Manuale Operativo Firma Elettronica Qualificata Cedacri - CP e CPS

Codice documento:	IA00G009-011
Stato del documento:	Approvato
Data emissione:	30/05/2023
Ente emittente:	CISO

Responsabile documento	Giuliano Merlo	
Redazione:	Domenico Garuffi	
Verifica:	ORGA, ICTGE	30/05/2023 Data*
Approvazione:	CISO	29/05/2023 Data
Codice Documento*:	IA00G009-011	30/05/2023
Stato Documento*:	Pubblicato	
Distribuzione:	Pubblico	

Data Emissione Prima Versione:	05/06/2017
Data di Stampa:	30/05/2023

LEGENDA

*Il redattore **non deve compilare** i campi contrassegnati con asterisco " * " in quanto le informazioni relative vengono aggiornate **automaticamente** in sede di stampa sulla base di quanto indicato nel frontespizio del documento. Per aggiornare a video tali campi, fare clic col pulsante destro del mouse e dal menù contestuale selezionare **aggiorna campo.***
*Per aggiornare a video ogni pagina con la corretta intestazione, fare doppio clic sull'intestazione stessa, selezionare col pulsante destro del mouse i campi del codice, data emissione e titolo, quindi scegliere dal menù contestuale **aggiornacampo**. Gli altri campi, anche se non pertinenti, vanno compilati **almeno con un carattere <spazio>.***

Distribuzione

La distribuzione è un campo da compilare manualmente e può assumere i valori:

- *Pubblica, se il documento può circolare senza restrizioni, sia internamente che esternamente;*
- *Riservata, se il documento è distribuibile solo agli Utenti Cedacri o all'interno di un Gruppo di Progetto (specificare il Gruppo di progetto);*
- *Confidenziale, se il documento è distribuibile internamente a livello personale (specificare le persone)*
- *Utente, se il documento è destinato all'Organizzazione del Cliente*
- *<altro>, da specificare.*

Storia delle Modifiche

Modifiche dalla Versione 1 alla Versione 2 (Giugno 2017)

Aggiornati massimali secondo Polizza aziendale in essere

Modifiche dalla Versione 2 alla Versione 3 (Giugno 2017)

Modificato paragrafo 1.2 “Nome ed identificativo del documento”

Rinominato paragrafo 9.2 “Risoluzione delle controversie e gestione dei reclami” inserendo modalità di gestione dei reclami

Modifiche dalla Versione 3 alla Versione 4 (Agosto 2017)

Modificato appendice 10.1

Modificato appendice 10.2

Modifiche dalla Versione 4 alla Versione 5 (Ottobre 2017)

Modificato paragrafo 5.7 e sottoparagrafo 5.7.1 in funzione della comunicazione AgiD del 19/04/17 riguardante i *“Requisiti di sicurezza relativi ai prestatori di servizi fiduciari - Adempimenti previsti dall'art. 19 del Regolamento (UE) 910/2014”*

Modificato paragrafo 5.8 “Cessazione del Servizio della CA o della RA”

Modifiche dalla Versione 5 alla Versione 6 (Settembre 2018)

Aggiornato paragrafo 1.4.1

Aggiornato paragrafo 4.5.2

Aggiornati riferimenti normativi paragrafo 5.3.3

Aggiornati riferimenti normativi paragrafo 9.4

Aggiornati riferimenti normativi paragrafo 9.4.4

Aggiornati riferimenti normativi paragrafo 9.14 – GDPR

Modifiche dalla Versione 6 alla Versione 7 (Luglio 2019)

Modifica capitolo 9 con inserimento dettagli di indennizzo nel paragrafo 9.2

Modifica Legale Rappresentante paragrafo 1.3.1

Aggiornato paragrafo 1.2 - Nome ed identificativo del documento

Aggiornato paragrafo 2.2.2 - Pubblicazione dei certificati

Aggiornato paragrafo 2.2.3 - Pubblicazione delle liste di revoca e sospensione

Aggiornato paragrafo 4.5.3 – Limiti d’uso e di valore

Aggiornato paragrafo 9.1.2 - Tariffe per l’accesso ai certificati

Aggiornato paragrafo 9.1.3 - Tariffe per l’accesso alle informazioni sullo stato di sospensione e revoca dei certificati

Aggiornato Paragrafo 9.13 – Leggi Applicabile

Inserito paragrafo 10.4 – ASN1 Dump Root CA Certificate

Inserito paragrafo 10.5 - ASN1 Dump End User

Aggiornato paragrafo 9.7 – Limitazioni di garanzia

Aggiornato paragrafo 9.7 – Limitazioni di responsabilità

Modifiche dalla Versione 7 alla Versione 8 (Agosto 2020)

Aggiornato Capitolo 10 – Eliminati tutti i riferimenti a Cedacricert CA 2017 in quanto dismessa

Modifiche dalla Versione 8 alla Versione 9 (Febbraio 2021)

Aggiornato paragrafo 1.2 – Ente Emittente

Aggiornato paragrafo 1.3.1 – Aggiornati i dati dell'Organizzazione

Aggiornato paragrafo 1.5.2 – Responsabile documento

Modifiche dalla Versione 9 alla Versione 10 (Giugno 2021)

Aggiornato paragrafo 1.5.4 – Revisione del Manuale Operativo e storia modifiche specificato revisione almeno annuale

Aggiornato 3.2.3 - Identificazione della persona fisica

Aggiornato paragrafo 4.9.3 **-** Procedure per richiedere la revoca aggiornando casistiche relative Revoca su iniziativa della Certification Authority

Modifiche dalla Versione 10 alla Versione 11 (Maggio 2023)

Aggiornato paragrafo 1.3.1 – Aggiornati i dati dell'Organizzazione

Aggiornato paragrafo 5.7.1 – Aggiornamento processo di comunicazione incident

Aggiunto paragrafo 1.7 – Riferimenti e Allegati

SOMMARIO

1. INTRODUZIONE

1.1. QUADRO GENERALE

In 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 è il Manuale Operativo del **Prestatore di Servizi Fiduciari Qualificato** (Qualified *Trust Service Provider - QTSP*) nel seguito anche Cedacri che fornisce servizi di firma elettronica qualificata.

Tale manuale contiene le politiche e le pratiche seguite nel processo di identificazione e emissione del certificato qualificato e tutto ciò che rende affidabile un 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 e recepisce le raccomandazioni del documento "Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" © Internet Society 2003.

1.2. NOME ED IDENTIFICATIVO DEL DOCUMENTO

Il presente documento si pone in continuità con il documento aziendale denominato "Manuale Operativo" avente le seguenti caratteristiche:

Codice IA00G009

Enti Emittenti System Security e Certificazioni

Nome Documento Manuale Operativo Firma Elettronica Qualificata Cedacri- CP e CPS

Data di validità: Il presente Documento ha validità dalla data di approvazione della Relazione di Conformità emessa dal CAB

Al documento è associato l'*object identifier* (OID); quello che identifica Cedacri è ***1.3.76.27***

Le policy per i certificati qualificati sono relative a:

- Manuale-operativo-certificato qualificato emesso a persona fisica e chiavi su dispositivo qualificato (QSCD) conforme alla policy QCP-n-qscd 0.4.0.194112.1.2

Questo documento è pubblicato in formato elettronico presso il sito Web del QTSP all'indirizzo: https://www.cedacricert.it/, sezione "Documentazione".

1.3. PARTECIPANTI E RESPONSABILITÀ

1.3.1 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:

0

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 Executive Chairman***
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 **Certification Authority** è tenuta ad adottare tutte le misure tecniche e organizzative idonee per un tale servizio.

In particolare, il Certificatore che rilascia certificati qualificati è tenuto a:

- accertarsi dell'identità della persona che fa richiesta di Certificato;
- rilasciare il relativo Certificato qualificato nelle modalità previste;
- informare i titolari sulle caratteristiche del servizio;
- adottare le necessarie misure di sicurezza per il trattamento dei dati personali;
- garantire che il dispositivo sicuro per la generazione della firma abbia le caratteristiche richieste dai regolamenti;
- garantire che il soggetto titolare mantenga sempre in modo esclusivo il controllo

delle proprie chiavi di firma;
- garantire che le chiavi private di firma generate all'interno degli HSM non possano essere esportate;
- mantenere aggiornata la lista dei Certificati revocati;
- mantenere aggiornata la lista dei Certificati sospesi;
- gestire tutte le procedure necessarie ai fini delle attività di cui sopra, secondo adeguate norme di sicurezza;
- mantenere le registrazioni di tutte le informazioni relative alla gestione del certificato qualificato per almeno venti anni.

Il QTSP è direttamente responsabile nei confronti dei Soggetti per il proprio operato, salvo ogni diritto di rivalsa

1.3.2 Registration authority (RA)

Il Certificatore può dare mandato a svolgere le funzioni di **Ente di registrazione** o **Registration Authority** a Banche, Istituti di Credito o altre Entità che avranno sottoscritto con il Certificatore uno specifico contratto di mandato.

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 verranno pubblicati sul sito web www.cedacricert.it .

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

1.3.3 Soggetto

Il **Soggetto** è la persona fisica titolare del certificato qualificato, all'interno del quale sono inseriti i dati identificativi fondamentali. In alcune parti del Manuale e in alcuni limiti d'uso può essere definito anche Titolare che 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, dei suoi obblighi in quanto Titolare e più in generale degli obblighi di cui al presente "Manuale".

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.

1.3.4 Utente

È il soggetto che riceve un documento informatico sottoscritto con il certificato digitale del Soggetto, e che fa affidamento sulla validità del certificato medesimo (e/o sulla firma digitale ivi presente) per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

L'**Utente** delle chiavi pubbliche certificate è tenuto a svolgere almeno le seguenti azioni:

- Verificare che la tipologia del certificato utilizzato;
- 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.

1.3.5 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. Il ruolo, quando presente, può essere assunto anche dalla RA.

Nello specifico si individuano le seguenti casistiche:

- 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, nel certificato viene inserita l'indicazione dell'Organizzazione a cui il Soggetto stesso è collegato, e/o del ruolo.

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

1.3.6 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. In tale veste, AgID effettua la vigilanza sui prestatori di servizi fiduciari qualificati stabiliti nel territorio italiano al fine di garantirne la rispondenza ai requisiti stabiliti dal Regolamento.

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.

1.4. USO DEL CERTIFICATO

1.4.1 Usi 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.

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

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

1.4.2 Usi 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.

1.5. AMMINISTRAZIONE DEL MANUALE OPERATIVO

1.5.1 Contatti

Cedacri è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. 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.

1.5.2 Soggetti responsabili dell'approvazione del Manuale Operativo

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

1.5.3 Procedure di approvazione

La redazione e approvazione del manuale segue le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda 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.

1.5.4 Revisione del Manuale Operativo e storia modifiche

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

Come descritto nel precedente paragrafo, tutte le variazioni al Manuale sono tracciate, in un'apposita sezione chiamata "Storia delle Modifiche" e una volta raggiunta l'approvazione, il documento viene prontamente pubblicato e reso disponibile secondo le modalità previste. 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.

E' garantita almeno una revisione annuale del Manuale Operativo.

1.5.5 Periodo e maccanismo di notifica

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

1.6. DEFINIZIONI E ACRONIMI

1.6.1 Definizioni

Dal regolamento europeo 910/2014 eIDAS, Art 3:

1) «identificazione elettronica», 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;

2) «mezzi di identificazione elettronica», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;

3) «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;

4) «regime di identificazione elettronica», 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;

5) «autenticazione», 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;

6) «parte facente affidamento sulla certificazione», una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario;

7) «organismo del settore pubblico», 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;

8) «organismo di diritto pubblico», un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio (1);

9) «firmatario», una persona fisica che crea una firma elettronica;

10) «firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

11) «firma elettronica avanzata», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;

12) «firma elettronica qualificata», 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;

13) «dati per la creazione di una firma elettronica», i dati unici utilizzati dal firmatario per creare una firma elettronica;

14) «certificato di firma elettronica», 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;

15) «certificato qualificato di firma elettronica», 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;

16) «servizio fiduciario», 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;

17) «servizio fiduciario qualificato», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;

18) «organismo di valutazione della conformità», 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;

19) «prestatore di servizi fiduciari», 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;

20) «prestatore di servizi fiduciari qualificato», 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;

21) «prodotto», un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;

22) «dispositivo per la creazione di una firma elettronica», un software o hardware configurato utilizzato per creare una firma elettronica;

23) «dispositivo per la creazione di una firma elettronica qualificata», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;

24) «creatore di un sigillo», una persona giuridica che crea un sigillo elettronico;

25) «sigillo elettronico», 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;

26) «sigillo elettronico avanzato», un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;

27) «sigillo elettronico qualificato», 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;

28) «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

29) «certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;

30) «certificato qualificato di sigillo elettronico», 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;

31) «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;

32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;

33) «validazione temporale elettronica», 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;

34) «validazione temporale elettronica qualificata», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;

35) «documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;

36) «servizio elettronico di recapito certificato», 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;

37) «servizio elettronico di recapito qualificato certificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;

38) «certificato di autenticazione di sito web», un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;

39) «certificato qualificato di autenticazione di sito web», 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;

40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;

41) «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

1.6.2 Acronimi

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)

1.7. RIFERIMENTI E ALLEGATI

[1]

Cedacri S.p.A.

IA99Q013 – Codice di Comportamento

Documento Interno

[2]

Cedacri S.p.A.

XQ99Q880 – Gestione delle Risorse Umane

Documento Interno

2. PUBBLICAZIONE E ARCHIVIAZIONE

2.1. ARCHIVIAZIONE

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

2.2. PUBBLICAZIONE DELLE INFORMAZIONI SULLA CERTIFICAZIONE

2.2.1 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 pubblicate presso l'elenco dei certificatori.

2.2.2 Pubblicazione dei certificati

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

2.2.3 Pubblicazione delle liste di revoca e sospensione

Le liste di Revoca revocati (CRL) sono disponibili sul sito https://www.cedacricert.it/ e vi si accede seguendo le istruzioni dei menu di navigazione.

2.3. PERIODO O FREQUENZA DI PUBBLICAZIONE

2.3.1 Frequenza di pubblicazione del manuale operativo

Il manuale operativo viene pubblicato con frequenza variabile se sono subentrati dei 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.

2.3.2 Frequenza pubblicazione delle liste di revoca e sospensione

I Certificati revocati vengono inseriti nella CRL (lista dei Certificati revocati), emessa dal QTSP, marcata temporalmente e pubblicata.

La pubblicazione ordinaria della suddetta lista, con validità di 24 ore, avviene con cadenza giornaliera ogni 6 ore.

In caso di richiesta di revoca immediata, la lista dei Certificati revocati (CRL) sarà prontamente pubblicata.

2.3.3 Controllo degli accessi agli archivi pubblici

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

3. IDENTIFICAZIONE E AUTENTICAZIONE

3.1. DENOMINAZIONE

3.1.1 Tipi di nomi

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

3.1.2 Necessità che il nome abbia un significato

L'attributo del certificato Distinguished Name (DN) identifica in maniera univoca il soggetto al quale è rilasciato il certificato.

3.1.3 Anonimato e pseudonimia dei richiedenti

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

3.1.4 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.

3.1.5 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 esso 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.

3.2. CONVALIDA INIZIALE DELL' IDENTITÀ

Questo capitolo descrive le procedure usate 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.

3.2.1 Metodo per dimostrare il 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

3.2.2 Autenticazione dell'identità delle organizzazioni

n/a

3.2.3 Identificazione della persona fisica

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

- Il Richiedente contatta l'azienda tramite i canali dedicati (mail a servizifiduciari-cedacri@iongroup.com o sistema di trouble ticketing), per ottenere un appuntamento con un RAO Cedacri al fine del rilascio Certificato
- 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 e mediante un collegamento interno, effettua l'autenticazione al sistema;
- Il RAO procede alla registrazione inserendo i dati anagrafici del Richiedente, più tutte le informazioni necessarie alla sua gestione successiva.

Come definito nell'articolo 24 del regolamento EIDAS, allorché rilascia un certificato qualificato per un servizio fiduciario, il QTSP verifica, mediante mezzi appropriati e conformemente al diritto nazionale, 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 concreta della persona fisica

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

Nel modulo di richiesta per il certificato qualificato sono contenute sia i dati relativi all'identità del Soggetto che le informazioni che consentono di gestire il rapporto fra QTSP e Soggetto.

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 email

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 attestandolo mediante Autocertificazione.

La ragione sociale o la denominazione e il codice identificativo dell'Organizzazione saranno invece riportate nel certificato se essa 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 che indichino un limite di valore degli atti unilaterali e dei contratti per i quali il certificato stesso può essere usato, ferma restando la responsabilità del QTSP, 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.

Ferma restando la responsabilità della CA, l'identità del Soggetto può essere accertata dai soggetti abilitati ad eseguire il riconoscimento, attraverso le seguenti modalità

3.2.4 Identificazione della persona giuridica

n/a

3.2.5 Informazioni del Soggetto o del Richiedente non verificate

n/a

3.2.6 Validazione dell'autorità

Cedacri ovvero la RA verificano le informazioni richieste, definite nei paragrafi 3.2.3 e 3.2.4, per l'identificazione e validano la richiesta.

3.3. IDENTIFICAZIONE E AUTENTICAZIONE PER RINNOVO DELLE CHIAVI E DEI CERTIFICATI

Questo paragrafo descrive le procedure usate per l'autenticazione e identificazione del Soggetto nel caso di rinnovo del certificato qualificato di firma.

Il periodo di validità del Certificato è quello compreso nell'intervallo di tempo specificato dai campi del Certificato "Valid from" e "Valid to": nel primo vengono indicate la data e l'ora di inizio validità, nel secondo la data e l'ora di fine validità.

I Certificati emessi dalla Cedacri S.p.A. - Servizio Cedacricert hanno validità non superiore a 3 anni.

Il Soggetto che intende rinnovare il proprio Certificato deve farne domanda al QTSP, almeno 30 giorni prima della scadenza di quello in suo possesso. 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. L'avvenuto rinnovo del Certificato sarà notificato al Soggetto via posta elettronica all'ultimo indirizzo e-mail comunicato.

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.

Trascorso il periodo di validità del certificato, non è più possibile effettuare il rinnovo, ma si dovrà procedere ad una nuova registrazione da parte del Richiedente.

3.4. IDENTIFICAZIONE E AUTENTICAZIONE PER LA RICHIESTA DI REVOCA O SOSPENSIONE

3.4.1 Richiesta di Sospensione

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

La sospensione di un certificato digitale può rendersi necessaria nel caso che si debba verificare preventivamente la revoca dello stesso (ad esempio quando si abbia il dubbio ma non la certezza della perdita del controllo di uno o più dati per l'utilizzo del servizio di firma digitale)

La sospensione può avvenire su richiesta del Soggetto oppure su iniziativa del QTSP o su richiesta di un Terzo interessato compilando e sottoscrivendo il modulo.

Una volta sospeso il certificato rimarrà in tale stato per un periodo massimo di 90 (novanta) giorni trascorsi i quali se non più ripristinato, verrà automaticamente e definitivamente revocato.

Le procedure per la sospensione del certificato sono completamente analoghe a quelle descritte per la revoca dello stesso.

3.4.2 Richiesta di Revoca

Il Soggetto può richiedere la revoca del Certificato per uno dei seguenti motivi:

- la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
- sia stato smarrito il dispositivo sicuro di firma che contiene la chiave;
- sia venuta meno la segretezza della chiave o del suo codice di attivazione (PIN);
- si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;
- il Soggetto non riesce più ad utilizzare il dispositivo sicuro di firma in suo possesso (es. guasto del dispositivo).

Nel caso il Soggetto consegni la richiesta di revoca compilando e sottoscrivendo il modulo di revoca, l'operatore dell'Ente di Registrazione, accertata la corretta compilazione e sottoscrizione del modulo, si collega al sito di gestione dei certificati qualificati e revoca il certificato come da richiesta.

Nel caso di revoca attraverso canale telefonico, il certificato verrà temporaneamente sospeso per 6 giorni di calendario consecutivi, in attesa della consegna da parte del Soggetto del modulo di revoca opportunamente compilato e sottoscritto. In tal caso la data di revoca decorrerà dalla data di sospensione.

Contestualmente alla revoca, il certificatore pubblica automaticamente il certificato all'interno della CRL e notifica l'avvenuta revoca al Soggetto.

4. OPERATIVITA'

4.1. RICHIESTA DEL CERTIFICATO

4.1.1 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 RegistrationAuthority (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 RegistrationAuthority (se presente)

4.1.2 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, non necessariamente in quest'ordine. Nel processo, i diversi attori hanno responsabilità differenziate e concorrono congiuntamente al buon esito dell'emissione:

- **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.

4.2. ELABORAZIONE DELLA RICHIESTA

Il processo di enroll ha il principale compito di emettere il certificato di sottoscrizione.

A tale scopo 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 3.2.3
- 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 dallaCA.

4.2.1 Informazioni che il Soggetto deve fornire

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 commonName (nome comune) del SubjectDN del certificato. Il commonName, nel caso in cui non venisse fornito alcun ulteriore nome dal Soggetto o dal Richiedente, sarà valorizzato con nome e cognome del Soggetto stesso.

4.2.2 Esecuzione delle funzioni di identificazione e autenticazione

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 i codici segreti PIN e PUK 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 suo onere (o del Richiedente) ricordare il PIN.

4.2.3 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 anti-frode, dubbi sull'identità del Soggetto o del Richiedente, ecc.

4.2.4 Tempo massimo per l'elaborazione della richiesta del certificato

Il tempo che intercorre dal momento della richiesta di registrazione al momento di emissione del certificato dipende dalla modalità di richiesta prescelta dal Soggetto (o Richiedente) e dalla eventuale necessità di raccogliere ulteriori informazioni ovvero di consegnare fisicamente il dispositivo.

4.3. EMISSIONE DEL CERTIFICATO

4.3.1 Azioni della CA 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.

4.3.2 Notifica ai richiedenti dell'avvenuta emissione del certificato

In caso di emissione su dispositivo crittografico il Soggetto (o il Richiedente) non ha bisogno di notifica poiché il certificato è presente nel dispositivo che ha ricevuto.

4.3.3 Attivazione

In entrambi i casi citati nel paragrafo 4.3.1. il QTSP opera in maniera tale effettuare la fase di attivazione del Certificato durante la fase di registrazione che avviene negli Uffici Cedacri per opera del RAO.

4.4. ACCETTAZIONE DEL CERTIFICATO

4.4.1 Comportamenti concludenti di accettazione del certificato

n/a

4.4.2 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

4.4.3 Notifica ad altri soggetti dell'avvenuta pubblicazione del certificato

n/a

4.5. USO DELLA COPPIA DI CHIAVI E DEL CERTIFICATO

4.5.1 Uso 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 nazionali e internazionali.
- 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.

4.5.2 Uso 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, di richiedere e verificare marche temporali.

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

4.5.3 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).

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 per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza.

È inoltre facoltà del Soggetto richiedere al QTSP l'inserimento nel certificato di limiti di valore che indichino un limite di valore degli 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.

4.6. RINNOVO DEL CERTIFICATO

4.6.1 Motivi per il rinnovo

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

4.6.2 Chi può richiedere il rinnovo

Il Soggetto può richiedere il rinnovo del certificato 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.

Il rinnovo di 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.

4.6.3 Elaborazione della richiesta di rinnovo del certificato

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

4.7. 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.

4.8. MODIFICA DEL CERTIFICATO

In caso di variazioni dei dati presenti all'interno del certificato, non è possibile in alcun modo effettuare delle modifiche. Il certificato, come indicato al punto 3 del paragrafo 4.9.1, va revocato e riemesso con i dati corretti.

4.9. REVOCA E SOSPENSIONE DEL CERTIFICATO

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, pubblicata nel registro dei certificati con periodicità stabilita dalla CA (6 ore). Inoltre, la CA può emettere una CRL non programmata in determinate circostanze particolari. L'efficacia della revoca e della sospensione si ha dal momento di pubblicazione della lista, prendendo come riferimento la data attestata nel Giornale di Controllo della CA.

4.9.1 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, ovvero sia presente uno dei seguenti casi:
    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 un 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

4.9.2 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 e infine, il certificato può essere revocato d'ufficio dalla CA.

4.9.3 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, 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 decorrenza. I motivi per i quali il QTSP può autonomamente revocare il certificato non scaduto possono essere legati – a titolo esemplificativo- 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.

4.9.4 Grace Period della richiesta di revoca

Il periodo di grazia 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 ad ogni parte coinvolta, questo periodo è più lungo del periodo di tempo di cui la CA ha bisogno 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 detto grace Period non supera comunque le 24 ore.

4.9.5 Tempo massimo di elaborazione della richiesta di revoca

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

4.9.6 Frequenza di pubblicazione della CRL

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dal QTSP, e pubblicata nel Registro pubblico. La CRL viene pubblicata in modo programmato ogni 6 ore (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 nell'apposita estensione 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.

4.9.7 Latenza massima della CRL

Il tempo di attesa tra la richiesta di revoca o di sospensione e la sua realizzazione tramite pubblicazione della CRL è al massimo di 18 ore.

4.9.8 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 ore 7 giorni su 7.

4.9.9 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.

4.9.10 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 può essere sospeso d'ufficio da Cedacri.

4.9.11 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 ha sempre una durata limitata nel tempo. 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, 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 revoca 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.

Cedacri 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.

4.9.12 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 firmato, che si trova sul sito Cedacricert accompagnato da un documento di identità in corso di validità. Può essere inviato anche via PEC.

4.10. SERVIZI RIGUARDANTI LO STATO DEL CERTIFICATO

4.10.1 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.

4.10.2 Disponibilità del servizio

Il servizio OCSP è disponibile 24 ore per 7 giorni su 7

4.10.3 Caratteristiche opzionali

N/A

4.11. 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.

4.12. DEPOSITO PRESSO TERZI E RECOVERY DELLA CHIAVE

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

5. MISURE DI SICUREZZA E CONTROLLI

Tutte le misure di salvaguardia di Cedacri S.p.A sono inquadrate nel contesto generale del Manuale della Sicurezza che fornisce le prescrizioni fondamentali per la gestione dei sistemi ed il trattamento dei dati in ambiente sicuro. L'esistenza stessa del Manuale della Sicurezza come documento aziendale impegnativo per la Direzione costituisce la prima misura di salvaguardia sul piano dell'organizzazione.

Il quadro generale è completato da due strumenti descritti nel Manuale della Sicurezza, in cui viene regolamentata l'applicazione delle misure di salvaguardia:

- i Regolamenti d'Applicazione, o Manuali di Riferimento, in cui sono prescritte e descritte le misure di salvaguardia nei diversi ambiti
- l'organizzazione del personale per la sicurezza, con personale dedicato alla sicurezza ed alla privacy, e da personale non dedicato che svolge funzioni collaterali di sicurezza e di controllo.

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

5.1. 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.

5.1.1 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.

5.1.2 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 sono protetti 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'entratan egli 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.

5.1.3 Impianto elettrico e di climatizzazione

Nel rispetto degli standard, tecnici e operativi, indicati con riferimento al Tier III (Concurrently Maintainable Site Infrastructure) nel paragrafo intitolato "Tier Performance Standards" del documento pubblicato dall'Uptime Institute e intitolato "White Paper – Tier Classification Define Site Infrastructure Performance", il sito principale di Collecchio ed il sito secondario di Castellazzo Bormida hanno raggiunto la sostanziale conformità allo standard, come attestato dal report rilasciato da un ispettore certificato dall'Uptime Institute come Accredited Tier Designer (certified ATD Number 250 Uptimes Institute).

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 anti-allagamento. 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.

5.1.4 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.

5.1.5 Prevenzione e protezione contro gli incendi

Le Aree Riservate in cui sono collocati i sistemi dal Servizio di Firma Digitale Qualificata, sono soggetti a misure preventive antincendio e antiallagamento e, più in generale, verso incidenti fisici:

- non vi è contenuta carta né infiammabili, né mobilio o arredi facilmente combustibili, né quadri elettrici sprotetti; il carico d'incendio potenziale è ridotto al minimo
- non vi si trovano bombole di gas e sistemi locali di spegnimento degli incendi
- il sottopavimento è mantenuto pulito con interventi periodici ed i collegamenti elettrici che vi passano sono a norma del Decreto del Ministero dello Sviluppo Economico del 22 gennaio 2008, n.ro 37 [13].

Tutto l'edificio C2 è protetto da un impianto di rilevazione di fumo costituito da rilevatori ottici.

In ogni piano dell'edificio sono installati, in prossimità dei vani scala interni, idranti UNI 45 perfettamente corredati e mantenuti secondo le norme vigenti, in particolare UNI EN 14384:2006, UNI EN 14339:2006 UNI EN 14540:2006 e UNI 9487:2006 [15].

Sono installati vari estintori portatili che per numero e ubicazione sono tali da garantire un primo intervento, perfettamente corredati e mantenuti.

Nell'Area Riservata dell'edificio C2 Sala Server è inoltre in funzione un impianto di spegnimento automatico di incendio realizzato con estinguente NAF S3, in grado di proteggere l'intera Area Riservata.

Tutti i particolari degli impianti di rilevazione e spegnimento sono riportati nella documentazione "Valutazione del Rischio Incendi", redatta da Cedacri S.p.A. come previsto dal DM 10/3/98 e nella relativa documentazione sui "Criteri generali di sicurezza antincendio e per la gestione dell'emergenza nei Posti di Lavoro" (DLGS 81/2008).

Nell'area non si trova di regola personale. Il caso di rilevazione di incendio è segnalato alla Vigilanza interna, presente 7 giorni su 7 24 ore su 24.

5.1.6 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.

5.1.7 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.

5.1.8 Off-site backup

È realizzato nel sito di Disaster Recovery presso la sede di Castellazzo Bormida.

5.2. CONTROLLI PROCEDURALI

5.2.1 Ruoli chiave

Cedacri definisce, e mantiene aggiornate, procedure che rappresentano le modalità di gestione dei processi aziendali prevedendo ruoli e responsabilità e definendo adeguaticontrolliperlariduzionedeirischidiusoimproprioaccidentaleodeliberatodelsistema 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.

5.3. 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).

Si rimanda al documento XQ99Q880 Gestione delle Risorse Umane che descrive il processo di gestione delle risorse umane a partire dalla fase di selezione, al periodo di permenenza in azienda ed agli eventuali cambi di ruolo, fino alla fase di cessazione del rapporto di lavoro.

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

Si rimanda al documento XQ99Q880 Gestione delle Risorse Umane.

5.3.2 Procedure di controllo delle esperienze pregresse

Si rimanda al documento XQ99Q880 Gestione delle Risorse Umane.

5.3.3 Requisiti di formazione

Si rimanda al documento XQ99Q880 Gestione delle Risorse Umane.

5.3.4 Frequenza di aggiornamento della formazione

Si rimanda al documento XQ99Q880 Gestione delle Risorse Umane.

5.3.5 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.

5.3.6 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.

Si rimanda al documento XQ99Q880 Gestione delle Risorse Umane.

5.3.7 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).

5.3.8 Documentazione che il personale deve fornire

Si rimanda al documento XQ99Q880 Gestione delle Risorse Umane.

5.4. 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).

5.4.1 Frequenza di trattamento e di memorizzazione del giornale di controllo

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

5.4.2 Periodo di conservazione del giornale di controllo

Il giornale di controllo viene conservato per 20 anni.

5.4.3 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

5.4.4 Procedure di backup del giornale di controllo

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

5.4.5 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.

5.4.6 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,
- 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.

5.4.7 Notifica in caso di identificazione di vulnerabilità

Si applica il processo aziendale di gestione degli Incidenti di sicurezza (si veda paragrafo 5.7.1).

5.5. 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.

5.6. 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)

5.7. GESTIONE INCIDENTI E DISASTER RECOVERY

5.7.1 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.
L' incident è notificato presso l'Autorità di Vigilanza (AgiD) secondo le modalità condivise dall'Agenzia attraverso il portale (https://trustservices.agid.gov.it).

5.7.2 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.

5.7.3 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.

5.7.4 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.

5.8. 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 etc) 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

6. CONTROLLI TECNICI DI SICUREZZA

6.1. INSTALLAZIONE E GENERAZIONE DELLA COPPIA DI CHIAVI DI CERTIFICAZIONE

Per svolgere la sua 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 si firmano i certificati dei Soggetti.

Una volta generata le coppie 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 di persone.

Gli HSM dedicati al servizio sono posti uno a Collecchio e l'altro a Castellazzo e in entrambe le sedi le smart card precedentemente descritte sono conservate in apposite cassaforti.

Le chiavi private della CA vengono duplicate, al solo fine del loro ripristino in seguito alla rottura 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 ha 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 digenerazione;
- 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.

Quanto fatto ai punti precedenti sarà verbalizzato e il verbale sarà conservato dal QTSP per 20 anni

6.1.1 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.

6.1.2 Consegna della chiave privata al Richiedente

La chiave privata è contenuta nel dispositivo crittografico QSCD.

Con la consegna del dispositivo crittografico al Soggetto, questo entra in pieno possesso della chiave privata, che può utilizzare unicamente attraverso l'uso del PIN, di cui ha conoscenza esclusiva; tale dispositivo è consegnato non appena sono generate le chiavi.

6.1.3 Consegna della chiave pubblica alla CA

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

6.1.4 Consegna della chiave pubblica agli utenti

La chiave pubblica è contenuta nel certificato rilasciato solo al soggetto richiedente.

In conformità se il Richiedente ne fa richiesta, viene pubblicato anche nel registro pubblico, da dove può essere recuperato dall'Utente.

6.1.5 Algoritmo e lunghezza delle chiavi

La coppia di chiavi asimmetriche di certificazione è generata all'interno di un 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.

6.1.6 Controlli di qualità e generazione della chiave pubblica

I dispositivi utilizzati sono certificati secondo alti standard di sicurezza (si veda il par 6.2.1) 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.

6.1.7 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 in questo manuale operativo l'unico utilizzo permesso è il "*nonripudio*", ovvero possono essere utilizzati esclusivamente per firmare.

6.2. PROTEZIONE DELLA CHIAVE PRIVATA E CONTROLLI INGEGNERISTICI DEL MODULO CRITTOGRAFICO

6.2.1 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.

6.2.2 Controllo di più persone della chiave privata di CA

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

6.2.3 Deposito presso terzi della chiave privata di CA

n/a

6.2.4 Backup della chiave privata di CA

Il backup delle chiavi è contenuto in 4 differenti cassaforti 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 chi ha l'accesso ad almeno 2 cassaforti.

6.2.5 Archiviazione della chiave privata di CA

n/a

6.2.6 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.

6.2.7 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 cancellando il contenuto.

6.2.8 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

6.2.9 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 chiude inaspettatamente. La chiave così disattivata può essere riutilizzata solo dopo una nuova autenticazione del sottoscrittore del dipositivo.

6.2.10 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).

6.2.11 Classificazione dei moduli crittografici

n/a

6.3. Altri aspetti della gestione delle chiavi

n/a

6.3.1 Archiviazione della chiave pubblica

n/a

6.4. 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 al 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.

6.4.1 Dati di attivazione della chiave privata

Si rimanda ai paragrafi 4.2 e 6.3.

6.5. Controlli sulla sicurezza informatica

6.5.1 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.

6.6. 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

6.7. 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.

Ogni utente deve rigorosamente osservare le seguenti regole generali:

6.8. 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.

7. FORMATO DEL CERTIFICATO, DELLA CRL E DELL'OCSP

7.1. 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, version 3 per l'intera struttura PKI.

In Appendice il tracciato dei certificati di root e dei soggetti, per persone fisiche.

7.1.1 Numero di versione

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

7.1.2 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 vedere Appendice.

7.1.3 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].

7.1.4 Forme di nomi

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

7.1.5 Vincoli ai nomi

Si veda in merito il paragrafo 3.1.

7.1.6 OID del certificato

Si veda in merito il paragrafo 1.2

7.2. 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"

7.2.1 Numero di versione

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

7.2.2 Estensioni della CRL

Per le estensioni della CRL si veda l'Appendice

7.3. FORMATO DELL'OCSP

Cedacri per 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". Questo protocollo specifica i dati che devono essere scambiati da un'applicazione che vuole verificare lo stato del certificato.

7.3.1 Numero di versione

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

7.3.2 Estensionidell'OCSP

Per le estensioni dell'OCSP si veda l'Appendice

8. CONTROLLI E VALUTAZIONI DI CONFORMITÀ

Cedacri è un QTSP per la firma elettronica qualificata ai sensi della normativa europea; pertanto, 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.

In aggiunta a quanto detto, Cedacri è conforme agli standard ISO 9001 e ISO 27001 ed il campo di applicazione comprende, tra i servizi erogati da Cedacri, anche la Firma.

La conformità alle procedure e agli standard di sicurezza è verificata tramite un processo di audit interno.

Gli audit interni sono pianificati per verificare la conformità del Sistema di Gestione ai requisiti di sicurezza definiti da Cedacri e dalle norme internazionali di riferimento.

8.1. 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

8.2. 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

8.3. 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 Presidente / CdA ed è indipendente dalle altre strutture aziendali.

Essa deve assicurare la pianificazione e la realizzazione/coordinamento degli interventi per garantire, attraverso un'attività di auditing continuativa e strutturata, il rispetto delle procedure e degli standard adottati dalla Società nello svolgimento delle attività e dei processi interni a Cedacri, coerentemente alle strategie ed alle politiche aziendali ed alle leggi vigenti e nell'ottica del miglioramento della qualità, dell'efficacia e dell'economicità dell'azione aziendale.

8.4. 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.

8.4.1 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

Le eventuali non-conformità rilevate da altri auditor sono portate all'attenzione della Direzione aziendale che stabilisce caso per caso come gestirle, tenendo conto delle indicazioni dell'auditor.

9. ALTRI ASPETTI LEGALI E DI BUSINESS

9.1. TARIFFE

9.1.1 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 del Certificatore.

Per informazioni, scrivere all'indirizzo di posta elettronica: servizifiduciari-cedacri@iongroup.com

9.1.2 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 e vi si accede seguendo le istruzioni dei menù di navigazione.

9.1.3 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 e vi si accede seguendo le istruzioni dei menù di navigazione.

9.1.4 Tariffe per altri servizi

Si veda 9.1.1.

9.1.5 Politiche per il rimborso

I clienti sono obbligati al risarcimento dei danni eventualmente sofferti da Cedacri nei seguenti casi:

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

9.2. RESPONSABILITÀ FINANZIARIA

9.2.1 Copertura assicurativa e Indennizzi

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

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

9.2.2 Altre attività

n/a

9.2.3 Garanzia o copertura assicurativa per I soggetti finali

Si veda il paragrafo 9.2.1.

9.3. CONFIDENZIALITÀ DELLE INFORMAZIONI DI BUSINESS

9.3.1 Ambito di applicazione delle informazioni confidenziali

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

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

n/a

9.3.3 Responsabilità di protezione delle informazioni confidenziali

n/a

9.4. PRIVACY

Le informazioni raccolte dal QTSP nell'esercizio delle proprie funzioni vengono inizialmente raccolte su supporti cartacei e successivamente immesse nel sistema informatico dello stesso. Esse sono da considerarsi riservate, fatte salve quelle destinate all'uso pubblico dei Certificati e quindi pubblicate nel Directory Server. 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.

9.4.1 Programma sulla 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.

Il sistema è vivo ed è mantenuto costantemente aggiornato; tutte le policies e le procedure aziendali sono disponibili ai dipendenti nella intranet aziendale, unitamente ad una adeguata e periodica erogazione di corsi sulla sicurezza dei dati e delle informazioni.

9.4.2 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.

9.4.3 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.

9.4.4 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.

Infatti 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.

9.4.5 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.

9.4.6 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 al Certificatore.

9.5. PROPRIETÀ INTELLETTUALE

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

Il Soggetto del certificato mantiene tutti gli eventuali diritti sui propri marchi commerciali (brand name), e sul proprio nome di dominio. Relativamente alla proprietà di altri dati ed informazioni si applicano le leggi vigenti.

9.6. 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

9.7. 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 i livelli di servizio indicati al paragrafo 9.14 del Manuale Operativo.

9.8. LIMITAZIONE DI RESPONSABILITÀ

Il Certificatore 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, il Certificatore 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. Il Certificatore, 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.

9.8.1 Termine

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

9.8.2 Risoluzione

Tali aspetti sono dettagliati nel contratto che regola il servizio.

9.8.3 Effetti della risoluzione

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

9.9. Canali di comunicazione ufficiali

Si rimanda ai canali di contatto presenti nel paragrafo 1.5

9.10. Risoluzione delle controversie e gestione dei reclami

Si rimanda alla contrattualistica che regolamenta il servizio per il dettaglio delle modalità di risoluzione delle controversie.

Cedacri ha messo in atto un processo di gestione degli eventuali reclami che dovessero pervenire via email a serviziﬁduciari-cedacri@iongroup.com garantendo un tempo di presa in carico della richiesta di al massimo 7 gg solari. La gestione interna prevede un sistema di trouble ticketing tracciato e strutturato che permette l'eventuale escalation del ticket alle strutture specialistiche competenti.

9.11. 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.

9.12. Legge applicabile

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

Ecco alcune delle principali leggi in vigore al momento della pubblicazione del presente manuale:

1. Regolamento UE N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (referenziato anche come Regolamento eIDAS)
2. Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale
3. Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001)
4. Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003) – Codice Privacy ess.mm.ii
5. DPCM 22 febbraio 2013 (GU n.117 del 21-5-2013) - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e71.
6. D.Lgs. 21 novembre 2007, n. 231 "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" ess.mm.ii
7. Decreto Legislativo 6 settembre 2005,n.206ess.mm.ii-CodicedelConsumo

8. Provvedimento Garante per la protezione dei dati personali 26 marzo 2003[1053753]
9. Deliberazione CNIPA n. 45 del 21 maggio 2009, come modificata dalle determine successive
10. Regolamento UE Generale sulla Protezione dei Dati 2016/679 in materia di trattamento dei dati personali e di privacy (GDPR)
11. D. lgs 101/2018 “Disposizioni per l’adeguamento della Normativa Nazionale alle Disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”

Si applicano inoltre tutte le circolari e le deliberazioni dell’Autorità di Vigilanza8, nonché gli atti di esecuzione previsti dal Regolamento eIDAS

9.13. Disposizioni varie

Si rimanda alla contrattualistica che regolamenta il servizio per ogni altra disposizione non compresa nel presente Manuale.

9.14. ALTRE DISPOSIZIONI

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 15:00 - 19:00
Sospensione del Certificato qualificato	7 giorni su 7	24 ore su 24
Revoca del Certificato qualificato	7 giorni su 7	24 ore su 24

10. APPENDICE

10.1. ASN1 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)
891001467680908246696812084556822785855283030736394072037921073770813…
          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…
```

10.2. ASN1 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)
1000101100001000010100011010101100011001100111000100011100110100110011…
```

10.3. VALORI 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

La richiesta OCSP contiene i seguenti campi:

	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

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]