2 Corruzione delle macchine, del software o dei dati

In caso di guasto del dispositivo sicuro di firma HSM contenente le chiavi di certificazione si fa ricorso alla copia di riserva della chiave di certificazione, opportunamente salvata e custodita nel sito secondario di Castellazzo, e non vi è necessità di revocare il corrispondente certificato della CA. In tutti i casi questi incidenti sono trattati nell'ambito degli incidenti critici di sicurezza (si veda paragrafo precedente).

I software e i dati sono soggetti a regolare backup come previsto dalle procedure interne.

6.7.3 Procedure in caso di compromissione della chiave privata della CA

Il Certificato può essere revocato su iniziativa del QTSP in caso di: sospetto o certezza di compromissione della Chiave privata della CA che effettuerà le seguenti attività:

- informa preventivamente il Soggetto in merito alla revoca comunicando data ed ora di efficacia della revoca;
- revoca il Certificato, pubblica la CRL;
- aggiornata ed informa contestualmente il Soggetto e l'Ente di registrazione.

In tutti i casi la comunicazione avviene via e-mail all'ultimo indirizzo comunicato dal Soggetto.

6.7.4 Erogazione dei servizi di CA in caso di disastri

Cedacri ha creato una struttura interna a cui è affidata la responsabilità di attuare tutte le misure preventive per soddisfare l'obiettivo del disaster recovery.

Il piano, che si applica al centro di elaborazione primario di Collecchio, prevede una ridondanza dei sistemi in campus sufficiente a soddisfare i requisiti di disponibilità dei sistemi previsti contrattualmente ed il ripristino dei servizi di elaborazione sul sito di disaster recovery presso una sede situata ad una distanza maggiore di 200 km dal centro di elaborazione primario.
Il piano di continuità operativa descrive a livello organizzativo e di processo le misure messe in atto da Cedacri per dichiarare un disastro, gestirlo e ritornare allo stato di normalità.

6.8 Cessazione del servizio della CA o della RA

Nel caso in cui Cedacri decida di cessare il proprio servizio di certificazione, dovrà :

- almeno 60 giorni prima della data esatta di cessazione del servizio, comunicare tale intenzione all' Organismo di Vigilanza (AgID) e all'Organismo di Verifica della Conformità (CAB);
- almeno 60 giorni prima della data esatta di cessazione del servizio, comunicare ad eventuali terze parti o RA delegate;
- sempre con un preavviso di almeno 60 giorni, comunicare il QTSP sostitutivo a tutti i clienti e pubblicare una nota informativa sul sito cedacricert con tutti i dettagli necessari;
- nel caso in cui non ci sia un QTSP sostitutivo, comunicare a tutti i clienti che i certificati emessi e non ancora scaduti alla data di cessazione, saranno automaticamente revocati;
- nel caso in cui non ci sia un QTSP sostitutivo, provvedere al deposito presso AgID entro 30 giorni di tutta la documentazione necessaria che ne garantisce la conservazione e la disponibilità;
- trasferire al QTSP sostitutivo tutta la conservazione delle evidenze (log, giornale di controllo, richiesta di emissione dei certificati ecc.) e trasferire a tale soggetto la responsabilità di pubblicare sul proprio sito la chiave pubblica della CA cessata;
- alla data di cessazione distruggere tutte le chiavi private di certificazione e il materiale crittografico necessario per il ripristino delle chiavi, stipulando apposito verbale che descriva tutti i passi di tale attività.

7 Controlli tecnici di sicurezza

7.1 Installazione e generazione della coppia di chiavi di certificazione

Nello svolgimento dell'attività il QTSP ha bisogno di generare la coppia di chiavi di certificazione per la firma dei certificati dei Soggetti.

Le chiavi sono generate solamente da personale esplicitamente incaricato di tale funzione. La generazione delle chiavi e della firma avviene all'interno di moduli crittografici dedicati e certificati come richiesto dalla normativa vigente in aree fisiche riservate dove l'accesso è riservato al solo personale strettamente abilitato con badge + PIN.

La generazione delle chiavi all'interno dei dispositivi di firma viene preceduta dall'inizializzazione dei dispositivi di firma utilizzati dal QTSP per il sistema di generazione dei certificati, con i quali vengono firmati i certificati dei Soggetti.

Una volta generata la coppia di chiavi, quelle private sono memorizzate su un dispositivo di firma di tipo crittografico HSM, il cui accesso è permesso mediante smartcard.

Secondo le regole del dual control, tali smart card vengono conservate in diverse buste anti-tampering, in casseforti differenti, che possono essere aperte da un numero limitato e autorizzato di persone.

Gli HSM dedicati al servizio sono localizzati uno a Collecchio e l'altro a Castellazzo.

Le chiavi private della CA vengono duplicate, al solo fine del loro ripristino in seguito a guasto del dispositivo sicuro di firma, secondo una procedura controllata che prevede la suddivisione della chiave e del contesto su più dispositivi come previsto dai criteri di sicurezza del dispositivo HSM.

Il modulo di crittografia utilizzato per la generazione delle chiavi e per la firma prevede requisiti tali da assicurare:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equi probabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione;
- che la generazione della firma avvenga all'interno del dispositivo in modo tale che non sia possibile l'intercettazione del valore della chiave privata utilizzata.

La procedura descritta ai punti precedenti sarà verbalizzata e conservata dal QTSP per 20 anni.

7.1.1 Generazione della coppia di chiavi del Soggetto

Le chiavi asimmetriche sono generate all'interno di un Dispositivo Sicuro per la Creazione della Firma SSCD ovvero QSCD utilizzando le funzionalità native offerte dai dispositivi stessi.

Nell'eventualità in cui il dispositivo non sia messo a disposizione del QTSP, il richiedente deve assicurare che il dispositivo rispetti la normativa vigente, presentando apposita documentazione ed essendo soggetto a audit periodici.

7.1.2 Consegna della chiave privata al Richiedente

La chiave privata è contenuta nel dispositivo crittografico QSCD.

Con la consegna del dispositivo crittografico al Soggetto o al Richiedente, quest'ultimo entra in pieno possesso della chiave privata, che può utilizzare unicamente attraverso l'uso del PIN.

7.1.3 Consegna della chiave pubblica alla CA

Il Soggetto crea una richiesta in formato PKCS#10 con la chiave pubblica generata.

7.1.4 Consegna della chiave pubblica agli utenti

La chiave pubblica è contenuta nel certificato rilasciato solo al Soggetto.

Conformemente, se il Soggetto o il Richiedente ne fa richiesta, viene pubblicata anche nel registro pubblico, da dove può essere recuperato dall'Utente.

7.1.5 Algoritmo e lunghezza delle chiavi

La coppia di chiavi asimmetriche di certificazione è generata all'interno del dispositivo crittografico hardware di cui sopra. Viene usato l'algoritmo asimmetrico RSA con chiavi di lunghezza non inferiore a 4096 bit.

Per le chiavi del Soggetto l'algoritmo di crittografia asimmetrica utilizzato è l'RSA e la lunghezza delle chiavi è non inferiore a 2048 bit.

7.1.6 Controlli di qualità e generazione della chiave pubblica

I dispositivi utilizzati sono certificati secondo alti standard di sicurezza (si veda il par. 7.2.1) e garantiscono che la chiave pubblica sia corretta e randomica. La CA, prima di emettere il certificato, verifica che la chiave pubblica non sia già stata utilizzata.

7.1.7 Scopo di utilizzo della chiave

Lo scopo di utilizzo della chiave privata è determinato dall'estensione KeyUsage come definita nello standard X509. Per i certificati descritti nel presente Manuale Operativo l'unico utilizzo permesso è il "*nonripudio*", ovvero possono essere utilizzati esclusivamente per firmare.

7.2 Protezione della chiave privata e controlli ingegneristici del modulo crittografico

7.2.1 Controlli e standard del modulo crittografico

I moduli crittografici utilizzati da Cedacri per le chiavi di certificazione (CA) e per il risponditore OCSP sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 + with AVA_VAN.5 .

Le smartcard utilizzate da Cedacri sono validate Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 an AVA_MSU.3) ovvero EAL5 Augmented by ALC_DVS.2, AVA_VAN.5 .

I moduli crittografici utilizzati da Cedacri per le chiavi di firma automatica del Soggetto sono validati FIPS 140 Level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4.

7.2.2 Controllo di più persone della chiave privata di CA

L'accesso ai dispositivi contenenti le chiavi di certificazione avviene tramite con due persone autenticate contemporaneamente.

7.2.3 Deposito presso terzi della chiave privata di CA

n/a

7.2.4 Backup della chiave privata di CA

Il backup delle chiavi è contenuto in quattro differenti casseforti ubicate in uffici diversi su siti diversi il cui accesso è consentito solo al personale che non ha accesso ai dispositivi HSM. Un eventuale ripristino richiede dunque la presenza sia del personale che ha accesso ai dispositivi sia di quello che ha accesso ad almeno due casseforti.

7.2.5 Archiviazione della chiave privata di CA

n/a

7.2.6 Trasferimento della chiave privata da un modulo o su un modulo crittografico

La chiave privata non è custodita in chiaro e il QTSP la può esportare esclusivamente per motivi di backup.

7.2.7 Memorizzazione della chiave privata su modulo crittografico

La chiave di certificazione viene generata e memorizzata in un'area protetta del dispositivo crittografico che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione blocca o rende illeggibile il dispositivo stesso cancellandone il contenuto.

7.2.8 Metodo di attivazione della chiave privata

La chiave privata di certificazione viene attivata tramite l'accesso in dual control sul dispositivo crittografico contenente il materiale crittografico.

7.2.9 Metodo di disattivazione della chiave privata

Per la disattivazione della chiave privata della CA valgono le regole di disattivazione dell' HSM.

Per il servizio di sottoscrizione automatica, l'HSM deve assicurare la disattivazione delle chiavi quando, a titolo esemplificativo, si verifica una mancata alimentazione elettrica oppure la connessione all'applicazione di firma si interrompe inaspettatamente. La chiave così disattivata può essere riutilizzata solo dopo una nuova autenticazione del sottoscrittore del dispositivo.

7.2.10 Metodo per distruggere la chiave privata della CA

Il personale Cedacri deputato a questo ruolo si occupa della distruzione della chiave privata quando il certificato è scaduto o revocato, secondo le procedure di sicurezza previste dalle politiche di sicurezza aziendali e quanto imposto dalle policy del fornitore degli apparati di sicurezza (HSM).

7.2.11 Classificazione dei moduli crittografici

n/a

7.3 Altri aspetti della gestione delle chiavi

n/a

7.3.1 Archiviazione della chiave pubblica

n/a

7.4 Periodo di validità del certificato e della coppia di chiavi

Il periodo di validità del certificato è determinato sulla base:

- dello stato della tecnologia;
- dello stato dell'arte delle conoscenze crittografiche;
- dell'utilizzo previsto per il certificato stesso.

L'intervallo di validità del certificato è espresso al suo interno nella modalità indicata nel presente Manuale.

Il certificato della CA ha una durata di 20 anni, mentre i certificati emessi a persona fisica hanno validità non superiore ai 3 anni.

Non sarà possibile emettere certificati qualificati che abbiano una durata superiore alla data di scadenza del certificato di CA.

7.4.1 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 5.2 e 7.3.

7.5 Controlli sulla sicurezza informatica

7.5.1 Requisiti di sicurezza specifici dei computer

I sistemi che concorrono al servizio di Firma Digitale Qualificata sono configurati in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione della CA.

L'accesso da parte degli Amministratori di sistema sono tracciati, loggati e conservati in conformità con quanto prescritto dalla normativa vigente.

7.6 Operatività sui sistemi di controllo

Cedacri sviluppa, mantiene e controlla un Sistema di Gestione della Qualità e Sicurezza delle Informazioni (SGQS), in conformità alla norma ISO/IEC 27001.

Nel SGQS sono previsti procedure e controlli per:

- gestione degli asset;
- controllo degli accessi;
- sicurezza fisica ed ambientale;
- sicurezza delle attività operative;
- sicurezza delle comunicazioni;
- acquisizione, sviluppo e manutenzione dei sistemi;

- gestione degli incidenti;
- continuità operativa.

Tali procedure seguono un iter di approvazione specifico e vengono condivise con tutto il personale attraverso la loro pubblicazione nel portale aziendale

7.7 Controlli di sicurezza della rete

Le reti sono adeguatamente gestite e controllate per proteggerle da minacce e mantenere la sicurezza dei sistemi e delle applicazioni che utilizzano la rete stessa, incluse le informazioni in transito.

I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione dei servizi di rete sono identificati e definiti contrattualmente con i fornitori per i servizi affidati all'esterno ed in procedure aziendali e/o contrattualmente con i clienti se forniti da Cedacri.

La rete di telecomunicazioni Cedacri è configurata in maniera tale da non presentare singoli punti di debolezza ed evitando componenti che, non disponendo di instradamenti alternativi, possono determinare la crisi dell'intera rete in caso di guasto.

Alla rete Cedacri possono collegarsi solo sistemi noti e riconosciuti; tutti i sistemi da cui provengono, o verso cui sono diretti, dati od operazioni, sono preventivamente identificati e registrati.

Ogni connessione fra reti, sub-network, elementi di rete, macchine o applicazioni di rete deve essere configurata in modo tale che nessuno dei componenti Cedacri sia esposto a degradazioni di sicurezza.

Tutti i sistemi con connessioni di rete dirette hanno un indirizzo unico (non duplicato) tramite il quale sono identificati.

Il numero di connessioni fra la rete di telecomunicazioni Cedacri e le reti esterne è limitata al minimo indispensabile.

I sistemi di sicurezza che si frappongono fra la rete Cedacri e le reti esterne sono protetti nei confronti di potenziali intrusori interni ed esterni ed installati in luoghi con accesso fisico limitato e controllato.

Tutti gli accessi alle connessioni fra rete Cedacri e reti pubbliche sono preventivamente ed esplicitamente autorizzati ed impiegano tecnologie e modalità operative definite da un'apposita struttura aziendale.

E' vietato l'uso di modem autonomi installati su stazioni di lavoro che siano simultaneamente connesse a LAN e ad altre reti di telecomunicazioni Cedacri per il collegamento diretto alla rete telefonica.

Gli accessi ad Internet sono controllati da "firewall" e, quando resi disponibili, sono in ogni caso consentiti unicamente per finalità professionali; è presente inoltre uno strumento che permette di definire, per categoria di utente, quali siti possono essere visitati.

7.8 Time stamping

In generale una marca temporale è una struttura di dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento temporale affidabile.

IL QTSP utilizza un sistema fidato, le cui chiavi sono certificate da una autorità di certificazione, ovvero Time Stamping Authority, per i propri servizi interni e per offrire un servizio di marcatura temporale ai propri utenti. Tutte le marche temporali emesse dal sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni. La marca temporale è valida per l'intero periodo di conservazione a cura del fornitore del servizio.

8 Formato del certificato, della CRL e dell'OCSP

8.1 Formato del certificato

Nel certificato compaiono le informazioni indicate nella richiesta di certificazione.

Il formato del certificato prodotto è conforme al Regolamento eiDAS e alla Deliberazione AgiD. In questo modo è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori europei.

Cedacri utilizza lo standard ITU X.509, versione 3 per l'intera struttura PKI.

In Appendice al presente Manuale Operativo è riportato il tracciato dei certificati di root e dei soggetti, per persone fisiche.

8.1.1 Numero di versione

Tutti i certificati emessi da Cedacri sono X.509 versione 3.

8.1.2 Estensioni del certificato

I certificati qualificati sono caratterizzati dalle estensioni presenti nei qcStatement clause 3.2.6 of IETF RFC 3739. Il loro utilizzo è regolato dalla norma ETSI 319 412-5.

Per le estensioni si rimanda all'Appendice.

8.1.3 OID dell'algoritmo di firma

I certificati sono firmati con il seguente algoritmo:

sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11].

8.1.4 Forme di nomi

Ogni certificato contiene un numero di serie univoco all'interno della CA che lo ha emesso.

8.1.5 Vincoli ai nomi

Si veda in merito il paragrafo 4.1.

8.1.6 OID del certificato

Si veda in merito il paragrafo 2.2, 2.4 e 5.5.3.

8.2 Formato della CRL

Per formare le liste di revoca CRLs, Cedacri utilizza il profilo RFC5280 “Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)” e aggiunge al formato di base le estensioni come definite da RFC 5280: “Authority Key Identifier”, “CRL Number”, “Issuing Distribution Point” e “expiredCertsOnCRL”.

8.2.1 Numero di versione

Tutti le CRL emesse da Cedacri sono X.509 versione 2.

8.2.2 Estensioni della CRL

Per le estensioni della CRL si veda l’Appendice.

8.3 Formato dell’OCSP

Cedacri, al fine di determinare lo stato di revoca del certificato senza fare richiesta alla CRL, utilizza il protocollo OCSP conforme al profilo RFC6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”. Tale protocollo specifica i dati che devono essere scambiati da un’applicazione che vuole verificare lo stato del certificato.

8.3.1 Numero di versione

Il protocollo OCSP utilizzato da Cedacri è conforme alla versione 1 del RFC6960.

8.3.2 Estensioni dell’OCSP

Per le estensioni dell’OCSP si veda l’Appendice.

9 Controlli e valutazione di conformità

In qualità di QTSP per la firma elettronica qualificata ai sensi della normativa europea, Cedacri è soggetta a un periodico accertamento di conformità ("vigilanza") da parte del Conformity Assessment Body (CAB).

Tale valutazione di conformità è effettuata ai sensi del Regolamento EIDAS e della Norma ETSI EN 319 401, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319_403 e UNI CEI EN ISO/IEC17065:2012.

Inoltre, Cedacri è conforme agli standard ISO 9001 e ISO 27001, anche con riferimento ai servizi di firma elettronica qualificata.

9.1 Frequenza o circostanze per la valutazione di conformità

La valutazione di conformità viene ripetuta ogni due anni, ma ogni anno il CAB esegue un audit di sorveglianza almeno annualmente.

9.2 Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da DNV-GL

Indirizzo: Via Energy Park 14, 20871 Vimercate MBTelefono:039 689 0029

9.3 Rapporti tra CEDACRI e CAB

Non esiste alcuna relazione tra Cedacri e DNV-GL (a titolo esemplificativo rapporti di partnership o interessi finanziari) che possa in alcun modo influenzare l'esito delle verifiche svolte.

Per quanto riguarda la struttura di Internal Auditing di Cedacri, essa risponde direttamente al board ed è indipendente dalle altre strutture aziendali.

9.4 Aspetti oggetto di valutazione

Il CAB valuta la conformità rispetto al Manuale Operativo, al Regolamento e alla normativa applicabile delle procedure adottate, dell'organizzazione della CA, dell'organizzazione dei ruoli, della formazione del personale, della documentazione contrattuale.

9.4.1 Azioni in caso di non conformità

Qualora in fase di audit dovessero essere rilevate degli aspetti non conformi rispetto alle normative di riferimento, sarà in carico al CAB decidere se inviare comunque il rapporto ad

Agid oppure riservarsi un congruo periodo di tempo necessario per verificare l'efficacia delle azioni correttive messe in atto per sanare tali anomalie.

10 Altri aspetti

10.1 Tariffe

10.1.1 Tariffe per il rilascio e il rinnovo dei certificati

Le tariffe per l'emissione, il rinnovo, la revoca e la sospensione dei certificati saranno definite su base progettuale.

Tali tariffe sono comunque in funzione delle quantità trattate e soggette all'andamento del mercato e pertanto non vengono pubblicate sul sito della CA.

Per informazioni, scrivere all'indirizzo di posta elettronica:

servizifiduciari-cedacri@iongroup.com

10.1.2 Tariffe per l'accesso ai certificati

Gli elenchi dei Certificati in vigore (previa autorizzazione del Soggetto alla pubblicazione), sono disponibili sul sito https://www.cedacricert.it.

10.1.3 Tariffe per l'accesso alle informazioni sullo stato di sospensione e revoca dei certificati

Gli elenchi dei Certificati revocati (CRL), sono disponibili sul sito https://www.cedacricert.it.

10.1.4 Politiche per il rimborso

I clienti dovranno risarcire Cedacri per eventuali danni eventualmente sofferti dalla stessa nei seguenti casi:

- falsa dichiarazione nella richiesta di certificazione;
- omessa informazione su atti o fatti essenziali per negligenza o dolo;
- utilizzo di nomi (per es. nomi di dominio, marchi commerciali) in violazione dei diritti di proprietà intellettuale.

10.2 Responsabilità finanziaria

10.2.1 Copertura assicurativa e indennizzi

Il massimale di indennizzo per eventuali danni causati dall'inadempienza o negligenza di Cedacri è fissato in:

- € 500.000 per singolo sinistro;
- € 1.500.000 per annualità assicurativa.

10.2.2 Altre attività

n/a

10.2.3 Garanzia o copertura assicurativa per i soggetti finali

Si veda il paragrafo 10.2.1.

10.3 Confidenzialità delle informazioni

10.3.1 Ambito di applicazione delle informazioni confidenziali

Nell'ambito dell'attività oggetto del presente Manuale Operativo non è prevista la gestione di informazioni confidenziali.

10.3.2 Informazioni non rientranti nell'ambito di applicazione delle informazioni confidenziali

n/a

10.3.3 Responsabilità di protezione delle informazioni confidenziali

n/a

10.4 Privacy

Le informazioni raccolte dal QTSP nell'esercizio delle proprie funzioni vengono raccolte su supporti cartacei e successivamente immesse nel sistema informatico dello stesso. Non sono presenti categorie particolari di dati personali e relativi a condanne penali e reati ai sensi degli artt. 9 e 10 del Regolamento UE 2016/679.

I supporti cartacei sono archiviati anche elettronicamente e mantenuti per il periodo di 20 anni.

I dati forniti sono divisi in due categorie: obbligatori e facoltativi, così come contrassegnati nella richiesta di attivazione.

I dati obbligatori sono quelli necessari per lo svolgimento dei Servizi, il loro conferimento è obbligatorio ed un eventuale rifiuto allo stesso comporterà l'impossibilità di concludere il contratto. Parte di essi sono pubblicati nel certificato, comunicati e diffusi, anche in Paesi al di fuori dell'Unione Europea, attraverso l'inserimento dello stesso nel registro dei certificati.

In ogni caso, il QTSP si atterrà a quanto previsto dal Regolamento UE 2016/679, nel trattamento dei dati personali di cui verrà in possesso e nell'adozione delle relative misure di sicurezza.

10.4.1 Gestione in ambito privacy

Cedacri adotta un approccio integrato al Sistema Qualità e Sicurezza in accordo con le normative ISO9001 e ISO 27001 che garantisce un insieme di policy, prassi e procedure di gestione dei processi aziendali e della integrità, riservatezza e disponibilità dei dati e delle informazioni gestiti conforme alle normative vigenti in materia.

10.4.2 Dati che sono trattati come personali

Sono trattati come dati i personali i dati che ricadono nella corrispondente definizione di cui alla normativa vigente; per dato personale si intende quindi qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

10.4.3 Dati non considerati come personali

I dati per i quali è previsto che siano resi pubblici dalla gestione tecnica della CA, ovvero chiave pubblica, certificato (se richiesto dal Soggetto), date di revoca e di sospensione del certificato, non sono considerati dati personali.

10.4.4 Informativa privacy e consenso al trattamento dei dati personali

L'informativa privacy è allegata ai Moduli di Richiesta ed è disponibile sul sito https://www.cedacricert.it nella sezione Download.

Mediante la compilazione del modulo "Richiesta di attivazione" Cedacri informa il Soggetto, ai sensi e per gli effetti di cui all'art. 13 del Regolamento UE 2016/679, che i suoi dati personali saranno trattati, con l'ausilio di archivi cartacei e di strumenti informatici e telematici idonei a garantire la massima sicurezza e riservatezza.

10.4.5 Divulgazione dei dati a seguito di richiesta da parte dell'autorità

La divulgazione di dati su richiesta delle Autorità è obbligatoria e viene svolta nelle modalità stabilite volta per volta dall'Autorità stessa.

10.4.6 Altri motivi di divulgazione

I dati forniti verranno trattati al fine di fornire i Servizi previsti nel presente contratto e potranno essere comunicati alle società che forniscono consulenza ed assistenza tecnica alla CA.

10.5 Proprietà intellettuale

Il presente Manuale è di proprietà di Cedacri che si riserva tutti i diritti ad esso relativi.

10.6 Rappresentanza e garanzie

Si rimanda alla contrattualistica tra la CA e il soggetto per il dettaglio delle garanzie e responsabilità in carico a ciascun soggetto.

10.7 Limitazione di garanzia

Cedacri non presta alcuna garanzia sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dal Titolare; su usi della chiave privata, del dispositivo sicuro di firma – quando presente - e/o del certificato di sottoscrizione, che siano diversi rispetto a quelli previsti dalle norme vigenti e dal presente Manuale Operativo; sul regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali; sulla validità e rilevanza, anche probatoria, del certificato di sottoscrizione - o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il certificato è riferito, ferma restando l'efficacia di firma autografa riconosciuta alla firma elettronica qualificata, ai sensi dell'art. 25 del Regolamento (UE) n. 910/2014; sulla segretezza e/o integrità di qualsiasi messaggio, atto o documento associato al certificato di sottoscrizione o confezionato tramite le chiavi a cui il certificato è riferito (nel senso che eventuali violazioni di quest'ultima sono, di norma, rilevabili dal Titolare o dal destinatario attraverso l'apposita procedura di verifica). Il Certificatore garantisce unicamente il funzionamento del Servizio, secondo quanto indicato al paragrafo 10.11.

10.8 Limitazione di responsabilità

Cedacri non assume alcun obbligo di sorveglianza in merito al contenuto, alla tipologia o al formato elettronico dei documenti e/o, eventualmente, degli hash trasmessi dalla procedura informatica indicata dal Richiedente o dal Titolare, non assumendo alcuna responsabilità, in merito alla validità e riconducibilità degli stessi all'effettiva volontà del Titolare. Fatto salvo il caso di dolo o colpa, Cedacri non assume responsabilità per danni diretti e indiretti subiti dai Titolari e/o da terzi in conseguenza dell'utilizzo o del mancato utilizzo dei certificati di sottoscrizione rilasciati in base alle previsioni del presente Manuale e delle Condizioni Generali dei Servizi di Certificazione. Cedacri non è responsabile di qualsiasi danno diretto e/o indiretto derivante in via anche alternativa dalla perdita, dalla impropria conservazione, da un improprio utilizzo, degli strumenti di identificazione e di autenticazione e/o dalla mancata osservanza di quanto sopra, da parte del Titolare. Cedacri, inoltre, fin dalla fase di formazione del Contratto per i servizi di Certificazione, e anche nel corso dell'esecuzione, non risponde per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informatico e della rete internet. Cedacri, salvo il caso di dolo o colpa, non sarà gravata da oneri o responsabilità per danni diretti o indiretti di qualsiasi natura ed entità che dovessero

verificarsi al Titolare, al Richiedente e/o a terzi causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati da parte di terzi non autorizzati da Cedacri.

10.8.1 Termine

Al termine del rapporto tra CA e Soggetto il certificato viene revocato.

10.8.2 Risoluzione

Tali aspetti sono dettagliati nel contratto che regola il servizio.

10.8.3 Effetti della risoluzione

Il contratto tra CA e il Soggetto si risolve automaticamente, con conseguente interruzione del Servizio, in caso di revoca del certificate.

10.9 Foro competente

I rapporti tra CA e il Soggetto sono regolati dalla legge italiana.

Per qualsiasi controversia dovesse sorgere in dipendenza dei Servizi disciplinati dal presente contratto il foro competente è quello di Milano.

10.10 Legge applicabile

La legge applicabile al presente Manuale Operativo è la legge italiana.

10.11 Erogazione del servizio

Il Servizio viene erogato come dalla seguente tabella:

Tipo del Servizio	Giorni di disponibilità	Orario di disponibilità
Disponibilità delle liste: Chiavi Pubbliche Chiavi Revocate (CRL)	7 giorni su 7	24 ore su 24 (disponibilità minima mensile 99%)
Rilascio del Certificato qualificato	Giorni feriali	09:00 - 13:00 e 14:00 - 18:00
Sospensione del Certificato qualificato	7 giorni su 7	24 ore su 24
Revoca del Certificato qualificato	7 giorni su 7	24 ore su 24

Tabella 4: Erogazione del servizio

11 Appendice

11.1ASN1 Dump Root CA certificate: Cedacricert EU 2019

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (58 bit) 145225339350479356
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (4 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-00432960342
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String Cedacri SpA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Cedacricert EU 2019
    SEQUENCE (2 elem)
      UTCTime 2019-07-09 10:08:21 UTC
      UTCTime 2039-07-10 10:08:21 UTC
    SEQUENCE (4 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-00432960342
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String Cedacri SpA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Cedacricert EU 2019
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (1 elem)
        SEQUENCE (2 elem)
                                                    INTEGER (4096             bit)
8910014676809082466968120845568227858552830307363940720379210737708 13…
          INTEGER 65537
    [3] (1 elem)
      SEQUENCE (5 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
```

```
          OCTET STRING (1 elem)
            OCTET STRING (20 byte) 4F2A6C3222EAC18E9DBFC997F49AC05B94F540AA
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              BOOLEAN true
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              [0] (20 byte) 4F2A6C3222EAC18E9DBFC997F49AC05B94F540AA
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.76.27.1.1.2
                SEQUENCE (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String http://www.cedacricert.it/cedacricert/en/documentazione/
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            BIT STRING (7 bit) 0000011
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
    NULL
  BIT                                   STRING (4096                                  bit)
1100111100011101101101000110010100100110101000011110000101000110111001…
```

11.2ASN1 Dump End User: Cedacricert EU 2019

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 8044746428757289316
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (4 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-0011111111
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String Cedacri SpA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Cedacricert EU 2019
    SEQUENCE (2 elem)
      UTCTime 2019-07-17 12:13:51 UTC
      UTCTime 2022-07-17 12:13:51 UTC
    SEQUENCE (8 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
```

```
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-02144370547
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String OrgName
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
          UTF8String Cognome
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
          UTF8String Nome
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
          PrintableString TINIT-DGDFDF87C26G343F
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Nome Cognome
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.46 dnQualifier (X.520 DN component)
          PrintableString DGDFDF87C26G343F
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (1 elem)
        SEQUENCE (2 elem)
                                                          INTEGER (2048             bit)
25513000521548391674762357327930318780190291616519842881795451608245 5…
          INTEGER 65537
    [3] (1 elem)
      SEQUENCE (8 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (1 elem)
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority
info access descriptor)
                [6] http://www.cedacricert.it/cedacricert/en/download/CertificatoRoot.html
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] http://www.cedacricert.it/ocspqual
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (1 elem)
            OCTET STRING (20 byte) B9359B2F374221FD09156C3031F9DA36DDC8D76E
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              [0] (20 byte) 4F2A6C3222EAC18E9DBFC997F49AC05B94F540AA
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
          OCTET STRING (1 elem)
```

```
          SEQUENCE (6 elem)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.194121.1.1
            SEQUENCE (1 elem)
                 OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862
qualified certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862
qualified certificates)
              INTEGER 20
            SEQUENCE (1 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified
certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.6.1
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.5
              SEQUENCE (1 elem)
                SEQUENCE (2 elem)
                  IA5String https://www.cedacricert.it/cedacricert/en/documentazione/
                  PrintableString en
       SEQUENCE (2 elem)
         OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
         OCTET STRING (1 elem)
           SEQUENCE (2 elem)
             SEQUENCE (2 elem)
               OBJECT IDENTIFIER 1.3.76.27.1.1.2.1
               SEQUENCE (1 elem)
                 SEQUENCE (2 elem)
                   OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                   IA5String https://www.cedacricert.it/cedacricert/en/documentazione/
             SEQUENCE (1 elem)
               OBJECT IDENTIFIER 0.4.0.194112.1.2
       SEQUENCE (2 elem)
         OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
         OCTET STRING (1 elem)
           SEQUENCE (1 elem)
             SEQUENCE (1 elem)
               [0] (1 elem)
                 [0] (1 elem)
                   [6] http://www.cedacricert.it/crl/crlEU2019.crl
       SEQUENCE (3 elem)
         OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
         BOOLEAN true
         OCTET STRING (1 elem)
           BIT STRING (2 bit) 01
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
    NULL
  BIT                                 STRING (4096                                bit)
1000101100001000010100011010101100011001100111000100011100110100110001…
```

11.3Valori ed estensioni per CRL e OCSP

Le CRL hanno le seguenti estensioni:

Extension	Value
Authority Key Identifier	Il valore dell'impronta 160-bit SHA-1 di issuerPublicKey
CRL number	Il numero univoco della CRL assegnato dalla CA
ExpiredCertsOnCRL	La data in formato GeneralizedTime dalla quale i certificati scaduti sono tenuti in CRL. Il valore è impostato uguale alla data di emissione
Issuing Distribution Point	Identifica il punto di distribuzione delle CRL e lo scopo: indica se la CRL è generata solo per certificati di CA, solo certificati di attributo o del soggetto
Invalidity Date	Data in formato UTC che indica la data da cui si ritiene che il certificate sia invalido

Tabella 5: Valori ed estensioni per CRL

La richiesta OCSP contiene i seguenti campi:

Field	Value
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Hash del DN dell'emittente
Issuer Key Hash	Hash della chiave pubblica dell'emittente.
Serial Number	Numero di serie del certificato

Tabella 6: Valori ed estensioni per OCSP

La risposta OCSP contiene i seguenti campi:

Field	Value
Response Status	Stato della rispsosta OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN del certificcato della risposta OCSP.

Produced at	Data in formato GeneralizedTime di quando è stata generate la risposta
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Subject Certificate Name Hash	Hash del subject's DN del certificato verificato
Subject Certificate Key Hash	Hash della chiave pubblica del certificato verificato
Serial Number	Numero di serie verificato
thisUpdate	LA data di verifica dello stato del certificato in formato GeneralizedTime
nextUpdate	LA data in cui lo stato del certificato verificato è cambiato
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

Tabella 7: Risposta per OCSP

12 Riferimenti

Codice	Titolo	Tipologia
PO00004	Codice di Comportamento	Documento Interno
PR00001	Gestione delle Risorse Umane	Documento Interno

13 Elenco allegati

- *Nessun allegato*