L'ENERGIA CHE TI ASCOLTA.

Information and Communication Technology
Security

CERTIFICATION PRACTICE STATEMENT

CERTIFICATI DIGITALI EROGATI DALLA CA ENEL

PROCEDURA AZIENDALE

Redatto da:	Fistetto Silvio, Gay Massimo, Iorillo Angelo	30/05/2008
Verificato da:	Rao Giuseppe	30/05/2008
Approvato da:	Ceccarelli Francesco	30/05/2008

SOMMARIO

Il presente documento costituisce il *Certification Practice Stament* (CPS) associato alla *Certificate Policy* (CP), identificata dal codice documento *PolicyPKI-CB-2.0*, della *CA Enel*.

LISTA DI DISTRIBUZIONE

Il documento è pubblicato e liberamente consultabile all'indirizzo [5].

MODIFICHE AL DOCUMENTO

Le modifiche riportate nella tabella seguente sono riferite alla versione precedente del documento.

DESCRIZIONE CAMBIAMENTI	RIFERIMENTO
Prima versione	CPSPKI-CB1.0
Seconda versione: • Adeguamento alle nuove Policy e Procedure generali Aziendali • Adeguamento ai nuovi servizi di certificazione, quali l'inserimento dei nuovi Certificati di Autenticazione Roaming e l'eliminazione dei Certificati di Marcatura Temporale • Adeguamento ai nuovi servizi Infrastrutturali ICT, quali l'Infrastruttura di Disaster Recovery Minor issuee: • Adeguamento conservazione LOG e accesso fisico	CPSPKI-CB2.0 CPSPKI-CB2.1

RIFERIMENTI BIBLIOGRAFICI

[1] Certificate Policy PKI - Certificati Digitali Erogati dalla CA Enel

[2] Gestione delle Abilitazioni al Sistema Informativo Aziendale - Processi e Procedure n. 74 – Circolare n. 147 del 7 giugno 2006

[3] Accesso ai Sistemi Informatici Enel

[4] Security Policy

URL DI RIFERIMENTO

[5] ***https://sar.enel/doc/cp/***

[6] ***https://autora6.enelit.it/***

GRUPPO DI LAVORO

Alla realizzazione di questo documento hanno partecipato le seguenti persone:

NOME	UNITÀ ORGANIZZATIVA
• **CECCARELLI FRANCESCO**	Corporate / Sede Corporate / Pers.Org.Serv. / Sicurezza ICT
• **FISTETTO SILVIO**	Enel Servizi / Information & Communication Technology Operations Sistemi e TLC / Sicurezza IT / Operation Security
• **GAY MASSIMO**	Corporate / Sede Corporate / Pers.Org.Serv. / Sicurezza ICT
• **IORILLO ANGELO**	Enel Servizi / Information & Communication Technology Operations Sistemi e TLC / Sicurezza IT / Design & implementation
• **RAO GIUSEPPE**	Enel Servizi / Information & Communication Technology Operations Sistemi e TLC / Sicurezza IT

INDICE

DEFINIZIONI

TERMINE O ACRONIMO	SIGNIFICATO
ACRN	La coppia di codici ("Authentication Code" e "Reference Number") utilizzati dal prodotto Entrust, in conformità con l'RFC2510, per autenticare l'utente che chiede la certificazione della chiave pubblica. Si tratta di codici generati in modo casuale da Entrust/Authority e correlati tra loro che, oltre ad autenticare l'utente, proteggono da intrusioni e alterazioni indebite il canale di comunicazione tra utente e Entrust/Authority. Essi vengono utilizzati solo in fase di certificazione e poi vengono cancellati da Entrust/Authority, evitando replay attack.
Certificate Policy (CP)	L' insieme di regole, contraddistinto da un codice, che indica se è possibile utilizzare determinati certificati nell'ambito di specifiche comunità o classi di applicazioni aventi comuni esigenze di sicurezza.
Certification Authority (CA)	L'entità che esegue il processo di certificazione, rilascia il certificato della chiave pubblica, lo rende disponibile insieme a quest'ultima e gestisce le liste di revoca (CRL).
Certification Practice Statement (CPS)	Il documento relativo alle regole pratiche utilizzate dalle diverse entità in una infrastruttura PKI. Vi sono descritti gli strumenti, le regole e le procedure implementate dalla CA per soddisfare quanto definito nel documento CP per emettere e gestire i certificati.
Certificato	Il risultato di un processo mediante il quale la chiave pubblica del titolare ed altre informazioni vengono associate univocamente al titolare della chiave privata, l'autenticità e l'integrità di tale associazione vengono assicurate tramite la firma digitale da parte della CA.
Challenge/Response	La coppia di parola d'ordine/controparola, scelta dall'utente stesso al momento della certificazione, utilizzata in caso di richieste di revoca o di recovery da parte del titolare effettuate per telefono.
Chiave Privata	L'elemento della coppia di chiavi destinato ad essere utilizzato e conosciuto dal solo soggetto titolare.
Chiave Pubblica	L'elemento della coppia di chiavi destinato ad essere reso pubblico.
Chiavi di Certificazione	Le chiavi utilizzate dalla CA ai fini della generazione e verifica delle firme apposte ai certificati e alle liste di revoca (CRL).
Chiavi di Cifratura	La coppia di chiavi utilizzate dall'operazione di cifratura per rendere segrete delle informazioni.
Chiavi di Marcatura Temporale	Le chiavi destinate alla generazione e verifica delle marche temporali.
Chiavi di Sottoscrizione	La coppia di chiavi destinate alla generazione ed alla verifica di firme digitali.

TERMINE O ACRONIMO	SIGNIFICATO
Codici Segreti	I codici riservati concordati tra utente e CA per stabilire un'identificazione sicura dell'utente all'atto della sua certificazione tramite AutoRA. Normalmente si utilizzano codici prelevati dai data base di applicazioni preesistenti.
Coppia di Chiavi	L'insieme costituito dalla chiave pubblica e dalla chiave privata ad essa associata.
Cross Certification **(Accordo di Mutua Certificazione)**	L'accordo mediante il quale la CA qui definita e un'altra CA assicurano il mutuo riconoscimento dei certificati rispettivamente emessi e delle policy che le governano. La cross certification si concretizza nella emissione del certificato della chiave pubblica di ciascuna delle due CA da parte dell'altra e, ove applicabile, dalla definizione della corrispondenza tra le rispettive policy.
Entità	Un elemento autonomo all'interno di una infrastruttura PKI. Un'entità non è necessariamente un individuo ma potrebbe essere un elaboratore o un applicazione. Per esempio una CA, una RA ed una singola persona sono delle entità.
Registration Authority (RA)	L'entità responsabile …. Non firma o emette certificati.
Marca Temporale	Il risultato di una procedura informatica con cui si attribuiscono ad uno o più documenti informatici una data ed un orario opponibili ai terzi.
Object Identifier (OID)	Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
Operazione di Cifratura	Il processo di trasformazione di dati in un formato che garantisca la riservatezza dei dati stessi. Tale operazione prevede l'utilizzo delle chiavi pubbliche dei soggetti a cui sono destinate le informazioni.
Operazione di Decifratura	Il processo di trasformazione inverso a quello di cifratura. Tale operazione prevede l'utilizzo della chiave privata da parte del titolare che intende decifrare il messaggio.
Passphrase	La password che risponde alle caratteristiche indicate in "Accesso ai Sistemi Informatici".
Profilo Utente	L'insieme delle informazioni crittografiche del titolare, tra cui, principalmente: chiavi private di firma e cifratura, certificati di firma e cifratura, autocertificato della CA.
Public Key Infrastructure (PKI)	L'insieme di hardware, software, persone, processi e regole che consentono di creare, gestire, conservare, distribuire e revocare i certificati, garantendo l'associazione tra le chiavi pubbliche ed i titolari. Sono previsti i seguenti impieghi per i certificati: riconoscimento sicuro delle entità (authentication), cifratura, firma digitale e marcatura temporale.

TERMINE O ACRONIMO	SIGNIFICATO
Referente alle Abilitazioni	La figura designata dall'organizzazione aziendale che ha la possibilità di autorizzare l'emissione dei certificati per i titolari a lui afferenti e richiederne la revoca. Ogni titolare afferisce ad uno o più responsabili, ogni Referente alle Abilitazioni può afferire a più titolari.
Security Policy (SP)	L'insieme delle regole e norme che definiscono e regolamentano le misure di sicurezza con cui un sistema o un'organizzazione protegge le proprie risorse critiche o riservate. Si considerano normalmente tre livelli di Security Policy
Sistema di Validazione Temporale **(Time Stamp Server – TSS)**	Il sistema in grado di produrre marche Temporali.
Timestamp Server Agent (TSA)	L'addetto della CA incaricato di gestire il TSS.
Titolare	L'entità per la quale è stato emesso un certificato, da parte della CA, contenente la sua chiave pubblica. E' responsabile dell'utilizzo della chiave privata corrispondente alla chiave pubblica.

ABBREVIAZIONI

ABBREVIAZIONE	DEFINIZIONE	RIFERIMENTO
ASN.1	Abstract Syntax Notation. Metodologia utilizzata per descrivere informazioni utilizzate in altri standard	CCITT, Recommendation X.208, "Specification of Abstract Syntax Notation One (ASN.1)"
CAST-128	Algoritmo di cifratura	RFC2144
CP/CPS	Certificate Policy / Certification Practice Statement	RFC3647 (sostituisce RFC2527)
Crittografia	Lo studio delle tecniche per mantenere sicure le informazioni. Due comuni applicazioni sono la cifratura e la firma digitale	
DES	Data Encryption Standard, è un algoritmo di cifratura.	American National Standards Institute, ANSI X3.106, "American National Standard for Information Systems - Data Link Encryption"
Diffie-Hellman	Algoritmo di cifratura a chiave pubblica	
DSS	Digital Signature Standard. Algoritmo di cifratura utilizzato per le firme digitali, è menzionato anche come DSA (Digital Signature Algorithm).	National Institute of Standards and Technology, FIPS Pub 186: Digital Signature Standard.
IESG	Internet Engineering Steering Group. Il gruppo che sovrintende a IETF e determina quali proposte diventano standard.	http://www.ietf.org/iesg.html
IETF	Internet Engineering Task Force. La principale organizzazione che crea standard per Internet	http://www.ietf.org/
LDAP	Lightweight Directory Access Protocol. Protocollo di accesso alle directory X.500	RFC4511 (sostituisce RFC2251)
PKI	Public Key Infrastructure.	
PKIX	Internet X.509 Public Key Infrastructure. Il nome del gruppo di lavoro IETF che crea standard per la PKI in Internet.	http://www.imc.org/ietf-pkix/
PUK	Pin Unblocking Key	
RFC	Request For Comments. Il metodo utilizzato da IETF per pubblicare documenti	
RFC1006	ISO Transport Service on top of the TCP Version: 3	

ABBREVIAZIONE	DEFINIZIONE	RIFERIMENTO
RFC3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	
RFC3447	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1	
RFC3647 (sostituisce RFC2527)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	
RFC4210 (sostituisce RFC2510)	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) Standard PKIX Certificate Managament Protocol	
RFC4248 (sostituisce RFC1378)	The telnet URI Scheme	
RFC4266 Sostituisce (RFC1378)	The gopher URI Scheme	
RFC4346	The Transport Layer Security (TLS) Protocol Version 1.1	
RFC4511	Lightweight Directory Access Protocol (LDAP): The Protocol	
RSA	Rivest-Shamir-Adelman. Nome di un algoritmo di cifratura a chiave pubblica. E' anche il nome della società che controlla i diritti di utilizzo dell'algoritmo	RFC3447 (sostituisce RFC2313)
SSL	Secure Sockets Layer. Protocollo di cifratura e d autenticazione per le connessioni Internet	
TBD	To be defined	
TLS	Transport Layer Security. La versione standard di SSL	RFC4346 (sostituisce RFC2246)
URI	Uniform Resource Identifier	RFC4248 e RFC4266
URL	Uniform Resource Locator	RFC4248 e RFC4266
URN	Uniform Resource Name. Utilizzato come identificatore di risorsa indipendentemente dalla sua locazione.	RFC2141

ABBREVIAZIONE	DEFINIZIONE	RIFERIMENTO
WG	Working Group. Usually used with reference to the IETF.	
X.400	Specifiche per client di posta e relativi server.	RFC1006
X.500	Specifiche per server di directory e modalità di accesso alle stesse	ITU-T Recommendation X.500 (1997), ISO/IEC 9594-1:1997, Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services
X.509	Specifiche per il formato dei certificati digitali.	RFC3280
X9.42	Specifiche per l'utilizzo dell'algoritmo Diffie-Hellman algorithms.	American National Standards Institute, "Agreement Of Symmetric Keys Using Diffie-Hellman and MQV Algorithms", ANSI 2003.

1. INTRODUZIONE

1.1. Generalità

Un *Certificato Digitale* associa una chiave pubblica di crittografia ad un insieme d'informazioni che identificano un'entità (individuo o dispositivo). Tale entità, il *Titolare* del certificato, possiede ed utilizza la corrispondente chiave privata. Altre entità, gli *Utenti*, identificano il *Titolare* verificando, tramite la chiave pubblica contenuta nel certificato, la corrispondenza con la chiave privata.

Gli *Utenti* fanno pertanto affidamento sul processo di certificazione della chiave pubblica della *CA* che svolge il ruolo di *terza parte fidata*.

Questo documento, impostato sulla base delle linee guida del RFC2527, rappresenta il *Certification Policy Statemet* (CPS) della *CA Enel*, ovvero specifica le procedure seguite dall'ente di certificazione Enel per la fornitura di servizi di certificazione, ivi inclusi rilascio, gestione, revoca e rinnovo di certificati.

Tali procedure sono conformi ai requisiti generali specificati nella corrispondente Certificate Policy (CP), identificata dal codice documento PolicyPKI-CB2.0, che è pubblicata e liberamente consultabile all'indirizzo [5].

La *CA Enel* è rappresentata dalla Funzione *Corporate / Sede Corporate / Pers.Org.Serv. / Sicurezza ICT*, che costituisce il diretto responsabile di questa *CPS*.

I servizi erogati dalla *CA Enel* sono sotto la responsabilità dalla Funzione *Enel Servizi / Information & Communication Technology / Operations Sistemi e TLC / Sicurezza IT*.

I certificati erogati e gestiti dalla *CA Enel* sono dei seguenti tipi:

- **CERTIFICATI DI SOTTOSCRIZIONE** – Da utilizzare per le operazioni di Firma Elettronica Avanzata (Decreto Legislativo 23 gennaio 2002, n. 10, art. 2, non sono idonei alla Firma Qualificata) ed Autenticazione; prevedono il salvataggio delle credenziali del titolare sulla postazione di lavoro del titolare stesso.
- **CERTIFICATI SOTTOSCRIZIONE FORTE** – Da utilizzare per le operazioni di Firma Elettronica Avanzata (Decreto Legislativo 23 gennaio 2002, n. 10, art. 2, non sono idonei alla Firma Qualificata) ed Autenticazione; essi prevedono il salvataggio delle credenziali del titolare sulla smart card del titolare stesso.
- **CERTIFICATI DI CIFRATURA** – Assegnati al titolare congiuntamente ai certificati di sottoscrizione.
- **CERTIFICATI DI AUTENTICAZIONE ROAMING** – Normalmente assegnati al titolare alternativamente ai certificati di sottoscrizione.

1.2. Identificazione

1.2.1. Identificatore alfanumerico

Questo CPS è identificato dal codice documento *PolicyPKI-CB2.0* ed pubblicato e liberamente consultabile all'indirizzo [5].

1.2.2. Identificatore Oggetto

Questo CPS non è stato registrato presso organismi preposti alla sua assegnazione nell'ambito degli standard internazionali ISO, e non dispone, pertanto, di un OID (Object Identifier) d'identificazione univoco certo.

1.3. Entità e Applicabilità

Il presente *CPS* si applica alle medesime entità indicate all'analogo capitolo della CP e i cui ruoli sono ivi definiti, per definire le procedure da seguire nell'emissione, gestione e utilizzo dei certificati e nell'utilizzo delle applicazioni indicate al punto1.3.6.

Le entità in questione sono vincolate al rispetto delle procedure riportate in questa *CPS*.

1.3.1. Certification Authority (CA)

La *CA* deve:

- Generare per tutte le entità la coppia di chiavi asimmetriche che esse utilizzeranno per scopi di cifra;
- Trasmettere in maniera sicura a ciascuna entità la corrispondente chiave privata di cifra;
- Conservare in modo sicuro una copia delle chiavi private di cifratura a scopo di recovery;
- Emettere i certificati di sottoscrizione forte e di cifratura per le entità di RA;
- Emettere i certificati previsti per le altre entità autorizzate, nel rispetto delle norme riportate nella CP e nel CPS;
- Emettere e gestire le liste dei certificati revocati (CRL) secondo le norme riportate nella CP e nel CPS;
- Pubblicare sulla directory i certificati di cifratura e le CRL, con le modalità previste nella CP e nel CPS;
- Effettuare il recovery delle chiavi di cifra, anche di quelle di cui sia scaduto il certificato (key history) ed effettuare il recovery dei profili utente;
- Gestire in sicurezza la rete ove sono installati i sistemi su cui opera, i sistemi stessi e gli altri dispositivi tramite i quali esercita le proprie funzioni;
- Assicurare la continuità di servizio prevista per il sistema di emissione dei certificati e per la directory.

1.3.2. Registration Authority (RA)

La RA è l'entità delegata dalla CA a gestire la relazione con le seguenti entità:

- *Referenti alle Abilitazioni*
- *Titolari*

La RA è tenuta a verificare l'identità delle entità che a lei si rivolgono, siano essi titolari (attuali o potenziali) di certificati o responsabili di certificati relativi a applicazioni/device.

La RA che, normalmente, non svolge un ruolo nei flussi informatici di generazione e gestione di certificati, può essere coinvolta in casi particolari d'emergenza, come quelli d'indisponibilità degli strumenti informatici previsti.

La RA, previa verifica di merito, provvede ad inoltrare alla CA:

- I dati dei futuri titolari dei certificati di sottoscrizione e di cifratura
- Eventuali richieste di revoca
- Eventuali richieste di recovery di chiave di cifratura e di profilo utente.

1.3.3. Titolari

Il titolare è l'entità cui è intestato un certificato.

I titolari sono responsabili delle chiavi loro assegnate, dei loro certificati e dell'utilizzo che ne fanno.

Ogni titolare può afferire a più certificati, ogni certificato può afferire univocamente ad un titolare.

I titolari si suddividono nelle seguenti tipologie:

- Titolari interni: titolari che appartengono alle società del gruppo *Enel*;
- Titolari esterni: titolari che non appartengono alle società del gruppo; possono far parte di questa tipologia i fornitori e i clienti *Enel*, e, più in generale, tutti coloro che hanno la necessità di accedere a servizi particolari erogati da *Enel*.

I titolari possono:

- Richiedere l'emissione dei certificati per il tramite del proprio Referente alle Abilitazioni;
- Richiedere la revoca dei propri certificati e di quelli relativi ai dispositivi hardware e software di cui sono eventualmente responsabili;
- Richiedere il recovery della propria chiave privata di cifratura e del proprio profilo utente e di quelli relativi ai dispositivi HW e SW di cui sono direttamente responsabili.

1.3.4. Referente alle Abilitazioni

Sia per i titolari interni che per i titolari esterni sono previste le figure di *Referente alle Abilitazioni*.

Il Referente alle Abilitazioni deve:

- Autorizzare la CA all'emissione di certificati per i titolari di sua competenza.

Il Referente alle Abilitazioni può:

- Richiedere la revoca dei certificati per i titolari di sua competenza;
- Richiedere e attivare la procedura di recovery delle chiavi di cifratura e del profilo utente per i titolari di sua competenza, come specificato nel par. 3.3.2.

1.3.5. Titolari di Certificati Erogati da Altre CA

Rientrano in questa tipologia i titolari di certificati erogati da CA in cross-certification con la *CA Enel*. Questi titolari sono soggetti ai diritti e ai doveri concordati tra le due CA.

Al momento, la *CA Enel* non è in cross-certification con altre CA.

L'eventuale futuro utilizzo di cross-certification sarà specificatamente trattato nell'ambito di questo CPS, attraverso la pubblicazione di una sua nuova edizione.

1.3.6. Applicabilità

Al presente CPS si applica quanto indicato al medesimo capitolo delle CP.

1.4. Riferimenti

1.4.1. Organizzazione

Le procedure qui definite sono a cura della Funzione *Corporate / Sede Corporate / Pers.Org.Serv. / Sicurezza ICT*, che costituisce il diretto responsabile di questa *CPS*.

I servizi erogati dalla *CA Enel* sono sotto la responsabilità dalla Funzione *Enel Servizi / Information & Communication Technology / Operations Sistemi e TLC / Sicurezza IT*.

1.4.2. Persone

Le persone responsabili per la gestione, l'aggiornamento e l'interpretazione del presente documento sono le seguenti:

- Responsabile della Funzione *Corporate / Sede Corporate / Pers.Org.Serv. / Sicurezza ICT*, come da organigramma aziendale, nel ruolo di *Approvatore*;
- Responsabile della Funzione *Enel Servizi / Information & Communication Technology / Operations Sistemi e TLC / Sicurezza IT*, come da organigramma aziendale, nel ruolo di *Verificatore*.

2. CONDIZIONI GENERALI

Questa sezione contiene le informazioni di dettaglio relative agli obblighi e alle responsabilità della CA, della RA, delle CA in cross-certification, dei titolari e degli utenti.

2.1. Obblighi

Questa sezione contiene le informazioni di dettaglio relative agli obblighi della CA, della RA e dei titolari.

2.1.1. Obblighi della CA

La CA opera secondo quanto definito nel presente CPS e nella relativa CP di riferimento.

La CA opera nei confronti dei titolari per il tramite della RA.

2.1.1.1. Informativa agli Utenti

All'indirizzo [5] sono pubblicati e liberamente consultabili questo CPS e la sua relativa CP di riferimento.

Attraverso la loro consultazione è possibile essere dettagliatamente informati relativamente a:

1. Tipologie di certificati disponibili
2. Dati necessari per il rilascio dei certificati
3. Dati personali dell'Utente, pubblicati sulla Directory pubblica
4. Modalità per l'effettuazione della richiesta di certificazione
5. Modalità per l'effettuazione della revoca
6. Modalità per la richiesta di recovery della chiave privata di cifratura e del profilo del titolare.
7. Obblighi e responsabilità inerenti all'attribuzione e l'utilizzo di un certificato
8. Modalità di certificazione cross-certification con altre CA

Il suddetto indirizzo è comunicato al Titolare, via e-mail, durante il processo di attivazione del relativo certificato.

Il Titolare è tenuto a consultare attentamente CP e CPS relativamente alle parti che lo riguardano.

I documenti vengono aggiornati ogni qual volta venga stipulato un nuovo accordo di certificazione cross-certification (cap. 8).

2.1.1.2. Identificazione delle Entità

La CA deve identificare l'entità che richiede il certificato, l'identificazione deve essere effettuata secondo quanto definito al punto 3.1.7.

2.1.1.3. Emissione dei Certificati

La procedura di emissione dei certificati è descritta al capitolo 4.2.

A fronte dell'emissione di un certificato la CA deve:

- Notificare l'avvenuta emissione del certificato al suo Referente alle Abilitazioni, come dettagliato al punto 2.8.1. Tale notifica è di tipo elettronico, via e-mail, per certificati di sottoscrizione e sottoscrizione forte, ed è effettuata tramite procedura di attivazione per i certificati di autenticazione roaming;
- Rilasciare al titolare i suoi certificati e l'autocertificato della CA pubblicare il certificato di cifratura nell'apposita directory.
- Rilasciare l'informativa sul trattamento dei dati personali del Titolare del certificato ai sensi del D.lgs 196/2003.

2.1.1.4. Gestione dei Certificati

La CA deve:

- Gestire il rinnovo di certificati emessi e prossimi alla data di scadenza secondo quanto definito al punto 3.2;
- Gestire il recovery delle chiavi private di cifratura emesse e del profilo utente, secondo quanto definito al punto 3.3.

2.1.1.5. Revoca dei Certificati

A fronte della revoca di un certificato, la CA deve:

- Notificare via e-mail la revoca del certificato al Referente alle Abilitazioni.
- Emettere e gestire le liste di revoca del certificato secondo quanto definito al punto 4.4.6.

2.1.1.6. Obblighi delle CA in Cross -Certification

La *CA Enel* prima di stipulare un accordo di cross-certification con un'altra CA ne verifica l'applicabilità e l'adeguatezza alle proprie politiche di sicurezza. Al riguardo, saranno esaminate, in modo riservato, le Security Policy, la CP e il CPS dell'altra CA.

Analoga verifica, viene autorizzata all'altra CA.

L'accordo di cross-certification prevedere:

- Il rispetto, da parte di ciascuna CA, della CP e del CPS dell'altra;
- Ciascuna CA è tenuta ad informare l'altra, delle modifiche apportate ai propri CP e CPS.

La *CA Enel* deve:

- Aggiornare il CPS riportandovi il nuovo accordo di cross-certification.
- Verificare periodicamente la corretta applicazione dell'accordo da parte dell'altra CA.

2.1.1.7. Altri Adempimenti

Oltre a quanto precedentemente specificato, la CA:

- Custodisce le chiavi private con cui essa firma i certificati in modo che non siano accessibili a persone diverse dal personale autorizzato;
- Gestisce un archivio storico dei certificati emessi e le liste di revoca;
- Custodisce in modo inalterabile i log dei vari sistemi per 10 anni;
- Si attiene ai vincoli legislativi di cui al punto 2.4 del CP corrispondente;
- Emette i certificati on line, come specificato al punto 4.2. Il servizio è disponibile dalle ore 9.00 alle ore 16.00 di ogni giorno lavorativo, garantendone la continuità per il 99,5% del tempo;
- Rende disponibile il servizio di emissione delle liste di revoca (CRL), descritto al punto 4.4, garantendone la continuità per il 99,5% del tempo, salvo eventi particolari al di fuori del suo controllo;
- Rende disponibile 24 ore su 24 l'accesso, mediante il protocollo LDAP v3 definito in RFC 2251, o LDAPv2 definito allo RFC 1777, alla directory ove sono pubblicati i certificati di cifratura e le liste di revoca (CRL), salvo eventi particolari al di fuori del controllo della *CA Enel*;
- Deve assicurare l'aggiornamento del clock di sistema dei dispositivi da lei utilizzati.

2.1.2. Obblighi della RA

La RA opera secondo quanto definito nel presente CPS, nel rispetto della delega ricevuta dalla CA.

Il servizio è disponibile dalle ore 7:00 alle ore 19:00.

2.1.2.1. Identificazione delle Entità

La RA ha l'obbligo di identificare:

- Le entità che le si rivolgono per richiedere il certificato secondo quanto definito al punto 3.1.7;
- Le entità che richiedono il recovery della chiave privata di cifratura e del profilo utente secondo quanto definito al punto 3.3;
- Le entità che richiedono la revoca di un certificato secondo quanto definito al punto 4.4.

2.1.2.2. Revoca dei Certificati

La RA, dopo aver identificato le entità che richiedono la revoca di un certificato, effettua le operazioni di propria competenza descritte di seguito nel par 4.4.

2.1.2.3. Altri Adempimenti

La RA deve:

- Custodire il dispositivo contenente il proprio profilo utente in modo che non sia utilizzabile da altri, proteggendo la passphrase in conformità con quanto disposto nel documento *Accesso ai Sistemi Informatici* [3];
- Assicurare l'aggiornamento del clock di sistema dei dispositivi da lei utilizzati, collegati in NTP con un time server che fornisce l'ora esatta alla rete Enel;
- Notificare l'avvenuta emissione del certificato al suo Referente alle Abilitazioni secondo quanto definito al punto 2.8.1;

- Notificare l'avvenuta recovery della chiave privata di cifratura e del profilo utente al Referente alle Abilitazioni. Tale notifica può essere è di tipo elettronico, secondo quanto definito al punto 2.8.1.

2.1.3. Obblighi dei Referenti alle Abilitazioni

I *Referenti alle Abilitazioni* possono:

- Abilitare i titolari loro afferenti ad ottenere i certificati;
- Richiedere e attivare le procedure di recovery delle chiavi di cifratura e del profilo utente per i propri titolari di loro competenza, come specificato nel par. 3.3.2.

I *Referenti alle Abilitazioni* devono:

- Informare i titolari sugli obblighi e le responsabilità inerenti all'attribuzione di un certificato comunicando ai titolari l'indirizzo URL ove è reperibile la documentazione di cui al punto 2.1.1.1.
- Richiedere la revoca dei certificati relativi ai titolari loro afferenti, come previsto al punto 4.4

2.1.4. Obblighi dei Titolari

Richiedendo un certificato, il titolare accetta di conformarsi al presente CPS e alla CP di riferimento e dichiara di avere fornito informazioni corrette per la sua identificazione e che il certificato sarà utilizzato esclusivamente per fini autorizzati.

I Titolari sono obbligati a:

- Conservare con la massima diligenza le chiavi private ed il dispositivo che le contiene al fine di garantirne l'integrità e la massima riservatezza;
- Conservare la passphrase di abilitazione all'uso delle chiavi private in modo da garantirne la massima riservatezza;
- Richiedere immediatamente la revoca di un certificato qualora la corrispondente chiave privata abbia, anche solo potenzialmente, perso le caratteristiche di riservatezza;
- Utilizzare i certificati per le sole applicazioni permesse dal CPS e dalla CP di riferimento;
- Non utilizzare una chiave privata di firma che si presume sia compromessa;
- Non utilizzare una chiave privata di firma revocata o scaduta;
- Non utilizzare certificati propri o altrui che siano stati revocati;
- Non violare alcuna norma sulla riservatezza delle informazioni personali, sulla proprietà intellettuale ed eventuali disposizioni aziendali sulla riservatezza delle informazioni;
- Distruggere la propria chiave privata di firma qualora non abbiano più titolo a possederla;
- Assicurare l'aggiornamento del clock di sistema dei dispositivi utilizzati.
- Leggere ed accettare l'informativa sul trattamento dei dati personali comunicati, resa disponibile eseguendo il processo di rilascio/emissione del certificato.

I titolari possono:

- Richiedere l'emissione dei certificati alla CA o alla RA, purché autorizzati dal proprio Referente alle Abilitazioni;

- Richiedere il recovery delle chiavi private di cifratura e del proprio profilo utente, ad esempio se è stata dimenticata la passphrase, se il certificato non è revocato né scaduto.

2.1.5. Responsabilità di Altre Entità

La *CA Enel* non è in alcun modo responsabile di alcuna conseguenza derivante dall'uso dei propri certificati da parte di entità certificate da CA terze e da essa non riconosciute mediante accordi specifici di cross-certification.

2.1.6. Responsabilità di Verifica di un Certificato

Chiunque utilizzi un certificato, sia esso stato emesso dalla *CA Enel* o da altra CA con essa cross-certified, è direttamente responsabile delle seguenti verifiche:

- Verifica della validità, oltre che della scadenza, anche accedendo all'ultima CRL emessa dalla rispettiva CA. Solo per i titolari di certificati di sottoscrizione forte non è previsto il caching delle CRL;
- Verificare che il certificato, emesso dalla *CA Enel* o da altra CA con essa cross certified, sia utilizzato per gli scopi ammessi dalla CP di Enel o della CA cross certified, purché quest'ultima CP sia considerata equivalente alla CP di Enel;
- Qualora il certificato sia stato emesso da una CA diversa dalla CA di Enel, verificare se con tale CA esiste un accordo di mutua certificazione (par. 2.1.1.1). Nel caso che tale accordo non esista, la *CA Enel* non è in alcun modo responsabile delle conseguenze derivanti dall'uso di detto certificato.

La *CA Enel* declina ogni responsabilità in merito alle conseguenze derivanti dalla mancata verifica di un certificato.

2.2. Garanzie e Limitazioni di Responsabilità

2.2.1. Responsabilità della CA

2.2.1.1. Garanzie

La CA garantisce che:

- I servizi di certificazione ed i servizi di repository sono conformi al presente documento CPS;
- L'emissione dei certificati viene effettuata in accordo con il presente documento CPS;
- La revoca dei certificati emessi viene effettuata in accordo con il presente documento CPS;
- La gestione delle liste di revoca viene effettuata in accordo con il presente documento CPS;
- L'effettuazione del servizio di recovery della chiave privata di cifratura e del profilo utente viene effettuata in accordo con il presente documento CPS;
- Opererà nel rispetto delle norme contenute in questo documento CPS con la dovuta diligenza e competenza, nell'ambito delle mansioni attribuitele dalla direzione aziendale;
- Il trattamento dei dati personali degli utenti avverrà nel rispetto di quanto definito dal D.lgs 196/2003, Codice in materia di dati personali.

- I documenti CP e CPS verranno aggiornati annualmente e comunque ogni qualvolta si renda necessario.

2.2.1.2. Limitazioni

Al presente CPS si applicano le medesime limitazioni di responsabilità indicate all'analogo punto delle CP.

2.2.2. Responsabilità della RA

2.2.2.1. Garanzie

La RA garantisce di attenersi al processo di identificazione delle entità definito al punto 3.1.7 di questo documento CPS e a quanto definito nelle CP.

2.2.2.2. Limitazioni

Al presente CPS si applicano le medesime limitazioni di responsabilità indicate all'analogo punto delle CP.

2.3. Responsabilità Finanziaria

Al presente punto del documento CPS si applica quanto specificato all'analogo punto del documento CP relativo.

2.4. Interpretazione e Competenze Legislative

Al presente punto del documento CPS si applica quanto specificato all'analogo punto del documento CP relativo.

2.5. Tariffe

Al presente punto del documento CPS si applica quanto specificato all'analogo punto del documento CP relativo.

2.6. Pubblicazione e repository

2.6.1. Pubblicazione di informazioni

Il documento CP e il documento CPS sono liberamente reperibili in formato pdf all'indirizzo [5].

L'aggiornamento di questi documenti avverrà secondo le modalità descritte al capitolo 8 di ciascuno di essi.

I certificati di cifratura e le CRL emesse sono reperibili nella directory X.500, accessibile mediante i protocolli LDAPv2 e LDAPv3.

La DE 1999/93, Allegato II, punto l, terzo capoverso, prevede che i certificati di firma possano essere accessibili alla consultazione del pubblico solo nei casi in cui si abbia il consenso del titolare. Inoltre la pubblicazione dei certificati di firma non aggiunge nulla alla funzionalità della PKI, in quanto a ciascun documento firmato è allegato il corrispondente certificato.

In considerazione di quanto sopra i certificati di sottoscrizione e di sottoscrizione forte non sono pubblicati nella directory differenza dei certificati di cifratura.

2.6.1.1. Distribution Point delle CRL

Allo scopo di ottimizzare il traffico sulla rete e di ridurre i tempi di elaborazione, è prevista la ripartizione dei certificati tra diverse CRL, in tal modo ogni certificato fa capo ad una CRL "settoriale", di dimensioni limitate e quindi di più agevole accesso.

Nei certificati è di conseguenza valorizzata l'EXTENSION cRLDistributionPoints.

2.6.2. Frequenza di Aggiornamento delle Informazioni Pubblicate

I certificati di cifratura sono normalmente pubblicati contestualmente con la loro emissione. Eventuali situazioni di emergenza possono ritardarne la pubblicazione che avrà luogo nel più breve tempo possibile.

Le liste di revoca sono pubblicate ogni dodici ore.

Versioni aggiornate del documento CP e del documento CPS vengono rilasciate nel più breve tempo possibile, nel rispetto della procedura indicata al capitolo 8.

2.6.3. Controllo di accesso

Non è richiesto alcun controllo sugli accessi al documento CP né al documento CPS.

2.7. Verifiche di conformità alle Policy Aziendali

E' previsto il controllo di conformità alle norme indicate nel presente CPS e nelle relative Security Policy [4] della prassi realmente seguita dalle entità: CA, RA, responsabili, titolari di certificati, CA cross-certified.

2.7.1. Conformità alle Policy Aziendali

2.7.1.1. Conformità della CA

2.7.1.1.1. Frequenza

La frequenza delle verifiche dei processi seguiti dalla CA è indicata nelle CP di riferimento.

Ulteriori dettagli sulle condizioni a seguito delle quali possono essere attivate ispezioni di audit non pianificate sono descritte nelle Security Policy. In linea di massima tali ispezioni saranno indette ove

sussistano concreti sospetti di inadempienza o dopo che se ne sia riscontrata una grave in precedenza. Nelle Security Policy vengono specificate in dettaglio le norme attuative di questa ultima casistica.

Ispezioni di audit da parte di CA cross certified potranno essere fatte, per reciprocità, secondo quanto definito al punto 2.7.1.3.2.

2.7.1.1.2. Processi Soggetti a Controllo

Le ispezioni di audit saranno svolte su tutte le procedure contemplate nel presente documento CPS e su quanto disposto dalle Security Policy. Sono comunque previste ispezioni di controllo almeno per i seguenti elementi di questo CPS a cui si fa riferimento nei punti indicati tra parentesi:

- Identificazione ed autenticazione del personale di gestione (3.1.7.1)
- Competenza del personale rispetto alle mansioni che ricopre (5.4)
- Ripartizione dei compiti (5.2.1.1).
- Presenza del numero minimo di persone per attivare le funzioni critiche (5.2.2).
- Procedure di sicurezza dei sistemi della CA e della directory (6.4).
- Disaster recovery e gestione dell'emergenza (4.8).
- Sicurezza ambientale, procedurale e sul personale (5)
- Sicurezza tecnica (6)
- Profili dei certificati e delle liste di revoca (7)
- Amministrazione delle policy (8)

2.7.1.1.3. Azioni da intraprendere in caso di inadempienza

I risultati di azioni di verifica e controllo sono sottoposti all'attenzione di Enel.

In base alle irregolarità riscontrate ed al loro impatto sulla infrastruttura PKI è possibile:

- L'ente che ha rilevato le infrazioni, sentito il parere del responsabile della PKI e delle persone che espletano le funzioni indicate al punto 5.2.1.1, definirà le azioni correttive che la CA deve intraprendere entro un periodo di tempo convenuto tra la funzione di audit e la PKI.
- Revocare eventuali certificati emessi dalla CA.

  Questa è una condizione estrema e in ogni caso sarà il responsabile della CA a valutare se il risultato dell'audit comporti la necessità di effettuare questo tipo di intervento. Egli darà allora disposizione ai responsabili della CA di revocare i certificati.

  Qualora in fase di audit si verificasse l'esistenza di condizioni atte a causare la compromissione della chiave privata della CA, ne sarà revocato il relativo certificato, con la procedura indicata al punto 4.8.1.

2.7.1.2. Conformità della RA

2.7.1.2.1. Frequenza

La frequenza delle verifiche dei processi seguiti dalle RA è indicata nelle CP di riferimento.

Ulteriori dettagli sulle condizioni a seguito delle quali possono essere attivate ispezioni di audit non pianificate sono descritte nelle Security Policy.

2.7.1.2.2. Processi Soggetti a Controllo

Le azioni di controllo sono effettuate su:

- Identificazione ed autenticazione dei titolari (3)
- Requisiti gestionali (da 4.1 a 4.6)
- Sicurezza ambientale, procedurale e sul personale (5)
- Sicurezza tecnica (6)
- Profilo dei certificati (7.1)

2.7.1.2.3. Azioni da Intraprendere in Caso di Inadempienza

I risultati delle verifiche e dei controlli effettuati sono sottoposti all'attenzione del responsabile della sicurezza della CA il quale è responsabile di stabilire le eventuali azioni correttive.

In taluni casi, a giudizio del responsabile della sicurezza, potrà essere prevista la revoca dei certificati emessi. In tal caso egli darà disposizione ai *Referenti alle Abilitazioni* dei titolari interessati a richiedere le relative revoche.

2.7.1.3. Conformità delle Altre Entità

2.7.1.3.1. Titolari e Referenti alle Abilitazioni

In linea generale per i titolari è possibile verificare:

- Il rispetto della segretezza dei codici di abilitazione iniziale alla certificazione
- La modalità di custodia per:
  - Il proprio profilo
  - La smart card (ove applicabile)
  - La passphrase di sblocco
- Se la firma sia apposta con finalità estranee all'ambito definito al punto 1.1 del documento CP.

Per i *Referenti alle Abilitazioni* oltre a quanto già esposto per i titolari è possibile verificare:

- Il rispetto delle norme di autorizzazione dei titolari
- La tempestività nella richiesta di revoca dei certificati come previsto al punto 4.4.

2.7.1.3.2. CA Cross Certified

Le CA con cui esistano accordi di mutua certificazione potranno essere soggette ad ispezioni da parte di auditor della *CA Enel* o terzi effettuate in conformità degli accordi medesimi. Analoga ispezione, per reciprocità, potrà essere fatta sulla *CA Enel*.

2.7.2. Identità e Qualifica dei Controllori

Le figure delle azioni di verifica e controllo effettuate sulle entità hanno una significativa esperienza nell'ambito delle tecnologie utilizzate dall'infrastruttura PKI e sui processi di cifratura.

2.7.3. Relazioni tra i Controllori e l'Infrastruttura PKI

Si veda l'analogo punto delle CP di riferimento.

2.7.4. Comunicazione dei risultati

I risultati delle azioni di verifica e di controllo saranno comunicati al responsabile della PKI e al responsabile della sicurezza e saranno considerati riservati e gestiti secondo quanto definito al punto 2.8.

2.8. Policy di Riservatezza

Tutte le informazioni raccolte, generate, trasmesse e gestite dall'infrastruttura PKI all'interno della quale opera la CA sono considerate riservate e trattate secondo quanto definito alla relativa CP.

2.8.1. Comunicazione ai Responsabili

Alle figure *Referenti alle Abilitazioni* dei titolari vengono comunicate le seguenti informazioni:

1. Notifica di emissione di certificati per i titolari loro afferenti
2. Notifica di recovery della chiave privata di cifratura e del profilo utente per i titolari loro afferenti a seguito della perdita della passphrase
3. Notifica di revoca dei certificati per i titolari loro afferenti

La comunicazione viene normalmente effettuata in forma elettronica.

La notifica via e-mail è sempre cifrata per il destinatario e firmata dalla funzione RA operante.

2.8.2. Comunicazione di Informazioni ad Organi Ufficiali

Informazioni di tipo riservato possono essere comunicate ad organi ufficiali che ne facciano richiesta secondo le modalità previste dalla legge.

2.9. Copyright e Leggi sulla Proprietà Intellettuale

I certificati, il documento CP, il documento CPS, ecc. sono di proprietà della società Enel Spa.

3. IDENTIFICAZIONE E AUTENTICAZIONE

Vengono qui specificate le procedure utilizzate dalla CA e dalla RA per l'identificazione e l'autenticazione delle entità che:

- Sono coinvolte nel processo di emissione dei certificati
- Sono coinvolte nel processo di rinnovo dei certificati
- Richiedono la revoca dei certificati
- Richiedono il recovery dei certificati e del profilo utente

3.1. Registrazione iniziale

3.1.1. Nomi assegnabili

Il campo *subject prt*, per tutte le tipologie dei certificati emessi dalla *CA Enel*, è sempre valorizzato e costituito dai seguenti elementi:

- S/N, serial number
- CN, common name
- OU, organizational unit
- O, organization
- C, country name

Valorizzati nel seguente modo:

S/N

- Nel caso il titolare fosse una persona fisica viene utilizzato il codice fiscale, più un progressivo numerico che identifica il certificato
- Nel caso il titolare fosse un dispositivo non è richiesto

CN

- Nel caso il titolare fosse una persona fisica viene utilizzato il cognome ed il nome (es. Rossi Mario)
- Nel caso il titolare fosse un dispositivo viene utilizzato un identificativo che riconduca al dispositivo stesso (codice applicazione, URL, TSO1 ES, TSO1 SV…)

OU

- Viene utilizzata la società di appartenenza del responsabile a cui il titolare o il dispositivo afferiscono (Enel, Wind, Terna, Fiat S.p.A, QChannel. …)

O

- Viene valorizzato con la stringa "*CA Enel*"

C

- Viene valorizzato con la stringa "it"

Il campo *subject alternative name* deve essere sempre valorizzato mediante le seguenti informazioni:

- indirizzo e-mail secondo quanto definito in RFC 822. Nel caso di certificati dove il titolare è una persona fisica deve essere indicato l'indirizzo e-mail della persona fisica mentre nel caso di dispositivi (computer, applicazioni,…) l'indirizzo e-mail della persona responsabile della richiesta.

3.1.2. Significatività dei nomi

Il nome definito nel campo *subject* ha una ragionevole associazione con il nome del titolare. A fronte di una stessa entità con più certificati il campo *subject* può contenere un codice identificativo in modo da rendere univoco tale campo.

3.1.3. Regole per l'interpretazione dei nomi

Il codice citato al punto 3.1.2 è di almeno tre caratteri e costituito da un numero progressivo (da 000 a 999).

3.1.4. Univocità dei nomi

Il nome del soggetto del certificato non può essere ambiguo ed è univoco per tutti i certificati emessi dall'infrastruttura PKI.

3.1.5. Risoluzione di conflitti sui nomi

La CA si riserva il diritto di prendere decisioni in merito alla risoluzione di conflitti sull'assegnazione dei nomi di comune accordo con il Referente alle Abilitazioni che ha abilitato il titolare a richiedere il certificato.

3.1.6. Prova di possesso della chiave privata

All'atto della certificazione la CA verifica automaticamente che i titolari siano in possesso della chiave privata corrispondente a quella pubblica di cui chiedono la certificazione, conformemente con gli standard RFC 2510 e PKCS#10.

3.1.7. Autenticazione delle entità

3.1.7.1. Autenticazione degli addetti alla CA e alla RA

La struttura degli addetti è di tipo funzionalmente gerarchico, al cui vertice ci sono i Master User, che installano e successivamente personalizzano e attivano il sistema. Essi attivano personalmente la certificazione del primo dei Security Officer che potrà attivare gli altri, i quali a loro volta certificano e autorizzano gli Entrust Administrator. Le RA sono particolari tipi di Entrust Administrator.

Le operazioni svolte direttamente sul sistema CA dai Master User e sulla Directory dai DIT Administrator vengono svolte in presenza di un numero minimo di persone come definito nel capitolo 5.2.2.

Le operazioni svolte vengono memorizzate in modo autonomo a cura degli applicativi della PKI e custodite per un periodo di almeno 10anni.

3.1.7.2. Autenticazione dei titolari

Al fine di associare un certificato all'entità titolare e garantire l'identità di quest'ultima sono previste le seguenti forme di autenticazione, a seconda del tipo di certificato.

Per poter essere certificato dalla *CA Enel* ciascun titolare deve essere stato autorizzato dal proprio Referente alle Abilitazioni.

I *Referenti alle Abilitazioni* sono essi stessi titolari di certificati di sottoscrizione, definiti dalla propria struttura di appartenenza.

Nel caso dei certificati per dispositivi HW o SW, il relativo gestore verrà autorizzato a richiedere i certificati necessari.

3.1.7.2.1. Certificati di sottoscrizione e sottoscrizione forte

Nel caso in cui non fosse coinvolta la RA il titolare deve:

- Essere stato abilitato alla richiesta da parte del suo Referente alle Abilitazioni attraverso l'applicazione della procedura [2];
- Collegarsi alla CA, attraverso applicativo web o client PKI, e successivamente fornire i codici segreti di cui solo lui e la CA sono a conoscenza.

Qualora la RA fosse stata coinvolta, deve:

- Identificare il titolare il quale deve essere stato abilitato alla richiesta da parte del suo Referente alle Abilitazioni mediante [2].
- Assistere il titolare durante il processo di certificazione secondo quanto definito al punto 4.2.2

3.1.7.2.2. Certificati di cifratura

I certificati di cifratura sono rilasciati automaticamente a tutti i titolari di certificati di sottoscrizione e di sottoscrizione forte, per cui non è richiesta un'autenticazione apposita.

3.1.7.2.3. Certificati di autenticazione roaming

Nel caso in cui non fosse coinvolta la RA il titolare deve:

- Essere stato abilitato alla richiesta da parte del suo Referente alle Abilitazioni attraverso l'applicazione della procedura [2];
- Collegarsi alla CA, mediante applicativo Web, e successivamente fornire il codice segreto di cui solo lui e la CA sono a conoscenza.

Qualora la RA fosse stata coinvolta, deve:

- Identificare il titolare il quale deve essere stato abilitato alla richiesta da parte del suo Referente alle Abilitazioni mediante [2].
- Assistere il titolare durante il processo di certificazione secondo quanto definito al punto 4.2.2

3.2. Richiesta di rinnovo dei certificati

La CA è in grado di rinnovare automaticamente chiavi e certificati in accordo con il protocollo di gestione dei certificati (RFC 2510).

Per i titolari abilitati il rinnovo avviene in modo automatico nell'ultima fase del periodo di vita del certificato non appena il titolare utilizza i servizi della PKI.

La durata di questa fase è fissata a 100 giorni della scadenza della chiave privata del certificato d'autenticazione.

I certificati scaduti non possono essere rinnovati. Le entità devono richiedere dei nuovi certificati secondo quanto definito al punto 3.1.7.

3.3. Richiesta di recovery

Il recovery delle chiavi private di cifratura e del profilo utente può essere richiesto dal titolare e dal proprio Referente alle Abilitazioni.

3.3.1. Richiesta di recovery da parte del titolare

Nel caso in cui non disponga più del proprio profilo (smarrimento, furto, danneggiamento, ecc.), il titolare:

1. Può attivare la procedura di recovery descritta al punto 6.2.2 collegandosi all'indirizzo [6] ed autenticandosi tramite challenge/response da lui definito durante il processo di emissione dei certificati.
2. Qualora non avvenisse con successo l'autenticazione tramite challenge/response, dovrà seguire le indicazioni del punto 3.3.2.
3. Presentarsi alla RA la quale dovrà identificarlo e attivare il processo di recovery della chiave privata e del profilo utente secondo quanto indicato al punto 6.2.2

Al termine della procedura di recovery (creazione di un nuovo certificato), la RA effettuerà la revoca del precedente certificato.

Tale procedura si applica ai certificati di sottoscrizione e sottoscrizione forte.

3.3.2. Richiesta di Recovery da parte del Referente alle Abilitazioni

CERTIFICATI DI SOTTOSCRIZIONE E SOTTOSCRIZIONE FORTE

Per i soli certificati di autenticazione ed autenticazione forte e solo per innescare recupero della titolarità del challenge-response necessario al titolare per procedere in autonomia alla recovery:

- Il Referente alle Abilitazioni invia un'e-mail alla casella di posta ***enelpki@enel.it*** della RA, specificando:
  - Nome e cognome e serial number (codice fiscale) del titolare
  - Le motivazioni della richiesta

La RA deve:

- Rispondere al Referente alle Abilitazioni con un messaggio firmato della cui autenticità il referente stesso dovrà accertarsi;

- Verificare la posizione del Referente alle Abilitazioni, la sua appartenenza alla struttura del titolare e la validità della richiesta;
- Attivare tramite procedura web (previa autenticazione con il proprio certificato digitale) il processo di recupero della titolarità del challenge-response;
- Il processo invierà un codice segreto al titolare ed uno al referente che ha effettuato la richiesta;
- Il titolare, previa ricezione della parte di codice ricevuta dal referente, procederà poi in autonomia alla recovery delle proprie credenziali.

CERTIFICATI DI AUTENTICAZIONE ROAMING

Per i soli certificati di autenticazione roaming, il referente alle abilitazioni:

- Attiva il processo di recovery della chiave privata;
- Riceve in forma cifrata un nuovo segreto, condiviso con la CA e utilizzabile una sola volta per l'attivazione del profilo roaming;
- Consegna il segreto al titolare il quale in autonomia procede all'attivazione della sua nuova credenziale di autenticazione roaming.

3.4. Richiesta di revoca dei certificati

La richiesta di revoca dei certificati deve essere effettuata secondo quanto definito al punto 4.4.

4. REQUISITI GESTIONALI

Vengono qui specificate le regole gestionali per le attività che coinvolgono le diverse entità.

4.1. Richiesta di certificati

Le modalità di richiesta di emissione dei certificati dipendono dal tipo di certificato e dal tipo di entità richiedente.

Per quanto riguarda l'autenticazione del richiedente si rimanda a quanto definito al punto 3.1.7.

4.2. Emissione dei certificati

La modalità d'emissione di un certificato è funzione delle caratteristiche del titolare e del certificato stesso.

L'emissione dei certificati ha come prerequisito l'abilitazione e la valorizzazione delle informazioni del titolari da parte del suo Referente alle Abilitazioni. La richiesta d'emissione è effettuata dal Referente alle Abilitazioni mediante procedura web.

Per la generazione dei certificati i titolari possono collegarsi alla CA tramite un web server.

Mediante un codice segreto, il titolare si autentica alla CA su un canale cifrato (oggi realizzato con SSL), quindi, in modo per lui trasparente, riceve i due codici ACRN che permettono di effettuare autenticazione forte con la CA, conformemente con lo standard RFC2510.

A fronte dell'autenticazione da parte del titolare, il processo di certificazione prevede che la coppia di chiavi asimmetriche di firma sia sempre creata dal titolare con il client o con il dispositivo di firma mentre la coppia di chiavi di cifratura viene creata centralmente dalla CA, che invia al titolare quella privata. La CA conserva copia di quest'ultima, così da poterne permettere l'eventuale recovery.

A fronte di un esito positivo della verifica di possesso della chiave privata di firma da parte del titolare, la CA emette i certificati di firma e cifratura che invia al titolare insieme con il proprio autocertificato.

A fronte di una verifica di possesso non valida, la CA non rilascia i certificati corrispondenti.

Al termine del processo, il titolare sarà in possesso del proprio profilo costituito delle chiavi private di firma e di cifratura, dei certificati di firma e di cifratura e dell'autocertificato della CA.

Nel caso di sottoscrizione forte, il profilo sarà custodito sulla smart card del titolare. Nel caso di sottoscrizione semplice esso sarà sul sistema client. Nel caso di generazione di certificati di sottoscrizione presso RA, verrà registrato direttamente su supporto fisico elettronico e consegnato al titolare.

Per l'emissione di un Certificato di Autenticazione Roaming, il Titolare, mediante un prorpio account personale e un codice segreto utilizzabile una sola volta, si autentica alla CA su un canale cifrato (SSL) e procede all'attivazione del suo certificato personale, precedentemente creato da procedure specifiche della CA.

In tale fase viene effettuata la protezione crittografica del proprio certificato con una nuova passphrase nota al solo titolare. Al termine del processo il titolare riceve tramite l'applicazione di attivazione un codice (PUK) che potrà utilizzare in autonomia per il ripristino della sua credenziale in caso di smarrimento della passphrase.

Al termine del processo, il titolare potrà utilizzare il proprio profilo richiedendolo al repository centralizzato del sistema di roaming, utilizzando il suo account e la passphrase da lui impostata.

A cura della CA viene:

- Pubblicato il certificato di cifratura emesso contenente le informazioni del titolare specificate nel cap. 3.1.
- Memorizzato il codice challenge/response fornito dall'utente utilizzabile secondo quanto definito ai punti 4.2.1e 4.2.2 per quanto riguarda il certificato di autenticazione e autenticazione forte.
- Notificata la generazione del certificato al suo Referente alle Abilitazioni, in forma elettronica.

Qualora il titolare riceva segnalazione di avvenuta certificazione abusiva, comunica l'evento al proprio Referente alle Abilitazioni il quale deve provvedere immediatamente alla revoca dei certificati artefatti.

4.2.1. Certificati di sottoscrizione forte

Il Referente alle Abilitazioni deve:

- Fornire i dati utili alla generazione del certificato e alla sua gestione;
- Abilitare il titolare alla richiesta del certificato.
- Rendere disponibile alla CA le informazioni relative al certificato richiesto;
- Comunicare al titolare che può presentarsi presso la RA per ottenere il certificato.

Nel caso in cui la RA dovesse operare direttamente, la RA stessa deve:

- Identificare il titolare che si è presentato per ottenere il certificato secondo quanto definito al punto 3.1.7.2.
- Verificare che il titolare sia stato abilitato alla richiesta del certificato~~;~~
- Richiedere al titolare di verificare i dati forniti dal Referente alle Abilitazioni
- Richiedere al titolare di definire e comunicare al sistema il codice challenge/response utilizzabile per le funzioni di recovery e/o revoca
- Accettare l'utilizzo da parte dell'infrastruttura dei dati personali per gli scopi afferenti alla certificazione
- Consegnare al titolare il dispositivo di firma

Il titolare inserisce il dispositivo di firma appena ricevuto nel lettore di un sistema affidabile sotto il controllo della RA innesca così il processo automatico di certificazione on line.

Con tale processo viene effettuata:

- La generazione da parte del dispositivo di firma della coppia di chiavi da utilizzare per la firma
- La generazione da parte del server di CA della coppia di chiavi di cifra
- La verifica dell'effettivo possesso della chiave privata di firma
- La generazione da parte della CA dei certificati di firma e cifra
- L'invio dei certificati, insieme all'autocertificato in vigore della CA, al client richiedente che li inserisce nel dispositivo di firma
- La pubblicazione del certificato di cifratura sulla directory

- La notifica della generazione dei certificati al titolare e al suo Referente alle Abilitazioni in forma elettronica o cartacea

Contemporaneamente all'emissione del certificato di sottoscrizione forte viene sempre associato al titolare un distinto certificato di cifratura.

4.2.2. Certificati di sottoscrizione

Il Referente alle Abilitazioni in ottemperanza alla procedura [2] deve:

- Fornire i dati utili alla generazione del certificato e alla sua gestione
- Abilitare il titolare alla richiesta del certificato
- Rendere disponibile alla CA le informazioni relative al certificato richiesto
- Comunicare al titolare la parte di codice segreto necessaria alla successiva emissione del certificato

Il titolare deve:

- Ricevere il codice segreto in possesso del Referente alle Abilitazioni
- Collegarsi all'indirizzo [6] per richiedere i certificati
- Accettare i terminie le condizioni espresse nel documento CP e nel documento CPS
- Autenticarsi mediante il serial number, il codice segreto del titolare ed il codice segreto fornito dal Referente alle Abilitazioni
- Verificare i dati forniti al sistema dal Referente alle Abilitazioni
- Definire e comunicare al sistema il codice challenge/response utilizzabile per le funzioni di recovery e revoca.
- Accettare l'utilizzo da parte dell'infrastruttura dei dati personali per gli scopi afferenti alla certificazione
- Attivare il processo di certificazione che prevede in modo automatico e trasparente per il titolare:
  - La generazione e l'utilizzo di due codici ACRN per la realizzazione di un canale sicuro, in conformità con RFC 2510
  - La generazione della coppia di chiavi da utilizzare per la firma
  - La generazione da parte del server di CA della coppia di chiavi di cifra
  - La verifica dell'effettivo possesso della chiave privata di firma
  - La generazione da parte della CA dei certificati di firma e cifra
  - L'invio dei certificati, insieme all'autocertificato in vigore della CA, al client richiedente che li inserisce nel dispositivo di firma
  - La pubblicazione del certificato di cifratura sulla directory
  - La notifica della generazione dei certificati al titolare ed al suo Referente alle Abilitazioni in forma elettronica o cartacea

Contemporaneamente all'emissione del certificato di sottoscrizione viene sempre associato al titolare un distinto certificato di cifratura.

Qualora la generazione del certificato di sottoscrizione fosse effettuata tramite la RA, quest'ultima deve registrare il profilo contenente i certificati direttamente su supporto fisico elettronico che consegnerà al titolare.

4.2.3. Certificati di autenticazione roaming

Il Referente alle Abilitazioni, in ottemperanza alla procedura [2], deve:

- Inserire tramite applicazione web i dati utili alla richiesta del certificato e alla sua gestione
- Comunicare al Titolare il codice segreto (One Time Password) ricevuto in forma cifrata (mail) dall'applicazione web

Il titolare deve:

- Ricevere il codice segreto (One Time Password) dal Referente alle Abilitazioni
- Collegarsi al sito indicato presso [6] per attivare il certificato roaming
- Autenticarsi mediante la propria matricola aziendale ed il codice segreto (One Time Password) ricevuto dal proprio Referente alle Abilitazioni
- Verificare i dati forniti al sistema dal Referente alle Abilitazioni.
- Attivare il processo di certificazione che prevede in modo automatico e trasparente per il titolare:
  - La generazione della coppia di chiavi da utilizzare per la firma
  - La generazione da parte del server di CA della coppia di chiavi di cifratura (tali chiavi sono generate da un automatismo ma rese inutilizzabili mediante policy applicate all'infrastruttura PKI)
  - La verifica dell'effettivo possesso della chiave privata di firma
  - Il salvataggio delle proprie chiavi sul sistema centralizato (roaming server)
  - La notifica della generazione al suo Referente alle Abilitazioni in forma elettronica (mail)

4.3. Accettazione dei certificati

Come parte del processo di emissione dei certificati, il Titolare accetta il certificato emesso dalla CA.

Accettando il certificato, il titolare accetta i termini e le condizioni contenute nella presente CPS e nel relativo CP, e, ai sensi dell'art.13 del D.Lgs. 30 giugno 2003, n.196 e successive integrazioni e modifiche (Codice in materia di protezione dei dati personali), diviene consapevole che i propri dati personali, specificati nel cap. 3, saranno divulgati su una directory pubblicamente accessibile mediante protocollo LDAP v3.

Come ultima parte del processo di emissione dei certificati, il titolare deve verificare l'esattezza dei dati in esso riportati, ed attivare immediatamente la procedura di revoca descritta al punto 4.4 nel caso dovesse riscontrare inesattezze.

4.4. Revoca dei certificati

Tutte le richieste di revoca e le risultanti azioni devono essere archiviate e conservate per un periodo di almeno 10 anni.

4.4.1. Motivazioni per la revoca

Un certificato viene revocato nei seguenti casi, ad ognuno dei quali sarà assegnato il relativo codice di revoca *CRLReason*:

1. Recovery del profilo senza compromissione della chiave privata, *CRLReason:* ***Superseded***;
2. Compromissione della chiave privata del titolare, *CRLReason:* ***Key Compromise***;
3. I dati del certificato sono modificati o obsoleti, in questo caso ricade anche l'eventualità che un titolare non accetti i certificati emessi a suo nome in quanto i dati sono errati, *CRLReason:* ***Affiliation Changed***;
4. Cessazione repentina, in condizioni di conflittualità, o non, del titolare dalle mansioni per le quali gli erano stati rilasciati i certificati, *CRLReason:* ***Cessation of operation***;
5. Cessazione preventivata dalle mansioni per le quali sono stati rilasciati i certificati al titolare, *CRLReason:* ***Cessation of operation***;
6. Mancato rispetto da parte del titolare degli obblighi di cui al punto 2.1.4, in misura tale che il Referente alle Abilitazioni o la RA ritengano necessaria una revoca immediata, *CRLReason:* ***Unspecified***;
7. Altri casi, *CRLReason:* ***Unspecified***;

Nel caso di compromissione della chiave privata del titolare (*CRLReason*: ***Key Compromise***), viene anche chiesto quale sia stato l'ultimo momento in cui la chiave non fosse ancora compromessa (questo si riflette nella valorizzazione della Extension invalidityDate della entry di CRL relativa al certificato in questione).

4.4.2. Entità idonee alla richiesta di revoca dei certificati

Le seguenti entità possono richiedere la revoca di certificati:

- Il titolare
- Il Referente alle Abilitazioni
- La RA
- La CA

4.4.3. Procedura per la revoca dei certificati

Nel caso la richiesta sia **effettuata dal titolare** può essere inoltrata:

- Mediante un messaggio di posta elettronica cifrato e siglato dal proprio certificato di sottoscrizione alle persone preposte alla funzione di RA
- Per via telefonica, autenticandosi mediante il codice challenge/response fornito nel processo di emissione dei certificati
- Presentandosi personalmente alla RA

Nel caso la richiesta sia effettuata dal Referente alle Abilitazioni può essere inoltrata:

- Mediante l'invio di un messaggio di posta elettronica, firmato col proprio certificato di sottoscrizione, alle persone preposte alla funzione di RA o alla casella pki.certificati@enel.it (Enel PKI - Certificati Digitali)
- Mediante applicativo web, previa autenticazione, per i certificati di autenticazione e autenticazione forte
- Mediante applicativo web, previa autenticazione, effettuata con il proprio certificato di sottoscrizione per i soli certificati di tipo roaming

Qualora sia coinvolta nel processo di revoca, la RA deve:

- Identificare il titolare o il Referente alle Abilitazioni
- Verificare la validità della richiesta
- Attivare il processo di revoca del certificato

La CA e la RA possono originare in modo autonomo, in caso di emergenza, una richiesta di revoca. La motivazione deve essere documentata e firmata da almeno un rappresentante della CA o della RA.

I certificati revocati non possono essere rinnovati.

Notifica di revoca del certificato deve essere inoltrata al titolare e al suo Referente alle Abilitazioni in forma elettronica o cartacea.

Tutte le richieste di revoca e le risultanti azioni devono essere archiviate e conservate per un periodo di almeno 10 anni.

4.4.4. Periodo di tempo per revocare i certificati

La richiesta di revoca di un certificato viene verificata ed eseguita nel più breve tempo possibile e comunque non superiore a dodici ore dal momento in cui la richiesta perviene alla CA.

Nel caso in cui il Referente alle Abilitazioni non abbia già ottemperato agli obblighi previsti al punto 2.1.3, la CA o la RA possono revocare autonomamente i certificati dei titolari, il cui rapporto di lavoro risulti:

- Cessato da almeno tre mesi per il personale dipendente
- Cessato da almeno 6 mesi per il personale dirigente

oppure può revocare quei certificati emessi ai titolari esterni per attività di collaborazione, che risultino scaduti

4.4.5. Periodo di tempo per elaborare le richieste di revoca

La richiesta di revoca di un certificato viene verificata ed eseguita nel più breve tempo possibile e comunque non superiore a dodici ore dal momento in cui la richiesta perviene alla CA.

Nel caso in cui il Referente alle Abilitazioni non abbia già ottemperato agli obblighi previsti al punto 2.1.3, la CA o la RA possono revocare autonomamente i certificati dei titolari, il cui rapporto di lavoro risulti:

- Cessato da almeno tre mesi per il personale dipendente
- Cessato da almeno 6 mesi per il personale dirigente

oppure può revocare quei certificati emessi ai titolari esterni per attività di collaborazione, che risultino scaduti

4.4.6. Frequenza di emissione della CRL e loro disponibilità

Le liste di revoca sono pubblicate ogni dodici ore e comunque nel più breve tempo possibile a fronte della compromissione di certificati o del mancato rispetto dei propri obblighi da parte del titolare.

La disponibilità della directory per la consultazione dei certificati di cifratura e delle CRL è assicurato 24 ore su 24, nel rispetto di quanto indicato al par. 2.6.2.

4.4.7. Verifica della validità dei certificati

Solo per i titolari di certificati di sottoscrizione forte è prevista la disabilitazione del caching delle CRL.

Un utente che verifichi la validità di un certificato dovrà accertarsi che:

1. Sia valido il certification path indicato di seguito;
2. Non sia stato revocato (per i certificati di cifra) o che non fosse revocato o scaduto al momento in cui ne è stata usata la corrispondente chiave privata (per i certificati di firma).

In modo automatico viene controllato sulla base dell'ora di emissione se la CRL ricevuta è l'ultima emessa compatibilmente con la frequenza di emissione. Qualora il momento previsto per l'emissione della CRL aggiornata sia stato superato la CRL non deve essere presa in considerazione e la verifica di validità del certificato deve essere rinviata a quando sarà disponibile la CRL aggiornata.

Per quanto riguarda le CRL emesse estemporaneamente il sistema non garantisce da attacchi del tipo "man in the middle" che ne impediscano l'accesso, in quanto non è possibile essere a conoscenza della loro emissione.

Nel caso in cui, durante la verifica di una firma digitale il corrispondente certificato risulti revocato o scaduto, la firma viene considerata valida se la data di apposizione è anteriore alla data di revoca o a quella di scadenza del certificato.

Non essendo prevista una root CA, il **certification path validation** è basato sui seguenti elementi da prendere in esame in successione da parte degli utenti della PKI:

- Auto certificato emesso dalla propria CA per la sua chiave pubblica – tale certificato è consegnato a tutti i titolari durante il processo di certificazione
- Certificati di cross certification tra la *CA Enel* e le CA con cui siano stati stabiliti accordi di mutua certificazione

A questi elementi, nel caso di rinnovo delle chiavi della CA (vedi punto 4.9), si aggiunge, conformemente all'RFC2510, la coppia di certificati:

- "old with new" (certificato della vecchia chiave pubblica firmato con la nuova chiave privata)
- "new with old" (certificato della nuova chiave pubblica firmato con la vecchia chiave privata)

4.5. Procedure di verifica e controllo

4.5.1. Tipi di eventi registrati

Vengono effettuate tutte le registrazioni necessarie, utili alla verifica e al controllo delle operazioni svolte nell'ambito della CA.

Eventi generati dal server ospitante la CA, dalla CA stessa sono registrati in file di log in modo automatico, eventi esterni sono in parte registrati su supporti elettronici, in parte collezionati manualmente.

4.5.1.1. Eventi del software CA

L'elenco della tipologia dei record di log presi automaticamente dalla CA è riportato nel manuale del prodotto.

4.5.1.2. Eventi registrati al di fuori del controllo della CA

Gli eventi del tipo indicato di seguito sono registrati con le modalità indicate a fianco a ciascuno di essi. I dettagli operativi e di controllo sono di responsabilità delle funzioni competenti.

- Aggiornamenti del software: automatico per alcuni eventi, manuale per altri;
- Manutenzione programmata ed estemporanea dei sistemi e dei locali: automatico per alcuni eventi, manuale per altri
- Accesso ai locali: automatico nei casi in cui si utilizzano controlli accessi automatici, manuale negli altri
- Variazione del personale che ricopre i ruoli di gestione della PKI; manuale

4.5.2. Analisi dei log

I log di competenza della PKI sono verificati con periodicità adeguata a riscontrare tempestivamente l'eventuale insorgere di malfunzionamenti, deviazioni dalla procedura, ecc.

I dettagli sulle modalità gestionali e periodicità delle verifiche sono oggetto di norme interne.

4.5.3. Conservazione dei log

I log vengono conservati per un periodo di tempo non inferiore a 10 anni.

4.5.4. Protezione dei log

L'accesso ai log è protetto sia fisicamente che logicamente.

Tutte le informazioni presenti nei log riportano la data e l'ora di generazione.

I file di log riportano la data e l'ora di ultimo aggiornamento.

I singoli record di log del software CA sono protetti da alterazioni con MAC.

L'integrità e la riservatezza dei log prodotti automaticamente da altre procedure viene ottenuta in maniera commisurata all'importanza dei dati.

Quella dei log manuali è protetta con i tradizionali metodi: registrazione su giornali a pagine non asportabili numerate progressivamente e monotonicamente, inizializzate preventivamente dalla funzione responsabile e da essa vistate successivamente al loro riempimento per conferma di integrità.

4.5.5. Copia di riserva dei log

Copie di riserva dei file di log sono prodotte giornalmente e conservate localmente. Ogni settimana una copia consolidata viene predisposta in un sito differente da quello principale.

4.5.6. Eventi controllati e collezionati

La CA nel suo complesso, inclusi la directory, verificano e controllano almeno i seguenti eventi:

- Inizializzazione e chiusura dei servizi della CA,
- Eventi di creazione, modifica, rimozione, disattivazione, attivazione, e ripristino dei profili dei titolari
- Eventi di creazione, modifica, rimozione, disattivazione, attivazione e recovery di profili relativi a personale addetto alla CA e alle RA
- Eventi di generazione, aggiornamento e recovery delle chiavi e dei profili utente
- Esecuzione di Backup e restore degli archivi della CA,
- Esecuzione di Backup, restore e cancellazione dei log
- Operazioni di manutenzione del sistema schedulate e non
- Aggiornamenti del software applicativo

4.5.7. Notifica a fronte di eventi critici

I sistemi di monitoraggio implementati e documentati nel "Manuale di Esercibilità" notificano al personale addetto alla CA ogni discrepanza o evento critico rilevato.

L'elenco degli eventi di questo tipo è elencato nel manuale relativo al software della CA: "Administering Entrust PKI".

Gli eventi al di fuori del controllo della CA sono oggetto di norme interne documentate dal gruppo che sovrintende l'esercizio.

4.6. Informazioni archiviate

4.6.1. Tipi di informazioni archiviate

La CA archivia i seguenti tipi di informazioni:

- Eventi relativi a verifiche e controlli, secondo quanto definito al punto 4.5.1
- Certificati
- Chiavi private di cifra, in forma protetta, per consentire la gestione della key history,

- Documentazione
- Accordi di cross certification
- Documentazione cartacea ed elettronica: corrispondenza, richieste di certificazione, richieste di recovery del profilo o della chiave privata di cifratura, richieste di revoca integrate della documentazione necessaria, report di independent audit, ecc.
- Sottoscrizione dell'informativa ed accettazione del consenso al trattamento dati, da parte del Titolare del certificato.
- Richieste di accesso alle informazioni archiviate.

4.6.2. Periodo di conservazione degli archivi

Documentazione relativa ad accordi di cross certification e la documentazione cartacea sono mantenuti per un periodo di tempo non inferiore ai 10 anni.

4.6.3. Protezione degli archivi

Gli archivi sono protetti sia dal punto di vista fisico che logico.

Sono in generale previste adeguate forme di protezione da elementi ambientali quali temperatura, umidità oltre che da tentativi di manomissione e di accesso non autorizzato.

4.6.4. Copie di riserva degli archivi

Per i log, i certificati, le CRL e le chiavi di cifratura custodite dalla CA sono effettuate giornalmente copie di riserva, mantenendo valida la tutela dell'integrità e della riservatezza delle informazioni.

Giornalmente è predisposta una copia di questi elementi presso un sito differente da quello principale, mantenendo valida la tutela dell'integrità e della riservatezza delle informazioni.

4.6.5. Procedura per verificare ed ottenere informazioni archiviate

Le richieste per accedere ad informazioni archiviate sono sottoposte alla CA in forma scritta e gestite secondo quanto definito al punto 2.8.

4.7. Rinnovo delle chiavi della CA

Il rinnovo della chiave della CA e del relativo certificato avviene in modo pianificato non oltre 3 mesi prima della scadenza del certificato stesso

La vecchia chiave pubblica sarà certificata con la nuova chiave privata e la nuova chiave pubblica sarà certificata con la vecchia chiave privata. Il risultato di questa "cross certification" e l'autocertificato della nuova chiave pubblica saranno pubblicati nella directory, insieme con l'autocertificato relativo alla coppia vecchia di chiavi.

Nel certificato di ogni coppia di chiavi della CA il Name dello issuer, *CA Enel*, è uguale per tutte le coppie di chiavi della CA mentre lo auhorityKeyIdentifier è specifico per ogni coppia di chiavi ed è il digest ottenuto con SHA-1 della chiave pubblica della CA. Questo consente di "navigare" lungo la sostituzione delle chiavi della CA in ambedue i sensi.

4.8. Procedure di emergenza e disaster recovery

Per assicurare la normale continuità del servizio, la *CA Enel* dispone di un apposito sito di Disaster Recovery e di apposite procedure di restore dei dati e delle configurazioni, in modo da ricreare un ambiente identico a quello di produzione in caso di assoluta indisponibilità di quest'ultimo.

La procedura di restore è da considerarsi *a freddo*, ovvero, le basi di dati vengono ripristinate sul sistema di Disaster Recovery partendo da un backup del sistema di produzione risalente al momento più prossimo prima del disastro.

La gestione del sito di Disaster Recovery, la definizione delle relative procedure e la loro applicazione sono di responsabilità dell'Unità *Enel Servizi / Information & Communication Technology Operations Sistemi e TLC*, che ha, appunto, l'obbligo di garantire il rispetto della CP e del relativo CPS, anche in condizioni di disastro.

4.8.1. Revoca della chiave della CA

La chiave della CA può essere revocata solo per sua compromissione.

La CA deve notificare per iscritto a tutti i titolari e alle CA riconosciute tramite cross certification le modalità di prosecuzione delle attività, in accordo con le presenti policy e le leggi in vigore.

4.9. Termine dell'attività della CA

Qualora la CA cessi le proprie attività essa provvederà a:

- Stipulare accordo con altra organizzazione, adeguatamente strutturata, la quale si impegnerà al rispetto degli adempimenti di sua competenza indicati nel punto successivo.
- Informare in forma scritta, almeno sei mesi prima della data prevista di cessazione, tutte le CA riconosciute tramite cross certification ed i propri titolari. Questa comunicazione sarà firmata dal medesimo livello di potere di firma che ha firmato l'accordo di cross certification e conterrà le seguenti informazioni:
    - indicazione di dove saranno resi disponibili i propri archivi che saranno mantenuti per un periodo di tempo non inferiore ai 10 anni.
    - indicazione di dove sarà resa disponibile la directory contenente l'ultima CRL. Questa CRL verrà conservata fino a quando non sarà trascorsa la scadenza naturale di tutti i certificati revocati in essa elencati.
- Revocare i certificati emessi non ancora scaduti al momento della cessazione della propria attività, tra i quali l'autocertificato della CA. Per quest'ultimo il momento da cui decorre la revoca coincide con il momento di emissione dell'ultima CRL.

5. SICUREZZA AMBIENTALE, PROCEDURALE E DEL PERSONALE

Questa sezione specifica i controlli per la sicurezza ambientale, procedurale e del personale richiesti per tutelare le operazioni di:

- Generazione delle chiavi
- Autenticazione delle entità
- Emissione, recovery e revoca dei certificati
- Verifica e controllo
- Archiviazione dei dati

5.1. Sicurezza ambientale

Sono implementati dei controlli di accesso all'hardware ed al software utilizzati per la fruizione dei servizi offerti dalla CA.

5.1.1. Luoghi ed edifici

I dispositivi utilizzati dalla CA per il proprio funzionamento si trovano in un ambiente completamente chiuso, ad accesso controllato, all'interno di edifici sui quali il Gruppo ENEL ha piena libertà di effettuare le modifiche tecniche necessarie nel rispetto della normativa vigente, a loro volta protetti da adeguati servizi di sicurezza, operanti con continuità.

5.1.1.1. Sede della CA

La *CA Enel* si trova presso la sede Enel di Sesto S.Giovanni (Mi), è sorvegliata all'esterno da guardie giurate le quali sono tenute a rispettare le seguenti regole di accesso:

- Consentire libero accesso alla sede ENEL solo al personale che esibisca il tesserino aziendale valido, tesserino che dovrà essere esposto sempre e soltanto durante la permanenza all'interno della sede
- Riconoscere e registrare il personale sprovvisto di tale documento, dotandolo di tesserino provvisorio sostitutivo
- Registrare i visitatori, indicando anche il dipendente presso cui si recano. Il visitatore depositerà un documento di riconoscimento, i cui estremi saranno registrati, e riceverà un tesserino di riconoscimento provvisorio che dovrà tenere esposto in modo visibile

Il locale dove è ospitata la CA si trova nel locale di sala calcolo ed utilizza le stesse infrastrutture tecnologiche (Antincendio, doppia alimentazione da diverse cabine secondarie, gruppi di continuità) proprie del CED.

5.1.2. Accesso fisico

5.1.2.1. CA

L'accesso è controllato mediante l'utilizzo di dispositivi elettronici di riconoscimento e meccanismi di chiusura automatici, sotto allarme. L'area interessata è controllata senza soluzione di continuità dalle persone incaricate della sicurezza o da mezzi elettronici.

Le informazioni relative agli accessi sono registrate, manualmente o automaticamente, e controllate periodicamente.

Il personale addetto alle funzioni di servizio e manutenzione degli ambienti è scortato e sorvegliato.

5.1.2.2. RA

La RA deve implementare le seguenti funzioni di controllo:

- Il computer della RA non deve essere utilizzato da altre entità, se non sotto sorveglianza della RA stessa.
- Sono messe in atto misure di sicurezza per impedire intrusioni all'interno dei computer ed evidenziare gli eventuali tentativi. Tali misure di sicurezza sono dipendenti dal tipo di sistema utilizzato e comunque è necessario prevedere al minimo, in alternativa:
  - La limitazione dell'accesso all'interno del sistema mediante l'utilizzo di lucchetti o serrature la cui chiave è custodita dalla RA stessa
  - Utilizzare strumenti che evidenzino eventuali tentativi di intrusione

5.1.2.3. Titolari

I titolari devono proteggere ogni passphrase che permetta loro di accedere alla componente client della PKI o al profilo utente indipendentemente da dove esso sia memorizzato.

Le passphrase non devono essere scritte su supporti leggibili liberamente, a meno che non vengano custodite in modo da garantire l'accesso al solo titolare.

Le passphrase devono rispettare le norme indicate al documento "Accesso ai documenti informatici".

I supporti fisici su cui è custodita la chiave privata devono essere custoditi in modo sicuro ed accessibili al solo titolare.

I titolari non devono lasciare i loro computer incustoditi mentre è attiva la componente client della PKI (la passphrase è già stata digitata). Deve essere impostato un logoff automatico qualora il sistema non sia utilizzato per 5 minuti.

5.1.3. Energia elettrica, cablaggi di rete e condizionamento dell'aria

L'energia elettrica utilizzata dalla CA è fornita in modo ridondante mediante doppia alimentazione da diverse cabine secondarie per la distribuzione di energia. Sono inoltre presenti dei gruppi di continuità UPS.

I cablaggi di rete non sono direttamente accessibili in quanto posati sotto il pavimento flottante su cui si trovano i dispositivi della CA.

E' presente un sistema di condizionamento dell'aria.

5.1.4. Esposizione all'acqua

Si rimanda alle specifiche procedure aziendali di prevenzione e protezione all'esposizione all'acqua.

5.1.5. Misure di prevenzione e protezione dagli incendi

Si rimanda alle specifiche procedure aziendali di prevenzione e protezione dagli incendi.

5.1.6. Dispositivi di memorizzazione

I dispositivi di memorizzazione utilizzati dalla CA e dalla RA devono:

- Essere sottoposti a verifica della presenza di virus
- Essere conservati in ambienti con condizioni ambientali idonee ad accesso limitato e controllato
- Essere eliminati in modo da non poter recuperare i dati in essi memorizzati (es.: taglio dei CD e dei dischetti, degaussing dei nastri e dei dischi)

5.1.7. Gestione dei rifiuti

Le informazioni su supporti cartacei devono essere eliminate in modo da garantire la non leggibilità delle informazioni distrutte mediante l'utilizzo di inceneritori o strumenti idonei che triturino i fogli.

5.2. Sicurezza procedurale

La linea manageriale responsabile dei processi correlati al funzionamento della PKI è indicata di seguito:

1. Amministratore delegato Enel
2. Responsabile della funzione Esercizio Sistemi - Enel
3. Responsabile della CA

5.2.1. Profili

5.2.1.1. Profili per la CA

Le varie mansioni necessarie al funzionamento della PKI sono assegnate al personale secondo *Ruoli* funzionali distinti.

Tutto il personale è specificatamente addestrato a svolgere il proprio ruolo attraverso il piano di formazione specificato al punto 5.5.

5.2.2. Numero di persone necessarie per funzione

Per lo svolgimento di alcune delle funzioni della CA è necessaria la presenza di più persone, secondo quanto definito nella seguente tabella.

FUNZIONE CA	N. MINIMO DI PERSONE ABILITATE	N. MAX DI PERSONE NECESSARIE	N. MINIMO DI PERSONE PRESENTI
MASTER USER	3	3	2
FIRST OFFICER (*)	1	1	1
SECURITY OFFICER	3	4	1
ENTRUST ADMINISTRATOR	3	4	1
DIRECTORY ADMINISTRATOR	3	4	1

(*)E' il primo Security Officer attivato: ha il compito di attivare gli altri Security Officer e viene revocato immediatamente dopo la loro attivazione

5.2.3. Riconoscimento degli addetti

Si rimanda al punto 3.1.7.1.

5.3. Sicurezza sul personale

5.3.1. Addetti alla CA

Il personale di gestione della CA (par. 5.2.1.1) è esaminato e controllato dai responsabili della struttura organizzativa aziendale. I responsabili non sono autorizzati all'esecuzione delle attività assegnate al personale di gestione.

Il personale di gestione della CA ha le seguenti caratteristiche:

- E' personale dipendente di Enel a tempo indeterminato;
- Non è assegnato ad altri ruoli che possano influenzare con le proprie funzioni di gestione della CA;
- Non è stato responsabile di azioni di negligenza negli ultimi 5 anni;
- Il proprio ruolo gli è stato assegnato in forma scritta;
- Gli sono stati comunicati tutti i termini e le responsabilità del ruolo assegnatogli.

5.3.2. Addetti alla RA

La RA ha il compito di identificare le entità e comunicare le richieste di queste ultime alla CA. Essendo un punto di coordinamento per le entità che desiderano comunicare con la CA deve rispondere ai medesimi requisiti definiti al punto 5.3.1.

5.3.3. Titolari

I titolari sono messi al corrente dei rispettivi obblighi tramite il documento pubblicato secondo quanto definito al capoverso 7 del punto 2.1.1.1, ulteriormente dettagliato al punto2.1.4.

I *Referenti alle Abilitazioni* sono tenuti a fornire adeguata informativa ai propri titolari.

5.4. Qualifiche, esperienza e requisiti

5.4.1. Qualifiche

Le qualifiche aziendali degli addetti alla CA e alla RA devono essere tali da garantire un'adeguata autonomia decisionale in casi di emergenza, e tali da dare alle mansioni funzionalmente più delicate la possibilità di concedere o negare autorizzazioni di sicurezza ad altre persone, senza dover sottostare a pressioni gerarchiche.

5.4.2. Esperienza

Il personale addetto a svolgere i compiti presso la CA ha maturato una esperienza almeno quinquennale nell'ambito della conduzione di sistemi informatici.

E' stato inoltre formato professionalmente seguendo opportuni corsi teorico-pratici sui singoli prodotti utilizzati, secondo quanto definito al punto 5.5

5.4.3. Requisiti

5.4.3.1. Master Users

Accedono fisicamente ai server di Entrust/PKI per gestire Entrust/Authority usando Entrust/Authority Master Control.

I Master Users non possono fare login a Entrust/RA.

I Master User provvedono a:

- Attivare e arrestare i servizi di Entrust
- Effettuare il backup ed il restore del database di Entrust/Authority in casi straordinari

5.4.3.2. Security Officer

Usano Entrust/RA per eseguire le operazioni ad elevato contenuto di riservatezza di Entrust/PKI.

I Security Officers in sostanza impostano le security policy per la PKI e gestiscono gli altri administrator.

I Security Officers usano Entrust/RA per:

- Configurare Entrust/PKI in conformità con le security policies
- Predisporre i titolari per il key recovery
- Aggiungere e cancellare gli altri Security Officers, gli Administrator, gli Auditor e i Directory Administrator

5.4.3.3. Entrust Administrator

Usano Entrust/RA per svolgere le funzioni rivolte all'utente:

- Aggiungere, cancellare, abilitare, disabilitare e modificare i DN degli utenti di Entrust
- Revocare i certificati

- Effettuare il recovery delle chiavi private di cifratura degli utenti.

5.4.3.4. Directory Administrator

Usano gli strumenti della Directory in Entrust/RA per eseguire solo attività correlate alla Directory:

- Aggiungere e togliere elementi dalla Directory, in batch o uno alla volta
- Aggiungere attributi alle entry della Directory
- Modificare i DN degli utenti nella Directory, singolarmente o tramite procedure batch

5.4.3.5. Auditor

Possono utilizzare Entrust/RA solo per ispezionare: possono esaminare, ma non modificare gli audit log, i report, la security policy e le proprietà utente.

5.5. Formazione

5.5.1. Formazione del personale

La competenza del personale addetto alla CA e alla RA, riscontrata già all'atto della loro assegnazione a tale mansione, viene approfondita mediante periodici corsi di aggiornamento in funzione dei profili ed in particolare:

- Sull'utilizzo delle componenti software della CA
- Sull'utilizzo delle componenti hardware utilizzate dalla CA, compresi i dispositivi crittografici.
- Sulle misure di sicurezza da adottare in funzione del proprio profilo
- Sulle varie procedure operative indicate in questo documento CPS e nei documenti in esso menzionati
- Sulle procedure da seguire in caso di emergenza

5.5.2. Frequenza degli aggiornamenti

I corsi di aggiornamento del personale addetto alla CA e alla RA saranno seguiti in misura dipendente dal profilo, della durata non inferiore mediamente a 5 giorni annui, presso centri di istruzione interni ed esterni ad Enel.

5.6. Sequenza e variabilità dei profili

Onde evitare che la permanenza di una persona in un ruolo possa creare situazioni di difficile gestione, a cura dal responsabile della PKI definire la rotazione delle mansioni.

5.7. Sanzioni per azioni non autorizzate

Si rimanda alle Policy Aziendali generali in materia.

5.8. Documentazione

Gli addetti alla CA e alla RA sono forniti di documentazione che esponga in modo dettagliato le procedure da seguire per i processi che li vedono coinvolti: manuali dei prodotti, CP, CPS, procedure specifiche, Security Policy, Piano delle situazioni di emergenza, manuale di esercizio.

6. SICUREZZA TECNICA

6.1. Generazione e memorizzazione delle chiavi

6.1.1. Generazione delle chiavi

6.1.1.1. CA

Le coppie di chiavi della CA vengono generate in modo sicuro attraverso l'utilizzo della tecnologia Entrust.

6.1.1.2. Titolari

La generazione delle chiavi di firma viene effettuata sulle stazioni di lavoro dei titolari o sulla stazione di lavoro della RA, secondo quanto definito al punto 4.2.

Il software utilizzato per generare le coppie di chiavi dei titolari è certificato FIPS 140-1.

Le coppie di chiavi di cifratura sono generate da Entrust/Authority, certificato FIPS 140-1 e Common Criteria EAL3.

6.1.2. Rilascio della chiave privata al titolare

Per il certificato di sottoscrizione, la coppia di chiavi è generata dal titolare sulla propria stazione di lavoro o sulla stazione di lavoro della RA. Qualora la generazione del certificato di sottoscrizione fosse effettuata tramite la RA, quest'ultima provvederà a registrare direttamente il profilo contenente i certificati su supporto fisico elettronico che consegnerà al titolare.

Il certificato di sottoscrizione forte, generato dal titolare in presenza della RA, è memorizzato, come parte del profilo utente, sul dispositivo che viene consegnato dalla RA al titolare del certificato.

Per il certificato di cifratura, la coppia di chiavi è generata dalla CA e trasferita al titolare mediante un canale protetto secondo RFC 2510.

6.1.3. Rilascio della chiave pubblica di sottoscrizione alla CA

Una volta generata la coppia di chiavi, la chiave pubblica viene trasmessa alla CA, mediante una transazione on-line che rispetta il protocollo RFC 2510 di gestione dei certificati.

6.1.4. Rilascio della chiave pubblica della CA ai titolari

Durante la sessione di certificazione conforme a quanto definito in RFC 2510 viene rilasciato al titolare anche l'autocertificato della chiave pubblica della CA.

6.1.5. Dimensione delle chiavi

La lunghezza delle chiavi della CA è di 2048 bit, quella dei titolari è di 1024 bit.

6.1.6. Generatore delle chiavi

Le coppie di chiavi di firma della CA e quelle di cifratura dei titolari vengono generate da Entrust/Autority, il cui kernel crittografico è certificato FIPS 140-1(svolge anche la funzione di generazione delle chiavi).

Entrust/Autority è certificato Common Criteria EAL3 ed opera su un sistema UNIX, certificato ITSEC E3.

(non risulta che SUN Solaris 4.6 sia certificato ITSEC E3. Lo è SUN Solaris 2.6)

La chiave privata di firma della CA viene utilizzata da un modulo crittografico esterno, viene conservata nel database della CA ed è ivi cifrata in modo tale da poter essere estratta soltanto dalla CA e da poter essere utilizzata soltanto dal modulo crittografico stesso. In tal modo, sfruttando il backup del database della CA, è possibile ripartire rapidamente in caso di guasto del sistema della CA.

Le coppie di chiavi di firma dei titolari vengono generate da dispositivi certificati FIPS 140-1 a livello 1 se software.

6.1.7. Utilizzo dei certificati

Per limitare l'utilizzo dei certificati alle singole tipologie definite ai punti 1.3.6 delle CP è utilizzata l'extension *KeyUsage* come segue:

- Per i certificati di sottoscrizione valorizzare i campi digitalSignature e nonRepudiation
- Per i certificati di cifratura valorizzare il campo keyEncipherment
- Per i certificati di certificazione valorizzare il campo keyCertSign e il campo cRLSign

6.2. Protezione delle chiavi private

6.2.1. Standard per il modulo di cifratura

Tutte le operazioni di cifratura effettuate dalla CA, dalla RA e dai titolari sono effettuate tramite moduli software certificati FIPS 140-1.

6.2.2. Recovery delle chiavi private di cifratura e dei profili utenti

Le modalità di richiesta del recovery sono indicate al punto 3.3.

La copia della chiave privata di cifratura è conservata in forma cifrata dalla CA.

Il recovery della chiave privata di cifratura e del profilo viene effettuato coinvolgendo la figura di Entrust Administrator secondo la percentuale indicata al punto 5.2.2.

Il **recovery della chiave privata** di cifratura è effettuato quando il titolare dimentica la passphrase di sblocco del profilo.

Si ha il recovery del profilo dopo una revoca del certificato di firma o su dimenticanza di passphrase.

Quando l'utente effettua il recovery:

- Sarà stato già revocato dall' Entrust/Administrator il certificato di firma,

- Verrà generata una nuova coppia di chiavi di firma,
- Verrà inviata al titolare la key history, cioè l'insieme delle chiavi private di cifratura generate per lui fino al momento del recovery[1],
- Dovrà essere definito il nuovo codice challenge/response.

Notifica di recovery della chiave privata di cifratura o di recovery del profilo utente viene inoltrata al titolare e al suo responsabile in forma elettronica e, in casi eccezionali, cartacea secondo quanto definito al punto 2.8.1.

I certificati di cifratura revocati o scaduti possono essere oggetto di recovery da parte del Referente alle Abilitazioni del titolare in questione.

6.2.3. Backup delle chiavi private

Durante le procedure di Vaulting Back-up, il back-up delle chiavi della CA Enel è realizzato mediante cifrartura delle chiavi stesse, in modo automatico attraverso il prodotto Entrust.

Per le chiavi private di cifratura dei titolari viene effettuata una copia di backup automatica che consente sia di recuperare la chiave di cifratura in vigore (ad esempio per lo smarrimento della passphrase di sblocco da parte del titolare) sia di recuperare chiavi private sostituite da tempo con altre più recenti (key history). Quest'ultima funzione è indispensabile per decifrare file dopo che sia trascorso molto tempo dalla loro cifratura.

6.2.4. Deposito delle chiavi private di sottoscrizione

Non viene effettuato il deposito delle chiavi private di sottoscrizione.

6.2.5. Attivazione della chiave privata/profilo utente

La chiave privata deve essere attivata a fronte di un processo di login dove la passphrase del titolare è richiesta e validata.

6.2.6. Disattivazione della chiave privata/profilo utente

La disattivazione della chiave privata avviene come conseguenza del processo di logout dall'applicazione della CA o dall'utilizzo del profilo del titolare, a seconda dei casi. Il logout del titolare deve avvenire automaticamente a fronte di un periodo di inattività di 5 minuti.

6.3. Altri aspetti di gestione delle chiavi

6.3.1. Ciclo di vita delle coppie di chiavi

Le chiavi private dei titolari hanno normalmente un ciclo di vita non superiore ai 2 anni. I corrispondenti certificati di chiave pubblica hanno una durata di 5 anni.

[1] Nel caso di utilizzo delle smart card il numero di chiavi di cifratura storiche è limitato dalla memoria EEPROM della smart card. Qualora il titolare debba ricorrere a chiavi non conservate nella smart card dovrà fare ricorso al supporto della CA e non potrà quindi operare off line.

La chiave privata della CA ha una vita non superiore a 10 anni. L'autocertificato della corrispondente chiave pubblica ha una durata di 15 anni.

La durata della chiave privata del TSS è fissata in 2 mesi, quella del certificato in 24 mesi.

6.4. Sicurezza dei computer

Il sistema operativo dei sistemi di elaborazione utilizzati nelle attività di certificazione per la generazione delle chiavi, per la generazione dei certificati e per la gestione del registro dei certificati è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC o superiori.

L'accesso degli addetti è protetto dall'uso di passphrase nel rispetto di quanto previsto al documento "Accesso ai sistemi informatici".

6.5. Sicurezza della rete

La CA e i suoi repository sono protetti tramite firewall configurati in modo tale da accettare solamente i protocolli ed i comandi richiesti per i servizi offerti dalla CA.

7. CERTIFICATI E CRL

Questa sezione contiene le regole e le linee guida riguardo l'uso di certificati X.509 e delle liste di revoca.

7.1. Profilo dei certificati

I certificati emessi in accordo al presente documento CPS sono conformi allo standard ITU-T X.509v3 e allo RFC 2459 - PKIX 1 o successivi aggiornamenti.

Vi vengono indicati in particolare:

- issuer Name: *CA Enel*
- authorityKeyIdentifier: digest SHA-1 della chiave pubblica della CA– extension NON CRITICA
- cRLDistributionPoints: il fullName del DistributionPointName è il directoryName.

Il valore di altre extension è riportato al punto 6.1.7.

7.1.1. Versione

La CA emette certificati in formato X.509.v3 o successivi aggiornamenti.

7.1.2. Algoritmo

L'algoritmo asimmetrico utilizzato è:

- RSA (Rivest-Shamir-Adleman) in accordo con PKCS#1

Il client della PKI è in grado di riconoscere e verificare anche i seguenti algoritmi di firma:

- DSA (Digital Signature Algoritm) in accordo con DSS (FIPS PUB 186 e ANSI X9.30)
- ECDSA 192

Gli algoritmi di hashing utilizzati sono:

- MD5, come da RFC 1321
- SHA-1, come da ISO/IEC 10118-3, Dedicated Hash-Function 3

Gli algoritmi di cifratura simmetrici utilizzati sono:

- 3DES, come da ANSI X9.52
- CAST-128, come da RFC 2144
- IDEA – International Data Encryption Algorithm – European Patent Office *Patent No. 0482154* – US Pat. 5,214,703

7.2. Restrizioni sui nomi

L'extension *nameConstraint* non è supportata.

7.3. Utilizzo dell'estensione basic constraints

Nel certificato della *CA Enel* nella extension *basicConstraints* il valore di *pathLenConstraint* è 1.

7.4. Profilo della CRL

La CRL è del tipo X.509 v2, o successivi aggiornamenti, ed è conforme allo standard ITU-T X.509v3 e a RFC 2459 PKIX 1 o successivi aggiornamenti.

La extension reasonCode può essere impostata secondo quanto definito al punto 4.4.1 e solo per i seguenti CRLReason:

- unspecified
- keyCompromise
- affiliationChanged
- superseded
- cessationOfOperation.

E' possibile valorizzare il campo *invalidityDate*, per indicare l'ultima data nella quale la chiave privata risultava non essere compromessa.

8. AMMINISTRAZIONE DELLE POLICY

8.1. Nuovi Certification Practice Statements

E' prevista l'emissione di nuovi documenti CPS a fronte di variazioni significative delle modalità di emissione, relative anche a nuove tipologie di certificati o di titolari non previste dal presente documento.

I nuovi CPS potranno aggiungersi o sostituirsi a quelli già pubblicati, a giudizio della *CA Enel*. Nel caso siano sostitutivi, i titolari saranno informati secondo quanto definito al punto 2.8.1. Essi saranno pubblicati allo stesso URL del presente documento e vi verrà specificato se sono aggiuntivi o sostitutivi del medesimo.

8.2. Variazione delle CPS

8.2.1. Elementi modificabili senza preavviso

Sul presente documento CPS è possibile effettuare solo le seguenti modifiche, senza doverne notificare la riemissione:

- Editoriali
- Correzioni tipografiche
- Riferimenti a persone o organizzazioni

8.2.2. Elementi modificabili con preavviso

1. Ogni elemento presente in questo documento può essere modificato normalmente con 30 giorni di preavviso
2. Variazioni ad elementi che non hanno un impatto sostanziale sull'infrastruttura PKI possono essere effettuate con 15 giorni di preavviso.
3. A seguito di circostanze eccezionali possono essere effettuate delle variazioni con l'obbligo di notificarle entro 5 giorni dalla data di aggiornamento.

8.2.3. Notifica delle variazioni

Tutte le variazione proposte devono essere portate a conoscenza di:

- CA riconosciute tramite cross certification
- Titolari

Le informazioni possono essere pubblicate su Web server o trasmesse in posta elettronica.

8.2.4. Gestione dei commenti

I commenti alle variazioni sono sottoposti all'attenzione delle figure responsabili della definizione dei documenti CP e CPS indicate al punto 1.4.2 le quali sono libere di applicare o meno i suggerimenti forniti dagli utenti.

8.2.5. Applicazione delle correzioni

L'applicazione di eventuali correzioni derivanti da commenti pervenuti dalle entità coinvolte non richiede una ulteriore notifica delle variazioni.