L'ENERGIA CHE TI ASCOLTA.

Information and Communication Technology
Security

CERTIFICATE POLICY

CERTIFICATI DIGITALI EROGATI DALLA CA ENEL

CORPORATE POLICY

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

SOMMARIO

Il presente documento definisce le *Policy*, ovvero l'insieme delle regole generali, relative all'emissione e all'utilizzo dei *Certificati Digitali* erogati dalla *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	PolicyPKI-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 la nuova Infrastruttura di Disaster Recovery Minor issuee: • Adeguamento conservazione LOG e accesso fisico	PolicyPKI-CB2.0 PolicyPKI-CB21

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/***

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

[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

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

INDICE

1. INTRODUZIONE 14
1.1. Generalità 14
1.2. Identificazione 15
1.2.1. Identificatore alfanumerico 15
1.2.2. Identificatore oggetto 15
1.3. Entità e applicabilità 16
1.3.1. Certification Authority (CA) 16
1.3.2. Registration Authority (RA) 16
1.3.3. Titolari 16
1.3.4. Referente alle Abilitazioni 17
1.3.5. Titolari di Certificati Erogati da Altre CA 17
1.3.6. Applicabilità 17
1.3.6.1. Servizi previsti 17
1.3.6.2. Certificati 18
1.3.6.2.1. Certificati di sottoscrizione e di sottoscrizione forte 18
1.3.6.2.2. Certificati di cifratura 18
1.3.6.2.3. Certificati di certificazione 18
1.3.6.2.4. Certificati di autenticazione roaming 18
1.3.6.3. Ambiti di utilizzo 18
1.4. Riferimenti 19
1.4.1. Organizzazione 19
1.4.2. Persone 19

2. CONDIZIONI GENERALI 20
2.1. Obblighi 20
2.1.1. Obblighi della CA 20
2.1.1.1. Informativa agli utenti 20
2.1.1.2. Identificazione delle entità 20
2.1.1.3. Emissione dei certificati 21
2.1.1.4. Gestione dei certificati 21
2.1.1.5. Revoca dei certificati 21
2.1.1.6. Obblighi delle CA in cross certification 21
2.1.1.7. Altri adempimenti 21
2.1.2. Obblighi della RA 22
2.1.2.1. Altri adempimenti 22
2.1.3. Obblighi dei Referenti alle Abilitazioni 22
2.1.4. Obblighi dei titolari 22
2.1.5. Obblighi delle CA in cross certification 23
2.1.6. Responsabilità di altre entità 23
2.2. Garanzie e limitazioni di responsabilità 24
2.2.1. Responsabilità della CA 24
2.2.1.1. Garanzie 24
2.2.1.2. Limitazioni 24
2.2.2. Responsabilità della RA 25
2.2.2.1. Garanzie 25
2.2.2.2. Limitazioni 25
2.3. Responsabilità finanziaria 25
2.3.1. Indennizzi 25

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

2.3.2. Relazioni fiduciarie 25
2.4. Interpretazione e competenze legislative 25
2.4.1. Riferimenti 25
2.4.2. Modifiche organizzative della CA 25
2.5. Tariffe 26
2.5.1. Generazione e rinnovo dei certificati 26
2.5.2. Recovery della chiave privata di cifratura 26
2.5.3. Altri servizi 26
2.6. Pubblicazione e repository 26
2.6.1. Pubblicazione di informazioni 26
2.6.2. Frequenza di aggiornamento delle informazioni pubblicate 26
2.6.3. Controllo di accesso 27
2.7. Verifiche di conformità alla CP e al CPS 27
2.7.1. Conformità 27
2.7.1.1. Conformità della CA 27
2.7.1.1.1. Frequenza 27
2.7.1.1.2. Processi soggetti al controllo 27
2.7.1.1.3. Azioni da intraprendere in caso di inadempienza 27
2.7.1.2. Conformità della RA 28
2.7.1.2.1. Frequenza 28
2.7.1.2.2. Processi soggetti al controllo 28
2.7.1.2.3. Azioni da intraprendere in caso di inadempienza 28
2.7.1.3. Conformità delle altre entità 28
2.7.2. Identità e qualifica dei controllori 28
2.7.3. Relazioni tra i controllori e l'infrastruttura PKI 28
2.7.4. Comunicazione dei risultati 28
2.8. Policy di riservatezza 28
2.8.1. Comunicazione ai Referente alle Abilitazioni 28
2.8.2. Comunicazione di informazioni ad organi ufficiali 29
2.9. Copyright e leggi sulla proprietà intellettuale 29

3. IDENTIFICAZIONE E AUTENTICAZIONE 30
3.1. Registrazione iniziale 30
3.1.1. Nomi assegnabili 30
3.1.2. Significatività dei nomi 31
3.1.3. Regole per l'interpretazione dei nomi 31
3.1.4. Univocità dei nomi 31
3.1.5. Risoluzione di conflitti sui nomi 31
3.1.6. Prova di possesso della chiave privata 31
3.1.7. Autenticazione delle entità 31
3.2. Richiesta di rinnovo dei certificati 32
3.3. Richiesta di recovery 32
3.4. Richiesta di revoca dei certificati 33

4. REQUISITI GESTIONALI 34
4.1. Richiesta di certificati 34
4.2. Emissione dei certificati 34
4.3. Accettazione dei certificati da parte dei Titolare 35
4.4. Revoca dei certificati 35
4.4.1. Motivazioni per la revoca 35
4.4.2. Entità idonee alla richiesta di revoca dei certificati 35
4.4.3. Procedura per la richiesta di revoca dei certificati 36
4.4.4. Periodo di tempo per revocare i certificati 36

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

4.4.5. Frequenza di emissione della CRL e loro disponibilità 37
4.4.6. Verifica della validità dei certificati 37
4.5. Procedure di verifica e controllo 37
4.5.1. Tipi di eventi registrati 37
4.5.2. Analisi dei log 37
4.5.3. Conservazione dei log 37
4.5.4. Protezione dei log 37
4.5.5. Copia di riserva dei log 37
4.5.6. Eventi controllati e collezionati 38
4.5.7. Notifica a fronte di eventi critici 38
4.6. Informazioni archiviate 38
4.6.1. Tipi di informazioni archiviate 38
4.6.2. Periodo di conservazione degli archivi 39
4.6.3. Protezione degli archivi 39
4.6.4. Copie di riserva degli archivi 39
4.6.5. Procedura per verificare ed ottenere informazioni archiviate 39
4.7. Rinnovo delle chiavi della CA 39
4.8. Procedure di emergenza e disaster recovery 39
4.8.1. Revoca della chiave della CA 40
4.9. Termine dell'attività della CA 40

5. SICUREZZA AMBIENTALE, PROCEDURALE E DEL PERSONALE 41
5.1. Sicurezza ambientale 41
5.1.1. Luoghi ed edifici 41
5.1.2. Accesso fisico 41
5.1.2.1. CA 41
5.1.2.2. RA 41
5.1.2.3. Titolari 42
5.1.3. Energia elettrica, cablaggi di rete e condizionamento dell'aria 42
5.1.4. Esposizione all'acqua 42
5.1.5. Misure di prevenzione e protezione dagli incendi 42
5.1.6. Dispositivi di memorizzazione 42
5.1.7. Gestione dei rifiuti 42
5.2. Sicurezza procedurale 43
5.2.1. Profili 43
5.2.1.1. Profili per la CA 43
5.2.2. Numero di persone necessarie per azione 43
5.2.3. Riconoscimento degli addetti 43
5.3. Sicurezza sul personale 43
5.3.1. Addetti alla CA 43
5.3.2. Addetti alla RA 44
5.3.3. Titolari 44
5.4. Qualifiche, esperienza e requisiti 44
5.4.1. Qualifiche 44
5.4.2. Esperienza 44
5.4.3. Requisiti 44
5.5. Formazione 44
5.5.1. Formazione del personale 44
5.5.2. Frequenza degli aggiornamenti 45
5.6. Sequenza e variabilità dei profili 45
5.7. Sanzioni per azioni non autorizzate 45
5.8. Documentazione 45

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

6. SICUREZZA TECNICA 46
6.1. Generazione e memorizzazione delle chiavi 46
6.1.1. Generazione delle chiavi 46
6.1.1.1. CA 46
6.1.1.2. Titolari 46
6.1.2. Rilascio della chiave privata al titolare 46
6.1.3. Rilascio della chiave pubblica di sottoscrizione alla CA 46
6.1.4. Rilascio della chiave pubblica della CA ai titolari 46
6.1.5. Dimensione delle chiavi 46
6.1.6. Generatore delle chiavi 47
6.1.7. Utilizzo dei certificati 47
6.2. Protezione delle chiavi private 47
6.2.1. Standard per il modulo di cifratura 47
6.2.2. Recovery delle chiavi private di cifratura e dei profili utenti 47
6.2.3. Backup delle chiavi private 47
6.2.4. Deposito delle chiavi private 48
6.2.5. Archiviazione delle chiavi private di cifratura 48
6.2.6. Attivazione della chiave privata/profilo utente 48
6.2.7. Disattivazione della chiave privata/profilo utente 48
6.2.8. Distruzione della chiave privata 48
6.3. Altri aspetti di gestione delle chiavi 48
6.3.1. Archiviazione delle chiavi pubbliche 48
6.3.2. Ciclo di vita delle coppie di chiavi 48
6.4. Sicurezza dei computer 49
6.5. Sicurezza della rete 49

7. CERTIFICATI E CRL 50
7.1. Profilo dei certificati 50
7.1.1. Versione 50
7.1.2. Algoritmo 50
7.2. Restrizioni sui nomi 50
7.3. Utilizzo dell'estensione basic constraints 50
7.4. Profilo della CRL 51

8. AMMINISTRAZIONE DELLE POLICY 52
8.1. Nuove policy 52
8.2. Variazione delle policy 52
8.2.1. Elementi modificabili senza preavviso 52
8.2.2. Elementi modificabili con preavviso 52
8.2.3. Notifica delle variazioni 52
8.2.4. Periodo utile per ricevere commenti 52
8.2.5. Gestione dei commenti 53
8.2.6. Applicazione delle correzioni 53

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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.
Codici Segreti	I codici riservati concordati tra utente e CA per stabilire un'identificazione sicura dell'utente all'atto della sua certificazione tramite AutoRA.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

	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.
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

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

	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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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	

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

1. INTRODUZIONE

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*.

La presente *Cerificate Policy* (*CP*), impostata sulla base delle linee guida del RFC2527, definisce l'insieme delle regole generali relative all'emissione e all'utilizzo dei *Certificati Digitali* erogati dalla *CA Enel*.

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

La stessa Funzione Aziendale è anche responsabile della stesura e della gestione delle procedure e istruzioni contenute nel *Certification Policy Statemet* (*CPS*) associata a questa *CP*.

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 sua 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.

1.1. Generalità

Il presente documento definisce le regole per l'applicabilità dei certificati contenenti chiavi pubbliche del seguente tipo:

- Chiavi di sottoscrizione forte
- Chiavi di sottoscrizione
- Chiavi di cifratura
- Chiavi di certificazione
- Chiavi di autenticazione

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

Di seguito tali certificati saranno definiti come:

- Certificati di sottoscrizione forte
- Certificati di sottoscrizione
- Certificati di cifratura
- Certificati di certificazione
- Certificati di autenticazione roaming

CERTIFICATI DI SOTTOSCRIZIONE E DI SOTTOSCRIZIONE FORTE

Questi certificati vengono utilizzati nei seguenti ambiti:

- Autenticazione del titolare
- Garantire l'integrità e l'autenticità delle informazioni scambiate tra diverse parti

I certificati di sottoscrizione forte prevedono l'utilizzo della Smart Card da parte dei Titolari che, così, dispongono di un controllo di sicurezza a due fattori, particolarmente efficace, che riduce in modo significativo la possibilità di utilizzo fraudolento dei servizi crittografici ad essi assegnati.

Queste chiavi sono utilizzabili per sottoscrivere atti e documenti. Sottoscrizione che, in base al d.lgs. 82/2005, non conferisce al documento la validità della forma scritta che resta caratteristica esclusiva dei documenti validati con firma digitale o firma elettronica qualificata.

CERTIFICATI DI CIFRATURA

Questi certificati possono essere utilizzati per garantire la riservatezza delle informazioni.

CERTIFICATI DI CERTIFICAZIONE

Questi certificati sono utilizzati per verificare la firma apposta dalla CA sui certificati emessi e sulle liste di revoca. Il titolare delle chiavi corrispondenti è la CA stessa.

CERTIFICATI DI AUTENTICAZIONE ROAMING

Il loro utilizzo garantisce l'autenticazione ad un sito web in modalità sicura.

1.2. Identificazione

1.2.1. Identificatore alfanumerico

Il presente documento *Certificati Digitali Erogati dalla CA Enel – Certificate Policy* è identificato attraverso il seguente Codice Documento *PolicyPKI-CB2.0*.

1.2.2. Identificatore oggetto

Questo documento CP 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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

1.3. Entità e applicabilità

Questo capitolo specifica a quali entità (punti 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5) si applica la presente CP, relativamente all'utilizzo dei certificati e delle applicazioni secondo quanto indicato al punto 1.3.6.

1.3.1. Certification Authority (CA)

La CA è l'entità responsabile dell'emissione e della pubblicazione dei certificati, della pubblicazione delle liste dei certificati revocati, della definizione di relazioni di fiducia con altre CA. La CA è responsabile di tutte le attività gestionali necessarie al suo corretto funzionamento.

La CA si impegna a conformarsi alle specifiche di questo documento CP.

La CA pubblica un documento di CPS sulla base del presente documento CP.

Possono essere definite più CA relazionate tra di loro, ogni CA che soddisfi le policy qui definite può emettere certificati validi nell'ambito delle aziende appartenenti al gruppo Enel.

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*;

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- 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.

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

Le presenti policy si applicano alla CA, alla RA, ai certificati ed alle liste di revoca gestite dalla CA, e ai titolari per relativamente all'utilizzo dei servizi di seguito specificati.

1.3.6.1. Servizi previsti

I certificati emessi secondo le presenti policy possono essere utilizzati per:

- Autenticazione (certificati di sottoscrizione, di sottoscrizione forte e roaming)
- Verifica dell'integrità e dell'autenticità delle informazioni (certificati di sottoscrizione e di sottoscrizione forte)

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- Cifratura di informazioni (certificati di cifratura resi disponibili ai titolari di certificati sottoscrizione e di sottoscrizione forte)

1.3.6.2. Certificati

In accordo con le presenti policy la CA può emettere i seguenti tipi di certificati:

1.3.6.2.1. Certificati di sottoscrizione e di sottoscrizione forte

Il loro utilizzo garantisce l'identità del firmatario e l'integrità delle informazioni trattate. Atti, dati e documenti sottoscritti con firme apposte con queste chiavi non hanno l'efficacia probatoria di scrittura privata ai sensi dell'art 2702 c.c. (art.5 comma 1 d.p.r. n. 513/1997).

1.3.6.2.2. Certificati di cifratura

Il loro utilizzo garantisce la riservatezza dei dati sottoposti al processo di cifratura. Tale ulteriore certificato viene rilasciato automaticamente al titolare all'atto del rilascio del certificato di sottoscrizione o sottoscrizione forte.

1.3.6.2.3. Certificati di certificazione

Loro titolare esclusivo è la CA e non sono richiedibili da nessuna altra entità. Devono essere utilizzati per verificare l'autenticità dei certificati di sottoscrizione forte, di sottoscrizione, di cifratura.

1.3.6.2.4. Certificati di autenticazione roaming

Il loro utilizzo garantisce la sola autenticazione ad un sito web in modalità sicura. Il certificato roaming consente al Titolare il roaming delle sue Credenziali di autenticazione, rendendolo indipendente dalla postazione di lavoro utilizzata.

1.3.6.3. Ambiti di utilizzo

Gli ambiti di utilizzo dei certificati emessi secondo le presenti policy sono:

CERTIFICATI DI SOTTOSCRIZIONE FORTE

Le entità che possono avere questo tipo di certificati, per cui è prevista la dotazione di una Smart Card, sono:

- Referente alle Abilitazioni
- Titolari esterni con particolari esigenze di sicurezza (clienti che accedono a servizi particolari offerti dalle società del gruppo ENEL o che necessitano di comunicare in modalità riservata con Enel)
- Titolari interni con particolari esigenze di sicurezza (amministratori di sistema, personale addetto alla CA, dirigenti, eccetera)

CERTIFICATI DI SOTTOSCRIZIONE

Le entità che possono avere questo tipo di certificati sono:

- Titolari interni

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- Titolari esterni

CERTIFICATI DI CIFRATURA

Tutte le entità hanno questo tipo di certificati contestualmente al certificato di sottoscrizione o di sottoscrizione forte.

CERTIFICATI DI AUTENTICAZIONE ROAMING

Le entità che possono avere questo tipo di certificati, normalmente in alternativa ai certificati di sottoscrizione o di sottoscrizione forte, sono quelle entità che hanno necessità di effettuare solo operazioni di autenticazione e non di cifratura, esse sono:

- Titolari interni
- Titolari esterni

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, nei ruoli di *Verificatore*.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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

2.1.1. Obblighi della CA

La CA opera secondo quanto definito nella presente CP e nel relativo CP di riferimento;

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

La CA deve sostenere i diritti dei titolari che utilizzano i certificati nel rispetto delle presenti policy e del documento CPS.

2.1.1.1. Informativa agli utenti

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

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 nella 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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

2.1.1.3. Emissione dei certificati

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

- Notificare l'avvenuta emissione del certificato al suo Referente alle Abilitazioni. 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 e pubblicare il certificato di cifratura nell'apposita directory.
- Rilasciare l'informativa sul trattamento dei dati personali del Titolare, 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 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 emesso, 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

2.1.1.6. Obblighi delle CA in cross certification

La CA ha la possibilità di instaurare relazioni di cross certification con altre CA secondo quanto definito nel documento CPS, sempre che esse applichino misure di sicurezza e affidabilità compatibili con quelle della presente CP e del CPS associato.

2.1.1.7. Altri adempimenti

Oltre a quanto precedentemente elencato la CA deve:

- Proteggere la propria chiave di certificazione
- Gestire un archivio storico dei certificati emessi e delle liste di revoca
- Pubblicare le procedure per l'espletamento delle proprie attività (CPS) secondo quanto definito nel presente documento CP
- Attenersi ai vincoli legislativi di cui al punto 2.4.1
- Garantire la continuità del servizio di emissione dei certificati dalle ore 9.00 alle ore 16.00 di ogni giorno lavorativo, ed in ogni caso la revoca dei certificati e l'emissione delle liste di revoca (CRL) senza soluzione di continuità ad eccezione dei periodi di indisponibilità per manutenzione straordinaria.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- La CA deve pubblicare i certificati di cifratura e le liste di revoca (CRL) su una directory accessibile mediante protocollo LDAP v3 secondo quanto definito in RFC2251. 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 nel documento CPS, ad eccezione dei periodi di indisponibilità del servizio dovuta a particolari attività di manutenzione straordinaria.
- La CA deve assicurare l'aggiornamento del clock di sistema dei dispositivi da lei utilizzati

2.1.2. Obblighi della RA

La RA deve operare secondo quanto definito nella presente CP e nel CPS associato.

La RA autorizzerà allo svolgimento del proprio ruolo i Referenti alle Abilitazioni incaricati dalle strutture aziendali.

La RA fornisce supporto ai Referenti alle Abilitazioni nell'ambito delle loro attività, soprattutto nell'utilizzo degli strumenti tecnologici messi a disposizione dalla CA e nella risoluzione di eventuali problemi procedurali.

2.1.2.1. Altri adempimenti

La RA deve:

- Proteggere la propria chiave privata e la relativa passphrase
- Assicurare l'aggiornamento del clock di sistema dei dispositivi da lei utilizzati mantenendolo allineato all'ora della rete della *CA Enel*.

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.

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 sono reperibili CP e CPS.
- 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:

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- 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, effettuato dalla CA Enel, resa disponibile in modo automatizzato, eseguendo il processo di rilascio/emissione del certificato digitale.

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. Obblighi delle CA in cross certification

CA che hanno stipulato accordi di cross-certification con la *CA Enel* devono rispettare le proprie policy riconosciute equivalenti alla presente.

L'utilizzo di un certificato di una CA in cross certification, presuppone che sia verificata la validità del certificato stesso tramite liste di revoca aggiornate e la cui autenticità dovrà essere verificata utilizzando i certificati di cross certification.

2.1.6. Responsabilità di altre entità

Anche le entità non certificate dalla *CA Enel* o di CA non in cross certification con la *CA Enel*, sono responsabili della verifica della validità del certificato e più in generale del suo utilizzo. Nei loro confronti la *CA Enel* non ha alcun obbligo.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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 alle presenti policy
- L'emissione dei certificati viene effettuata in accordo con le presenti policy
- La revoca dei certificati emessi viene effettuata in accordo con le presenti policy
- La gestione delle liste di revoca viene effettuata in accordo con le presenti policy
- L'effettuazione del servizio di recovery della chiave privata di cifratura e del profilo utente viene effettuato in accordo con le presenti policy
- La CA opererà con la dovuta diligenza e competenza, nell'ambito delle mansioni attribuitele dalla direzione aziendale
- Il trattamento dei dati personali degli utenti avverrà nel rispetto dell'art. 13 del D.lgs 196/2003.
- I documenti CP e CPS verranno aggiornati annualmente e comunque ogni qualvolta si renda necessario.

2.2.1.2. Limitazioni

Salvo quanto espresso al punto 2.2.1.1 la CA non risponde di:

- Informazioni false o errate che le siano state fornite e sulle quali non è tenuta ad effettuare verifiche
- Informazioni false o errate presenti in certificati emessi da CA riconosciute tramite cross certification
- Negligenza, incuria e mancato rispetto degli obblighi previsti in questo documento CP e nel documento CPS, da parte dei titolari o di coloro che utilizzano i certificati
- Utilizzo di certificati da parte di entità non appartenenti alla *CA Enel* o non appartenenti a CA in cross certification con la CA Enel
- Qualsiasi conseguenza derivante dall'utilizzo dei certificati al di fuori delle modalità espressamente previste in questo documento CP e nel documento CPS
- Danni derivanti da attacchi perpetrati sulla rete e non imputabili a incompetenza o negligenza della CA o del personale addetto
- Eventuali problemi derivanti dalla mancata verifica, da parte degli utenti, delle CRL emesse
- Danni derivanti da eventi catastrofici o comunque imprevedibili
- Errori causati da prodotti software o hardware utilizzati dai titolari o da chi verifica l'affidabilità di un certificato che non siano stati forniti o autorizzati dalla CA qui definita, salvo quanto stipulato negli accordi di cross certification

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

2.2.2. Responsabilità della RA

2.2.2.1. Garanzie

La RA garantisce che la relazione di corrispondenza tra Titolare e Referente alle Abilitazioni sia corretta.

2.2.2.2. Limitazioni

Salvo quanto espresso al punto 2.2.2.1 la RA non risponde di:

- Informazioni false o errate che le siano state fornite e sulle quali non è tenuta ad effettuare verifiche
- Negligenza, incuria e mancato rispetto degli obblighi previsti in questo documento CP e nel documento CPS, da parte dei titolari o di coloro che utilizzano i certificati.

2.3. Responsabilità finanziaria

2.3.1. Indennizzi

La CA esclude ogni forma d'indennizzo per eventuali danni subiti dai titolari o da terzi.

2.3.2. Relazioni fiduciarie

La generazione di certificati in accordo con le presenti policy non rende la CA un agente, un fiduciario, un amministratore o altro tipo di rappresentante per i titolari.

2.4. Interpretazione e competenze legislative

2.4.1. Riferimenti

DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 – Codice in materia di protezione dei dati personali e successive modificazioni ed integrazioni.

2.4.2. Modifiche organizzative della CA

Eventuali modifiche organizzative che hanno impatti sulla *CA Enel* verranno comunicate a tutte le entità coinvolte con un anticipo di almeno due mesi rispetto alla loro attuazione.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

2.5. Tariffe

2.5.1. Generazione e rinnovo dei certificati

Le tariffe relative alla generazione ed al rinnovo dei certificati saranno definite in accordo con le strutture organizzative aziendali di appartenenza dei titolari interni o con le strutture organizzative esterne di appartenenza dei titolari esterni.

2.5.2. Recovery della chiave privata di cifratura

Le tariffe relative al recovery della chiave privata di cifratura saranno definite in accordo con le strutture organizzative aziendali di appartenenza dei titolari interni o con le strutture organizzative esterne di appartenenza dei titolari esterni.

2.5.3. Altri servizi

Nessun pagamento deve essere corrisposto per accedere a:

- Liste di revoca
- Alla presente CP pubblicata come specificato al punto 2.6.1
- Al CPS associato alla presente CP pubblicato come specificato al punto 2.6.1.

2.6. Pubblicazione e repository

2.6.1. Pubblicazione di informazioni

Saranno pubblicati e liberamente consultabili all'indirizzo [5] i seguenti documenti:

- Il documento CP
- Il documento CPS

E' gestita una struttura dati, consultabile liberamente, contente le liste di revoca mediante protocollo ldap ai seguenti indirizzi; ***ldap1.enelit.enel***, ***ldap2.Enel***, ***ldap3.Enel***, ***ladp5.enelit.enel***, ***ladp6.enelit.enel***.

2.6.2. Frequenza di aggiornamento delle informazioni pubblicate

I certificati di cifratura sono pubblicati nel più breve tempo possibile dal momento della loro emissione. L'intervallo di tempo tra l'emissione e la pubblicazione non deve essere superiore alle dodici ore.

Le liste di revoca sono pubblicate ogni dodici ore e tendenzialmente in modo immediato a fronte della compromissione di certificati o del mancato rispetto dei propri obblighi da parte del titolare.

Versioni aggiornate del documento CP e del documento CPS vengono rilasciate nel più breve tempo possibile.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

2.6.3. Controllo di accesso

Non è richiesto alcun controllo sugli accessi alla CP e al suo CPS.

2.7. Verifiche di conformità alla CP e al CPS

Sono previste le seguenti azioni di verifica e controllo:

- Confronto tra le regole pratiche definite nel documento CPS ed i processi realmente seguiti dalle entità
- Confronto tra le policy qui definite ed i processi realmente seguiti dalle funzioni della CA

2.7.1. Conformità

2.7.1.1. Conformità della CA

2.7.1.1.1. Frequenza

La verifica dei processi seguiti dalla CA è effettuata almeno ogni anno e comunque al verificarsi di eventi significativi.

2.7.1.1.2. Processi soggetti al controllo

Sono previste delle azioni di controllo per i seguenti elementi di queste policy:

- Identificazione ed autenticazione
- Requisiti gestionali
- Sicurezza ambientale, procedurale e sul personale
- Sicurezza tecnica
- Profili dei certificati e delle liste di revoca
- Amministrazione delle policy

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 CA è possibile:

- Revocare eventuali certificati emessi dalla CA
- Definire delle azioni di correzione che la CA deve intraprendere entro un periodo di tempo adeguato

Qualora si verificasse la compromissione della chiave privata della CA, ne sarà revocato il relativo certificato. In quest'ultimo caso la CA deve notificare a tutti i titolari e alle CA in cross certification le modalità di prosecuzione delle attività, in accordo con le presenti policy.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

2.7.1.2. Conformità della RA

2.7.1.2.1. Frequenza

La verifica dei processi seguiti dalla RA è effettuata almeno ogni anno e comunque al verificarsi di eventi significativi.

2.7.1.2.2. Processi soggetti al controllo

Le azioni di controllo sono effettuate secondo quanto definito al punto 2.7.1.1.2

2.7.1.2.3. Azioni da intraprendere in caso di inadempienza

I risultati delle verifiche e dei controlli effettuati sono sottoposti all'attenzione della CA la quale è responsabile delle eventuali azioni correttive.

2.7.1.3. Conformità delle altre entità

I titolari interni e i titolari esterni possono essere soggetti ad azioni di verifica e controllo. Per ulteriori dettagli si rimanda al documento CPS.

2.7.2. Identità e qualifica dei controllori

Le figure responsabili delle azioni di verifica e controllo effettuate sulle entità hanno una significativa esperienza nell'ambito delle tecnologie utilizzate dalla CA e dei processi di cifratura.

2.7.3. Relazioni tra i controllori e l'infrastruttura PKI

Al di fuori delle azioni di verifica e controllo le figure di controllore e le entità della infrastruttura PKI non hanno alcuna relazione in corso o pianificata di tipo finanziario, legale, o che possa portare ad un conflitto di interessi.

2.7.4. Comunicazione dei risultati

I risultati delle azioni di verifica e di controllo sono considerati riservati e gestiti secondo quanto definito al punto 2.8

2.8. Policy di riservatezza

Tutte le informazioni raccolte, generate, trasmesse e gestite dalla CA sono considerate riservate e trattate secondo quanto definito ai punti 2.4.1, 4.6, 5 e 6.

2.8.1. Comunicazione ai Referente alle Abilitazioni

Al Referente alle Abilitazioni vengono comunicate le seguenti informazioni:

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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

La comunicazione è effettuata in forma elettronica.

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 presente documento CP, il documento CPS, ecc. sono di proprietà della società Enel.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

3. IDENTIFICAZIONE E AUTENTICAZIONE

Vengono qui specificate le policy 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 Referente alle Abilitazioni a cui il titolare o il dispositivo afferiscono (*Enel*, Wind, Terna, Fiat S.p.A., QChannel …)

O

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- 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* conterrà un codice identificativo, attribuito in accordo alle procedure specificate nel CPS, in modo da rendere tale campo univoco.

3.1.3. Regole per l'interpretazione dei nomi

Si rimanda al punto 3.1.2 nell'ambito di quanto definito al punto 3.1.1.

3.1.4. Univocità dei nomi

Il nome del titolare non può essere ambiguo ed è univoco per tutti i certificati emessi dalla CA.

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 previo 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 viene verificato che i titolari siano in possesso della chiave privata corrispondente a quella pubblica di cui chiedono la certificazione, secondo le procedure indicate nel documento CPS.

3.1.7. Autenticazione delle entità

Al fine di associare un certificato al titolare e garantire l'identità di quest'ultima sono previste le seguenti forme di autenticazione:

CERTIFICATI DI SOTTOSCRIZIONE FORTE E CERTIFICATI DI SOTTOSCRIZIONE

La RA deve:

- Verificare che sia stato autorizzato il rilascio di un certificato di sottoscrizione o di sottoscrizione forte per il titolare da parte del suo Referente alle Abilitazioni, dopo averlo identificato

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- Collegarsi ai servizi di CA, usufruendo di un apposito servizio Web o del client di amministrazione, e successivamente fornire un'informazione segreta di cui solo il titolare e la CA sono a conoscenza
- Assistere, quando necessario, per il tramite dei suoi appositi addetti, il titolare durante il processo di certificazione

CERTIFICATI DI AUTENTICAZIONE ROAMING

La RA deve:

- Verificare che sia stato autorizzato il rilascio di un certificato di forte autenticazione roaming per il titolare da parte del suo Referente alle Abilitazioni;
- Collegarsi alla CA, usufruendo di un apposito servizio Web o del client di amministrazione, e successivamente fornire un'informazione segreta di cui solo il titolare e la CA sono a conoscenza;
- Assistere, se necessario, per il tramite dei suoi appositi addetti, il titolare durante il processo di certificazione.

I certificati di autenticazione roaming sono rilasciati a tutti i titolari per cui non è richiesta un'autenticazione apposita.

CERTIFICATI DI CIFRATURA

I certificati di cifratura sono rilasciati a tutti i coloro siano titolari di certificati di sottoscrizione e di sottoscrizione forte.

Per i titolari di certificati Roaming, viene inibito il servizio di cifratura.

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 (RFC2510).

I certificati vengono automaticamente rinnovati nell'arco temporale degli ultimi 100 giorni di validità della propria chiave privata di 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 oppure dal proprio Referente alle Abilitazioni.

La comunicazione da parte del titolare può essere effettuata in uno dei seguenti modi:

- Mediante un messaggio di posta elettronica cifrato e siglato dal proprio certificato di sottoscrizione
- Collegandosi alla CA, usufruendo di un Web server o del client specifici, autenticandosi mediante il codice segreto fornito durante processo di emissione dei certificati
- Presentandosi di persona alla RA.

La comunicazione da parte del Referente alle Abilitazioni può essere effettuata in uno dei seguenti modi:

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- Mediante un messaggio di posta elettronica cifrato e siglato dal proprio certificato di sottoscrizione
- Collegandosi alla CA, attraverso un applicativo web, al quale si deve autenticare mediante il proprio certificato di sottoscrizione
- Presentandosi di persona alla RA.

La CA, a fronte della richiesta, deve effettuare il recovery della chiave privata di cifratura e del profilo utente, secondo quanto definito al punto 6.2.2.

3.4. Richiesta di revoca dei certificati

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

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

4. REQUISITI GESTIONALI

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

4.1. Richiesta di certificati

Le informazioni necessarie alla CA per l'emissione dei certificati dipendono dal tipo di certificato e dal tipo di entità 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 RFC 2510.

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 il 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. Qualora quest'ultimo fosse quello della RA (generazione di certificati di sottoscrizione presso RA) verrà registrato direttamente su un floppy disk 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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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 successivo cap. 3.1.
- Memorizzato il codice challenge/response fornito dall'utente utilizzabile secondo quanto definito ai punti 3.3 e 4.4 per quanto riguarda il certificato di autenticazione e autenticazione forte.
- Notificata la generazione del certificato al titolare e 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 alla revoca urgente dei certificati artefatti.

4.3. Accettazione dei certificati da parte dei Titolare

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 CP e nel relativo CPS, 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 pubblicati su una directory accessibile mediante protocollo LDAP v3.

4.4. Revoca dei certificati

4.4.1. Motivazioni per la revoca

Un certificato deve essere revocato nei seguenti casi:

- Le informazioni contenute nel certificato variano o diventano obsolete
- Non è più garantita la riservatezza della chiave privata
- Malfunzionamenti del dispositivo di firma
- Il titolare non ha rispettato gli obblighi di cui al punto 2.1.4
- Cessazione del rapporto di lavoro del titolare interno
- Cessazione dell'attività di collaborazione del titolare esterno

4.4.2. Entità idonee alla richiesta di revoca dei certificati

Le seguenti entità possono richiedere la revoca di certificati:

- Il Referente alle Abilitazioni che, in accordo alle procedure stabilite nel CPS, è l'entità normalmente preposta al servizio di revoca
- Il titolare
- La CA

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- La RA

4.4.3. Procedura per la richiesta di 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
- 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 un messaggio di posta elettronica cifrato e siglato dal proprio certificato di sottoscrizione
- Mediante applicativo web previa autenticazione effettuata con il proprio certificato di sottoscrizione

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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

4.4.5. 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.

4.4.6. Verifica della validità dei certificati

La verifica della validità dei certificati viene eseguita in modalità on-line, come specificato nel documento CPS.

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

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.

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.

4.5.3. Conservazione dei log

I log sono conservati per un periodo di tempo non inferiore ai 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 e ne è protetta l'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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

4.5.6. Eventi controllati e collezionati

La CA verifica e controlla 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
- Eventi di generazione, aggiornamento e recovery delle chiavi e dei profili utente
- Eventi di creazione, aggiornamento revoca e recovery dei certificati
- 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 hardware e software

Eventi generati dal server ospitante la CA o dalla CA stessa devono essere registrati in file di log in modo automatico, eventi esterni possono essere collezionati manualmente.

I log possono essere trasferiti su supporti fisici esterni alla CA o al server ospitante.

4.5.7. Notifica a fronte di eventi critici

Il server ospitante o la CA notificano al personale addetto alla CA ogni discrepanza o evento critico rilevato.

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 4.5.6
- Certificati
- Chiavi private di cifra, in forma protetta, per consentire la gestione della key history,
- Documentazione
- Accordi 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 indipendent audit, ecc.
- Sottoscrizione dell'informativa ed accettazione del consenso sul trattamento dei dati personali del Titolare del certificato,
- Richieste di accesso alle informazioni archiviate.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

4.6.2. Periodo di conservazione degli archivi

Documentazione relativa ad accordi di cross certification e la corrispondenza 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 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 sono effettuate delle copie di riserva giornalmente, 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 ed il nuovo certificato della chiave pubblica saranno pubblicati nella directory.

4.8. Procedure di emergenza e disaster recovery

Per assicurare la normale continuità del servizio, la CA 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 Organizzativa *ICT Production*, con ha l'obbligo di garantire il rispetto della CP e del relativo CPS, anche in condizioni di disastro.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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

Si rimanda al documento CPS.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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.

5.1.2. Accesso fisico

5.1.2.1. CA

L'accesso ai locali ove è ospitata la CA è limitato e 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 almeno le seguenti funzioni di controllo:

- Il computer della RA non deve essere utilizzato da altre entità, se non in presenza della RA stessa
- Sono messe in atto misure di sicurezza per impedire intrusioni all'interno dei computer ed evidenziare gli eventuali tentativi.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- Se la chiave privata fosse contenuta in un dispositivo di cifratura hardware, quest'ultimo deve essere riposto in una cassetta di sicurezza durante i periodi di inutilizzo. Nel caso di cifratura software, non deve essere possibile asportare o comunque accedere al disco rigido del computer
- L'utilizzo del computer deve essere tutelato da adeguati sistemi di identificazione della RA stessa

Per ulteriori dettagli si rimanda al documento CPS.

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".

Qualora la chiave privata sia memorizzata su supporti non sicuri (es. floppy disk), questi ultimi devono essere custoditi in modo da essere 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).

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

Si rimanda al documento CPS.

5.1.4. Esposizione all'acqua

Si rimanda al documento CPS.

5.1.5. Misure di prevenzione e protezione dagli incendi

Si rimanda al documento CPS.

5.1.6. Dispositivi di memorizzazione

Si rimanda al documento CPS.

5.1.7. Gestione dei rifiuti

Si rimanda al documento CPS.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

5.2. Sicurezza procedurale

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

1. Responsabile *Corporate / Sede Corporate / Pers.Org.Serv. / Sicurezza ICT*
2. Responsabile *Enel Servizi / Information & Communication Technology / Operations Sistemi e TLC / Sicurezza IT*
3. Responsabile *Enel Servizi / Information & Communication Technology / Operations Sistemi e TLC / Sicurezza IT / Sicurezza IT*

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.

Una singola persona può essere associata a più ruoli e un ruolo è associato a più persone.

5.2.2. Numero di persone necessarie per azione

Per lo svolgimento di alcune delle funzioni della CA è necessaria la presenza di più persone, come indicato nel documento CPS.

5.2.3. Riconoscimento degli addetti

Si rimanda al documento CPS.

5.3. Sicurezza sul personale

5.3.1. Addetti alla CA

Il personale addetto ai differenti compiti relativi alla CA è verificato e controllato dai propri responsabili della struttura organizzativa aziendale. I responsabili non sono autorizzati all'esecuzione delle attività assegnate al personale addetto.

Il personale addetto alla CA e alla RA ha le seguenti caratteristiche:

- E' personale dipendente di Enel a tempo indeterminato.
- Non è assegnato ad altri ruoli che possano interferire con le proprie funzioni all'interno della PKI
- Non è stato autore di azioni di negligenza negli ultimi 5 anni
- E' stato assegnato, in forma scritta, a ricoprire il ruolo all'interno della PKI
- Gli sono stati comunicati termini e le responsabilità della sua posizione all'interno della PKI e deve essersi dichiarato, in forma scritta, d'accordo

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- Ha ricevuto un'adeguata formazione relativa al ruolo ricoperto nella PKI

5.3.2. Addetti alla RA

La RA ha il compito di identificare le entità e comunicare le richieste di questi ultimi alla CA. Essendo un punto di coordinamento per le entità che desiderano comunicare con la CA deve rispondere a quanto definito al punto 5.3.1.

5.3.3. Titolari

I titolari sono messi al corrente delle procedure da rispettare per proteggere gli strumenti utilizzati per usufruire dei servizi offerti dalla CA. I responsabili e la CA 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.

5.4.2. Esperienza

Il personale addetto a svolgere dei 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.

5.4.3. Requisiti

Si rimanda al documento CPS.

5.5. Formazione

5.5.1. Formazione del personale

Il personale addetto alla CA e alla RA riceve un'adeguata formazione in funzione dei profili ed in particolare:

- Formazione sull'utilizzo delle componenti software della CA
- Formazione sull'utilizzo delle componenti hardware utilizzate dalla CA

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- Formazione sulle misure di sicurezza da adottare in funzione del proprio profilo
- Formazione sulle varie procedure operative indicate nel documento CPS e nei documenti in esso menzionati
- Formazione sulle procedure da seguire in caso di emergenza.

5.5.2. Frequenza degli aggiornamenti

Almeno ogni anno è proposto un aggiornamento delle conoscenze degli addetti alla CA e alla RA.

5.6. Sequenza e variabilità dei profili

Si rimanda al documento CPS.

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.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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 attraverso la tecnologia Entrust.

6.1.1.2. Titolari

La generazione delle chiavi viene effettuata sulle stazioni di lavoro dei titolari o sulla stazione di lavoro della RA, nel rispetto di 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

Si rimanda al documento CPS.

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 l'autocertificato della chiave pubblica della CA.

6.1.5. Dimensione delle chiavi

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

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

6.1.6. Generatore delle chiavi

Le chiavi possono essere generate da moduli software o da dispositivi hardware, come indicato nel documento CPS.

6.1.7. Utilizzo dei certificati

Per limitare l'utilizzo dei certificati alle singole tipologie definite al punto 1.3.6.2 è utilizzata l'estensione *KeyUsage* .secondo quanto 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

La copia della chiave privata deve essere mantenuta segreta ed in forma cifrata.

Il recovery della chiave privata di cifratura viene effettuato per il tramite di un addetto della CA.

Il recovery dei profili utenti viene effettuato mediante un processo di certificazione semplificata.

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

Notifica di recovery della chiave privata di cifratura o di recovery del profilo utente deve essere inoltrata al titolare e al suo Referente alle Abilitazioni in forma elettronica o cartacea.

6.2.3. Backup delle chiavi private

Non è effettuata la copia delle chiavi private della CA.

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. Quest'ultima funzione è indispensabile per decifrare file dopo che dalla loro cifratura sia trascorso un tempo tale da aver comportato la sostituzione della coppia di chiavi di cifratura del titolare.

Per le chiavi private dei titolari viene effettuata una copia di backup.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

6.2.4. Deposito delle chiavi private

Non viene effettuato il deposito delle chiavi private di sottoscrizione.

6.2.5. Archiviazione delle chiavi private di cifratura

Si rimanda al punto 4.6

6.2.6. 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.

6.2.7. Disattivazione della chiave privata/profilo utente

La disattivazione della chiave privata deve essere una componente di un processo di logout. Il logout deve avvenire automaticamente a fronte del periodo di inattività stabilito nel documento CPS.

6.2.8. Distruzione della chiave privata

Si veda il documento CPS.

6.3. Altri aspetti di gestione delle chiavi

6.3.1. Archiviazione delle chiavi pubbliche

Si rimanda al punto 4.6.

6.3.2. Ciclo di vita delle coppie di chiavi

Si rimanda al documento CPS.

Le procedure di Fail-Over presenti in questo documento si distinguono in:

- Verifica dei requisiti del sistema di Disaster&Recovery in base a quanto stabilito dal presente documento
- Restore dei dati/configurazioni, in modo da ricreare un ambiente parallelo a quello di produzione.
- Validazione del sistema, consistente in test sistemistici ed applicativi

La procedura di restore è da considerarsi "a freddo": 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. Tale procedura richiede pertanto l'applicazione di un'attenta procedura di restore e verifica.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

Nel caso in cui, per un determinato applicativo, non sia presente una base dati da "ripristinare", la procedura consisterà nel solo porting dei dati di configurazione dell'applicativo stesso (parametri di configurazione).

6.4. Sicurezza dei computer

Il sistema operativo dei sistemi di elaborazione utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati e 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 devono essere protetti tramite firewall configurati in modo tale da accettare solamente i protocolli ed i comandi richiesti per i servizi offerti dalla CA.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

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.

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

Si rimanda al documento CPS.

7.3. Utilizzo dell'estensione basic constraints

Si rimanda al documento CPS.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

7.4. Profilo della CRL

La CRL è del tipo X.509 v2, o successivi aggiornamenti, ed è conforme a RFC 2459 PKIX 1 o successivi aggiornamenti.

Per ulteriori dettagli si rimanda al documento CPS.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

8. AMMINISTRAZIONE DELLE POLICY

8.1. Nuove policy

E' consentita l'emissione di nuovi documenti CP a fronte di tipologie di certificati, di titolari, di applicazioni per le quali siano utilizzabili i certificati non previste dalle policy già emesse.

E' consentito assegnare un nuovo codice identificativo alle policy modificate qualora l'impatto delle variazioni fosse di natura rilevante.

8.2. Variazione delle policy

8.2.1. Elementi modificabili senza preavviso

Sul presente documento CP è possibile effettuare solo le seguenti modifiche:

- Editoriali
- Correzioni tipografiche
- Riferimenti a persone o organizzazioni

8.2.2. Elementi modificabili con preavviso

- Ogni elemento presente in questo documento può essere modificato con 90 giorni di preavviso
- Variazioni ad elementi che non hanno un impatto sostanziale sull'infrastruttura PKI possono essere effettuate con 30 giorni di preavviso.
- 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
- I titolari

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

8.2.4. Periodo utile per ricevere commenti

Le informazioni di commento da parte delle entità interessate possono pervenire:

- entro 45 giorni nel caso di variazioni di cui al punto 8.2.1

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.

- entro 15 giorni nel caso di variazioni di cui al punto 8.2.2

8.2.5. 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.

I commenti ricevuti archiviati secondo quanto definito al punto 4.6.

8.2.6. Applicazione delle correzioni

L'applicazione di eventuali correzioni pervenute dalle entità coinvolte non richiede una ulteriore notifica delle variazioni.

Questo documento contiene informazioni di proprietà di Enel SpA e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di Enel SpA.