Aggiornamento dell'Infrastruttura per l'Utilizzo dei Certificati Digitali

Certification Practice Statement

Codice Documento: NPKI-CPS-A-00

Terna

Controllo del documento

Identificazione documento

Nome documento:	NPKI-CPS-A-00

Stato delle Revisioni

Rev.n°	Motivo della Revisione	Data
0.1	Revisione generale	01/09/2010
0.0	Prima stesura	24/05/2008

Approvazione ed emissione

		Data	Firma
Redatto da:	Daniele Guida Fabio De Sanctis		
Verificato da:	Pasquale Vaccaro		
Approvato da:	Pasquale Vaccaro Fabio De Sanctis		

Archiviazione

L'archiviazione di questo documento segue le regole di seguito specificate nell'ambito del capitolo che riguarda il Piano della Configurazione.

Controllo delle copie

Documento elettronico controllato. Ogni copia cartacea deve essere confrontata con l'originale elettronico prima dell'uso.

INDICE

1. Riferimenti 8

2. Definizioni ed acronimi 9

Introduzione 12

2.1. Sommario 12

2.2. Identificazione 12

2.3. Entità e applicabilità 12

2.3.1. Certification Authority (CA) 12

2.3.2. Registration Authority (RA) 12

2.3.3. Titolari 12

2.3.4. Applicabilità 12

2.4. Riferimenti 12

2.4.1. Organizzazione 12

3. Condizioni generali 13

3.1. Obblighi 13

3.1.1. Obblighi della CA 13

3.1.2. Obblighi della RA 14

3.1.3. Obblighi delle aziende interessate alla PKI TERNA 14

3.1.4. Obblighi dei titolari 14

3.1.5. Obblighi delle CA in cross certification 14

3.1.6. Obblighi di altre entità 14

3.1.7. Obblighi relativi alla Directory 14

3.2. Garanzie e limitazioni di responsabilità 15

3.2.1. Responsabilità della CA 15

3.2.2. Responsabilità della RA 15

3.3. Responsabilità finanziaria 15

3.4. Interpretazione e competenze legislative 15

3.5. Tariffe 15

3.6. Pubblicazione e repository 15

3.6.1. Pubblicazione di informazioni 15

3.6.2. Frequenza di aggiornamento delle informazioni pubblicate 15

3.6.3. Controllo di accesso 15

3.6.4. Directory 15

3.7. Verifiche di conformità alle norme 16

3.7.1. Frequenza 16

3.7.2. Identità e qualifica dei controllori 16

3.7.3. Relazioni tra i controllori e l'infrastruttura PKI 16
3.7.4. Processi e sistemi soggetti al controllo 16
3.7.5. Azioni da intraprendere in caso di inadempienza 17
3.7.6. Comunicazione dei risultati 17
3.8. Policy di riservatezza 17
3.9. Copyright e leggi sulla proprietà intellettuale 17
4. Identificazione e autenticazione 18
4.1. Registrazione iniziale 18
4.1.1. Nomi assegnabili 18
4.1.2. Significatività dei nomi 18
4.1.3. Regole per l'interpretazione dei nomi 18
4.1.4. Univocità dei nomi 18
4.1.5. Risoluzione di conflitti sui nomi 18
4.1.6. Proprietà dei marchi di fabbrica 18
4.1.7. Prova di possesso della chiave privata 18
4.1.8. Identificazione delle organizzazioni 18
4.1.9. Identificazione delle singole entità 18
4.2. Emissione Certificati di Autenticazione 19
4.3. Emissione Certificati di Firma e cifra 19
4.3.1. Richiesta di rinnovo dei certificati 19
4.4. Recovery delle chiavi private di cifra e del profilo utente 19
4.4.1. Richiesta di recovery da parte del titolare 19
4.4.2. Richiesta di recovery da parte di terzo interessato 19
4.5. Richiesta di revoca dei certificati 20
4.6. Richiesta di sospensione dei certificati 20
5. Requisiti gestionali 21
5.1. Richiesta dei certificati 21
5.1.1. Utenti Esterni 21
5.1.2. Utenti Interni 21
5.2. Emissione dei certificati dei Titolari 21
5.3. Accettazione dei certificati 22
5.4. Revoca dei certificati 22
5.4.1. Motivazioni per la revoca 22
5.4.2. Entità idonee alla richiesta di revoca dei certificati 22
5.4.3. Procedura per la richiesta di revoca dei certificati 23
5.4.4. Periodo di tempo per elaborare le richieste di revoca 23
5.4.5. Motivazioni per la sospensione 23
5.4.6. Entità idonee alla richiesta di sospensione 24
5.4.7. Procedure per la richiesta di sospensione 24

5.4.8. Durata massima della sospensione dei certificati 24
5.4.9. Frequenza di emissione della CRL e loro disponibilità 24
5.5. Procedure di verifica e controllo 24
5.5.1. Tipi di eventi registrati 24
5.5.2. Analisi dei log 25
5.5.3. Conservazione dei log 25
5.5.4. Protezione dei log 25
5.5.5. Copia di riserva dei log 25
5.5.6. Raccolta dei record di log 25
5.5.7. Notifica ai soggetti che hanno causato eventi critici 25
5.5.8. Valutazione delle vulnerabilità 25
5.6. Informazioni archiviate 25
5.6.1. Tipi di informazioni archiviate 25
5.6.2. Periodo di conservazione degli archivi 26
5.6.3. Protezione degli archivi 26
5.6.4. Copie di riserva degli archivi 26
5.6.5. Indicazione del tempo nei record di log 26
5.6.6. Procedura per verificare ed ottenere informazioni archiviate 26
5.7. Rinnovo delle chiavi 26
5.7.1. Rinnovo delle chiavi dei titolari 26
5.7.2. Rinnovo delle chiavi della CA 26
5.8. Procedure di emergenza e disaster recovery 27
5.8.1. Gestione dei disastri ambientali 27
5.8.2. Compromissione della chiave della CA 27
5.8.3. Guasti HW e SW 28
5.9. Termine dell'attività della CA 28
6. Sicurezza ambientale, procedurale e del personale 29
6.1. Sicurezza ambientale 29
6.1.1. Luoghi ed edifici 29
6.1.2. Accesso fisico 29
6.1.3. Energia elettrica, cablaggi di rete e condizionamento dell'aria 30
6.1.4. Esposizione all'acqua 30
6.1.5. Misure di prevenzione e protezione dagli incendi 30
6.1.6. Dispositivi di memorizzazione 30
6.1.7. Gestione dei rifiuti 30
6.1.8. Salvataggi in altri luoghi 30
6.2. Sicurezza procedurale 30
6.2.1. Profili 31
6.2.2. Numero di persone necessarie per azione 31

6.2.3. Riconoscimento degli addetti 31
6.3. Sicurezza sul personale 31
6.3.1. Addetti 32
6.3.2. Qualifiche ed esperienza 32
6.3.3. Formazione 32
6.3.4. Frequenza degli aggiornamenti 32
6.3.5. Sequenza e variabilità dei profili 32
6.3.6. Sanzioni per azioni non autorizzate 32
6.3.7. Documentazione 32
7. Sicurezza tecnica 33
7.1. Generazione e memorizzazione delle chiavi 33
7.1.1. Generazione delle chiavi 33
7.1.2. Rilascio della chiave privata al titolare 33
7.1.3. Rilascio della chiave pubblica di firma alla CA 33
7.1.4. Rilascio della chiave pubblica della CA ai titolari 33
7.1.5. Dimensione delle chiavi 33
7.1.6. Generatore delle chiavi 33
7.1.7. Utilizzo dei certificati 33
7.2. Protezione delle chiavi private 34
7.2.1. Standard per il modulo di cifratura 34
7.2.2. Gestione delle chiavi private 34
7.2.3. Key escrow delle chiavi private di sottoscrizione 34
7.2.4. Backup delle chiavi private 34
7.2.5. Archiviazione delle chiavi private 34
7.2.6. Inserimento della chiave privata nei moduli crittografici 34
7.2.7. Attivazione della chiave privata 34
7.2.8. Disattivazione della chiave privata 35
7.2.9. Distruzione della chiave privata 35
7.3. Altri aspetti di gestione delle chiavi 35
7.3.1. Archiviazione delle chiavi pubbliche 35
7.3.2. Ciclo di vita delle coppie di chiavi 35
7.4. Dati di attivazione 35
7.4.1. Generazione dei dati di attivazione e installazione 35
7.4.2. Activation Data Protection 36
7.5. Sicurezza dei computer 36
7.6. Sicurezza della rete 36
8. Certificati e CRL 37
8.1. Profilo dei Certificati dei Titolari della CA 37
8.2. Profilo della CRL 37

9. Amministrazione delle policy 38
9.1. Nuovi Practice Statements 38
9.2. Variazione delle CPS 38
9.2.1. Elementi modificabili senza preavviso 38
9.2.2. Elementi modificabili con preavviso 38
9.2.3. Notifica delle variazioni 38
9.2.4. Periodo utile per ricevere commenti 38
9.2.5. Gestione dei commenti 38
9.2.6. Applicazione delle correzioni 38
Appendice A: Verifica della validità dei certificati 38

1. Riferimenti

La seguente tabella elenca i principali documenti in ingresso al progetto:

Codice	Titolo/Documento/Informazione	Autore
n.a.	g1_formato_del_certificato_x509v3_rev.1.0.pdf	n.a.
n.a.	g2_direcory_x500_rev.1.0.pdf	n.a.
n.a.	g3_processi_e_ruoli_rev.1.0.pdf	n.a.
n.a.	i1_architettura_pki_rev.1.0.pdf	n.a.
n.a.	i2_architettura_web_rev.1.0.pdf	n.a.
n.a.	i3_architettura_ras_rev.1.0.pdf	n.a.
n.a.	i4_entrust_windows2000.rev.1.0.pdf	n.a.
n.a.	s1_installazione_configurazione_backup_restore_rev.1.0.pdf	n.a.
n.a.	s2_schede_tecniche_ambienti_esercizio_collaudo_rev.1.0.pdf	n.a.
n.a.	s3_hardening_rev.1.0.pdf	n.a.
n.a.	s4_integrazione_oracle_entrust_rev.1.0.pdf	n.a.
n.a.	s5_attivazione_plugin_autenticazione_oracle_applications_rev.1.0.pdf	n.a.
n.a.	u1_componenti_client_rev.2.1.pdf	n.a.
n.a.	u2_procedure_per_generazione_certificati_rev.2.0.pdf	n.a.
n.a.	u3_installazione_direct_client_rev.2.0.pdf	n.a.
n.a.	u4_manuale_utente_desktop_solutions_rev.2.0.pdf.	n.a.
n.a.	CP-GRTN-0.3.doc	n.a.
n.a.	CPS-GRTN-0.1.doc	n.a.
Modalità_Richiesta_Certificato_Digitale	Accesso alle applicazioni informatiche di TERNA e modalità per la richiesta del certificato digitale	TERNA
NPKI-TC-A-03	Profilo dei Certificati	TERNA
NPKI-CP-A-01	Certificate Policy	TERNA
NPKI-CVT-A-00	Procedure di Gestione dei Profili crittografici degli Utenti e delle Applicazioni.	SA

2. Definizioni ed acronimi

Di seguito l'elenco delle definizioni:

Definizione	Significato
Autocertificato	Certificato della chiave pubblica della CA firmato con la corrispondente chiave privata.
certification authority o certificatore	Entità che esegue il processo di certificazione, rilascia il certificato della chiave pubblica, lo rende eventualmente disponibile insieme a quest'ultima e gestisce le liste di revoca (CRL).
certificato	Risultato di un processo mediante il quale la chiave pubblica del titolare ed altre informazioni vengono associate univocamente al titolare della chiave privata corrispondente, l'autenticità e l'integrità di tale associazione vengono assicurate tramite la firma digitale da parte della CA.
chiave privata	Elemento della coppia di chiavi destinato ad essere utilizzato e conosciuto dal solo soggetto titolare.
chiave pubblica	Elemento della coppia di chiavi destinato ad essere reso pubblico.
chiavi di certificazione	Chiavi utilizzate dalla CA ai fini della generazione e verifica delle firme apposte ai certificati e alle liste di revoca (CRL).
chiavi di cifratura	Coppia di chiavi utilizzate dall'operazione di cifratura per rendere segrete delle informazioni.
chiavi di marcatura temporale	Chiavi destinate alla generazione e verifica delle marche temporali.
chiavi di sottoscrizione	Coppia di chiavi destinate alla generazione ed alla verifica di firme digitali.
coppia di chiavi	Insieme costituito dalla chiave pubblica e dalla chiave privata ad essa associata.
cross certification accordo di mutua certificazione	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.
documento di policy	Il presente documento. Esso consiste in un insieme di regole, contraddistinto da un codice, che indica se è possibile utilizzare determinati certificati o determinate marche temporali nell'ambito di specifiche comunità o classi di applicazioni aventi comuni esigenze di sicurezza.
documento di practice statement	Documento che riporta le procedure utilizzate dalla CA per emettere, gestire e revocare i certificati e per emettere e gestire le marche temporali.
Entità	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.
Marca Temporale	Risultato di una procedura informatica con cui si attribuiscono ad uno o più documenti informatici una data ed un orario opponibili ai terzi. Una marca temporale attesta che un certo dato era esistente al momento indicato nella marca temporale stessa.
operazione di cifratura	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	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.
profilo utente	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	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	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 responsabile può afferire a più titolari.
registration authority	Entità responsabile dell'identificazione e dell'autenticazione delle entità. Non firma o emette certificati.
Security policy (SP)	Insieme delle regole e norme che definiscono e regolamentano le misure di sicurezza con cui un sistema o un'organizzazione protegge le proprie risorse critiche o riservate. Si considerano normalmente tre livelli di Security Policy: • Strategico (o aziendale) in cui vengono date le direttive generali; • di Settore o di Sistema, ad esempio: SP per la Direzione del Personale, per il sistema PKI; • specifiche, ad esempio per le password, per la privacy della posta elettronica.
Sistema di Validazione Temporale (Time Stamp Server – TSS)	Sistema in grado di produrre marche Temporali.
Time Stamp Token	Marca Temporale.
Timestamp Server Authority (TSA)	Fornitore affidabile di servizi crittografici (Trusted Cryptographic Service Provider) che emette Marche Temporali tramite uno o più TSS.
Titolare	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.

Di seguito l'elenco delle sigle e delle abbreviazioni utilizzate:

Sigla	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)"
CA	Certification Authority	
CAST	Algoritmo di cifratura .	RFC 2144
CPS	Certification Practice Statement	
CP	Certificate Policy	
Crittografia	Lo studio delle tecniche per mantenere sicure le informazioni. Due comuni applicazioni sono la cifratura e la firma digitale	Cryptography links kept at Counterpane Systems
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	
DISP	Directory Information Shadowing Protocol	ISO/IEC 9594-1 ISO/IEC 9594-9
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	RFC 1777 – RFC 2251
NIST	National Institute for Standards and Technology	http://csrc.nist.gov

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/
RFC	Request For Comments. Il metodo utilizzato da IETF per pubblicare documenti	
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	RFC 2313
SSL	Secure Sockets Layer. Protocollo di cifratura e d autenticazione per le connessioni Internet	Hickman, Kipp, "The SSL Protocol", Netscape Communications Corp., Feb 9, 1995. A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.
SP	Security Policy	
TLS	Transport Layer Security. La versione standard di SSL	RFC 2246
URI	Uniform Resource Identifier	RFC 2396
URL	Uniform Resource Locator. Metodo per identificare una risorsa in Internet.	RFC 1738, 1808, 2368, 2396
URN	Uniform Resource Name. Utilizzato come identificatore di risorsa indipendentemente dalla sua locazione.	RFC 2141
WG	Working Group. Usually used with reference to the IETF.	
X.400	Specifiche per client di posta e relativi server.	CCITT Recommendations X.400-X.430: Message Handling Systems
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.	ITU-T Recommendation X.509 (1997), ISO/IEC 9594-8:1997, Information technology - Open Systems Interconnection - The Directory: Authentication framework.
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 draft, 1998.

Introduzione

2.1. Sommario

Il presente documento riporta l'insieme di procedure operative non riservate, applicate all'interno dell'infrastruttura PKI di TERNA per l'emissione di certificati digitali.

2.2. Identificazione

Il presente documento è identificato dal seguente nome file: **NPKI-CPS-A-01**

2.3. Entità e applicabilità

Questa CPS si applica alle entità specificate nell'analogo capitolo della CP di riferimento.

2.3.1. Certification Authority (CA)

Nessuna disposizione aggiuntiva rispetto a quanto indicato nell'analogo capitolo della CP di riferimento.

2.3.2. Registration Authority (RA)

Nessuna disposizione aggiuntiva rispetto a quanto indicato nell'analogo capitolo della CP di riferimento.

2.3.3. Titolari

Nessuna disposizione aggiuntiva rispetto a quanto indicato nell'analogo capitolo della CP di riferimento.

2.3.4. Applicabilità

I certificati emessi dalla infrastruttura a chiave pubblica di TERNA sono utilizzabili nell'ambito delle applicazioni specificate nel capitolo corrispondente delle Certificate Policy di riferimento.

2.4. Riferimenti

2.4.1. Organizzazione

Le policy qui definite, la loro gestione, aggiornamento e 'interpretazione è affidata alla responsabilità di:
TERNA - Sicurezza Aziendale
Via Galbani 70
00156 ROMA
Telefono: +39-06-83138384
Fax: +39-06- 83138267
e-mail: pki@TERNA.it
Indirizzo di reperibilità della directory: ldap://ldap.terna.it

3. Condizioni generali

Questa sezione specifica in dettaglio quali siano gli obblighi e le responsabilità della Certification Authority, della Registration Authority, dei titolari, delle CA con cui siano in atto rapporti di mutua certificazione e di chiunque faccia uso dei certificati emessi dalla CA di TERNA per la cifratura, la firma elettronica e l'autenticazione.

3.1. Obblighi

3.1.1. Obblighi della CA

La CA di TERNA opera nel rispetto di quanto definito all'analogo capitolo della CP di riferimento.

La CA opera nei confronti degli utenti tramite la RA, pertanto eventuali obblighi che richiedano il contatto diretto tra titolare e CA sono espletati dalle RA.

Identificazione delle entità

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.
Tale operazione è di norma delegata alle Registration Authority e avviene come indicato al punto 0.

Informativa agli utenti

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.
Tali informazioni sono disponibili sia in forma cartacea presso le RA che in formato elettronico presso l'indirizzo http://www.terna.it/ServizidiCertificazione/

Emissione dei certificati

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

Gestione dei certificati

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

Revoca e sospensione dei certificati

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

Obblighi riguardo le CA in cross certification

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.
La PKI TERNA prima di stipulare un accordo di cross certification con un'altra CA ne verifica l'adeguatezza alle proprie esigenze di sicurezza e di applicabilità dei certificati. Saranno oggetto di esame oltre alle Certificate Policy e al Certification Practice Statement, anche le politiche di sicurezza, almeno per la parte consentita dalle misure di riservatezza aziendale, purché tale parte sia sufficiente ad effettuare una valutazione di merito.

Analoga verifica, per motivi di reciprocità, viene consentita alle persone a ciò incaricate dall'altra CA, che dovranno sottoscrivere un impegno a non divulgare le informazioni acquisite durante questo processo.

Le CA che hanno stipulato accordi di mutua certificazione con la CA di TERNA si impegnano per iscritto a rispettare tutte le norme e procedure interne riconosciute equivalenti alla presente. Analogo impegno viene sottoscritto, per reciprocità, dalla CA di TERNA.

La CA di TERNA informa tempestivamente le CA con cui esistano accordi di mutua certificazione delle modifiche alle CP e alla CPS e delle variazioni organizzative di loro interesse, come risulterà dagli accordi stessi.

La CA verifica periodicamente che le CA certificate si attengano alla misure concordate.

Alla data di stesura del presente documento non esistono relazioni di cross in essere con altre certification authority.

Altri adempimenti

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.1.2. Obblighi della RA

La RA opera nel rispetto della delega ricevuta dalla CA e in ottemperanza a quanto definito nella CP di riferimento e nel presente CPS.
La RA inoltre deve:

- custodire in modo sicuro il profilo contente le credenziali per l'accesso agli applicativi di RA
- notificare l'attivazione del processo di recovery delle chiavi o del profilo utente con la consegna al titolare dei codici di attivazione
- rendere disponibile la propria struttura alle verifiche di conformità da parte della CA

3.1.3. Obblighi delle aziende interessate alla PKI TERNA

Le aziende interessate alla PKI TERNA, siano esse società terze che controllate o partecipate, devono:

- informare i titolari sugli obblighi e le responsabilità inerenti l'uso delle chiavi e dei certificati, indicando dove reperire la documentazione relativa, che deve essere letta prima di inoltrare la richiesta di certificazione
- autorizzare i titolari, che ne abbiano diritto, ad effettuare la richiesta di certificato
- identificare i titolari che possono ricevere il secondo codice di attivazione
- attivare il processo di revoca dei certificati di un titolare nei casi seguenti:
    - uso delle chiavi e dei certificati non conforme alle regole e che possa recare danno all'infrastruttura
    - cessazione del rapporto di lavoro
    - delega da parte del titolare che non è in grado di richiedere la revoca personalmente

Le aziende interessate alla PKI TERNA possono inoltre richiedere su loro iniziativa i certificati per i titolari loro afferenti.

3.1.4. Obblighi dei titolari

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.1.5. Obblighi delle CA in cross certification

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.1.6. Obblighi di altre entità

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.1.7. Obblighi relativi alla Directory

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.2. Garanzie e limitazioni di responsabilità

3.2.1. Responsabilità della CA

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

Garanzie

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

Limitazioni

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.2.2. Responsabilità della RA

Garanzie

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

Limitazioni

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.3. Responsabilità finanziaria

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.4. Interpretazione e competenze legislative

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.5. Tariffe

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.6. Pubblicazione e repository

3.6.1. Pubblicazione di informazioni

I certificati di cifra e le CRL sono reperibili dalla directory X.500 accessibile tramite i protocolli LDAPv3:

- dalla Intranet aziendale all'indirizzo **ldap://ldap.terna.it**
- da rete pubblica all'indirizzo **ldap://ldap.terna.it**

Il presente documento CPS e la CP di riferimento sono consultabili tramite protocollo http all'indirizzo http://www.terna.it/ServizidiCertificazione/

3.6.2. Frequenza di aggiornamento delle informazioni pubblicate

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.6.3. Controllo di accesso

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.6.4. Directory

La Directory di TERNA è conforme con lo standard ISO 9594-1 (ITU-T X.500) e gli altri standard della famiglia ISO 9594.
L'indirizzo a cui è accessibile la Directory è specificato ai capitoli precedenti.

La master copy è custodita all'interno di una rete sicura, inaccessibile dall'esterno.
Un numero di copie slave, mirrored dalla master, sono accessibili con I protocolli indicati di seguito.
Dall'esterno della rete pubblica:

1. LDAPv3 – RFC 2251

La replica dei dati e dello schema tra la directory master e le relative slave è il DISP.
Sul sito di produzione sono previste 4 copie della Directory Master due visibili dalla rete intranet ed altrettante dalla rete Internet

3.7. Verifiche di conformità alle norme

Le verifiche di conformità alle norme hanno lo scopo di valutare l'operatività del sistema per stabilire se se esso è costantemente adeguato alle esigenze dell'organizzazione e a quanto definito nel presente CPS e nelle relative CP

3.7.1. Frequenza

Le verifiche di conformità dei processi e dei sistemi della CA avvengono con le seguente cadenza per i vari tipi di verifica indicati al paragrafo 3.7.4:

- Ogni mese per i processi indicati ai punti 1, 2;
- Ogni sei mesi per i processi indicati ai punti 3, 5;
- Ogni anno per i processi indicati ai punti 4, 6.

Al verificarsi di eventi significativi, che possano essere ricondotti ad inadempienza del personale addetto o a cattivo funzionamento dei sistemi, possono essere effettuate verifiche estemporanee.
Ispezioni a scopo di audit possono essere eseguite anche da addetti delle CA con le quali sono in atto accordi di mutua certificazione, se ciò è previsto dagli accordi.

3.7.2. Identità e qualifica dei controllori

Nella tabella seguente viene riportata una sintesi delle figure organizzative responsabili dell'attività di audit

Direzione	Approva i piani di audit interno ed esterno
Responsabile della sicurezza	Pianifica le attività di audit interno ed esterno in accordo con il Responsabile dell'Auditing
	Rileva le necessità di eseguire audit interni ed esterni non programmati ma necessari a fronte di esigenze contingenti, e si fa carico di inserirli nel Piano delle verifiche.
Responsabile Auditing	Pianifica, in accordo con il Responsabile della Sicurezza, le attività di audit interno ed esterno e redige il relativo piano da sottoporre all'approvazione della Direzione
	Individua, informandone il responsabile della Sicurezza, il personale a cui assegnare gli incarichi di valutatori (auditors) e tra questi sceglie un Team leader
Responsabile dell'entità valutata	Assicura la propria collaborazione per una corretta ed efficace chiusura dell'audit
	Sottoscrive il verbale di chiusura e il report dell'audit

3.7.3. Relazioni tra i controllori e l'infrastruttura PKI

Il responsabile dell'Auditor e le persone da lui identificate non ricoprono ruoli operativi per tutte le componenti dell'infrastruttura PKI.

3.7.4. Processi e sistemi soggetti al controllo

Sono previste ispezioni di controllo periodico almeno per i seguenti elementi:

1. Integrità del log
2. Contenuto del log

3. Conformità alle procedure seguenti
    1. Policy di riservatezza (capitolo 3.8)
    2. Identificazione e autenticazione (capitolo 0)
    3. Requisiti gestionali (capitolo 5)
    4. Sicurezza ambientale, procedurale e del personale (Capitolo 5)
    5. Sicurezza tecnica (capitolo 6)
    6. Certificati e CRL (capitolo 7)
    7. Amministrazione delle policy (capitolo 8)Sicurezza ambientale, procedurale e del personale (Capitolo 6)
4. Operatività dei sistemi di back up
5. Rispondenza delle configurazioni degli HW e SW dei sistemi della PKI, dei firewall, con quelle previste
6. Verifiche a carico dei titolari:
    1. criteri di conservazione e protezione del profilo,
    2. custodia della password di sblocco
    3. conservazione dei dispositivi hardware di firma.

Le CA con le quali siano in atto accordi di mutua certificazione,potranno essere oggetto di verifiche da parte di incaricati di TERNA al fine di accertare la corretta applicazione delle procedure concordate, con le frequenze eventualmente previste negli accordi.

3.7.5. Azioni da intraprendere in caso di inadempienza

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.7.6. Comunicazione dei risultati

I risultati delle azioni di verifica e di controllo saranno comunicati al responsabile della PKI e al responsabile della sicurezza e saranno considerati riservati e gestiti secondo quanto definito al punto 3.8

3.8. Policy di riservatezza

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

3.9. Copyright e leggi sulla proprietà intellettuale

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

4. Identificazione e autenticazione

Questa sezione descrive le procedure impiegate presso la CA o la RA per l'identificazione e l'autenticazione di tutte le entità coinvolte nei processi seguenti:

1. Registrazione iniziale ed emissione del certificato
2. Rinnovo dei certificati
3. Recovery delle chiavi
4. Revoca dei certificati
5. Sospensione dei certificati

4.1. Registrazione iniziale

Nella fasi di registrazione iniziale i dati dei futuri titolari di certificato vengono immessi in modo sicuro sul Data Base della CA utilizzando la console di Amministrazione della Certification Authority stessa.

4.1.1. Nomi assegnabili

Il campo *subject* del certificato è costituito da una stringa di nomi X.500, valorizzato secondo quanto indicato nel documento di Policy dei Certificati di cui al documento "NPKI-TC-A-03"

4.1.2. Significatività dei nomi

I nomi vengono assegnati in modo da identificare in maniera univoca il titolare ed avere una ragionevole associazione con la persona fisica, casi di omonimia vengono risolti con l'uso del codice fiscale a cui viene aggiunto un numero sequenziale per identificare profili multipli assegnati allo stesso titolare.

4.1.3. Regole per l'interpretazione dei nomi

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

4.1.4. Univocità dei nomi

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

4.1.5. Risoluzione di conflitti sui nomi

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

4.1.6. Proprietà dei marchi di fabbrica

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

4.1.7. Prova di possesso della chiave privata

Durante il processo di richiesta ed emissione del certificato la CA esegue automaticamente la verifica del possesso della chiave privata, il controllo viene fatto secondo le procedure indicate nello standard RFC 2510 dal protocollo del PKIX-CMP.

4.1.8. Identificazione delle organizzazioni

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

4.1.9. Identificazione delle singole entità

Autenticazione degli addetti alla CA e alla RA

Gli addetti alla CA e alla RA sono organizzati come segue:

1. I Master User sono addetti all'installazione, configurazione e attivazione della PKI, si autenticano al sistema mediante user-name e password. Sono responsabili della configurazione di tutti i servizi di CA e attivano personalmente la creazione del primo Security Officer, che prende il nome di First Officer. Il First Officer alla fine delle operazioni di inizializzazione dell'ambiente è revocato.
2. I Security Officer sono titolari di certificati digitali con cui si autenticano agli applicativi di RA, certificati emessi dalla CA e associati al profilo di amministratori.
3. Gli Administrators e gli Auditor sono titolari di certificati digitali per l'autenticazione agli applicativi di RA.

Autenticazione dei titolari

I titolari, siano essi dipendenti di TERNA, di società controllate o di clienti o fornitori, per ottenere un certificato, devono richiedere l'autorizzazione al loro incaricato, che ha il compito di fare da garante presso il responsabile del servizio di certificazione.
Il titolare che è stato autorizzato, riceverà i codici di attivazione mediante modalità di consegna sicure (e.g. attraverso l'uso di due canali di consegna diversi come Posta Elettronica e Posta Tradizionale).

4.1.10. Emissione Certificati di Autenticazione

I processi di autorizzazione sono descritti nella documentazione disponibile sul Portale di Certificazione.

4.1.11. Emissione Certificati di Firma e cifra

I certificati di cifra e firma vengono emessi contestualmente ai certificati di autenticazione, non necessitano perciò di una procedura di identificazione/autenticazione apposita.

4.2. Richiesta di rinnovo dei certificati

È previsto che i certificati per i titolari interni siano rinnovati automaticamente prima della loro scadenza. Il processo viene attivato in modo trasparente al primo login che il titolare fa al proprio profilo, durante l'intervallo di rinnovo e viene condotto in accordo con il protocollo standard RFC2510
Se l'utente non esegue mai il login, nell'intervallo di rinnovo, il certificato scade e non può essere rinnovato automaticamente. In questo caso tutti i certificati associati al profilo del titolare scadono e quest'ultimo deve seguire la procedura di recovery.

4.3. Recovery delle chiavi private di cifra e del profilo utente

Il recovery delle chiavi private di cifra e del profilo può essere richiesto sia dal titolare che dal suo responsabile, secondo le modalità descritte nei punti seguenti.

4.3.1. Richiesta di recovery da parte del titolare

I processi di autorizzazione sono descritti nella documentazione disponibile sul Portale di Certificazione

4.3.2. Richiesta di recovery da parte di terzo interessato

Il terzo interessato (responsabile del titolare, o altra persona indicata nello specifico accordo), può richiedere il recovery delle chiavi di un suo sottoposto.
La procedura avviene nel modo seguente:

1. L'incaricato invia una richiesta alla casella del responsabile dei certificati in cui specifica le motivazioni della richiesta.
2. L'operatore dopo aver verificato la validità della richiesta e l'effettiva sua abilitazione a tale richiesta, attiva il processo di recovery con la generazione dei codici di recovery

3. Si possono qui avere due casi diversi:
4. il recovery è fatto dal titolare o dal terzo interessato:
5. Uno dei codici viene inviato cifrato all'incaricato e l'altro al titolare
6. Il titolare si reca a ritirare il secondo codice dal terzo interessato che lo deve identificare
7. il recovery è fatto dal terzo interessato (ad esempio per poter decifrare documenti di un titolare non più dipendente dell'azienda): i due codici di attivazione vengono inviati al terzo interessato.

4.4. Richiesta di revoca dei certificati

I processi di autorizzazione sono descritti nella documentazione disponibile sul Portale di Certificazione.

4.5. Richiesta di sospensione dei certificati

I processi di autorizzazione sono descritti nella documentazione disponibile sul Portale di Certificazione.

5. Requisiti gestionali

5.1. Richiesta dei certificati

Le modalità di richiesta dei certificati sono differenti e dipendono dalla tipologia del titolare.
I titolari si dividono in:

1. Utenti Esterni
2. Utenti Interni

5.1.1. Utenti Esterni

Il processo autorizzativi per l'emissione dei certificati esterni sono descritti nella documentazione disponibile sul Portale di Certificazione.

5.1.2. Utenti Interni

Il processo di registrazione degli utenti interni sono sono descritti nella documentazione disponibile sul Portale di Certificazione.

5.2. Emissione dei certificati dei Titolari

L'emissione dei certificati segue un'unica procedura indipendentemente dalla tipologia dell'utente e dal numero di certificati previsti per ogni titolare
L'emissione di un certificato ha come prerequisito la registrazione presso la CA delle informazioni riguardanti l'utente e l'abilitazione alla richiesta da parte del responsabile dei certificati.
Il titolare, una volta in possesso dei due codici:

1. Si collega al portale del certificatore, esegue il download dell'applet di emissione (l'applet svolge le stesse operazioni del client fisico non richiedendo alcuna componente Entrust installata sulle postazioni di lavoro)
2. L'applet presenta al titolare la maschera di richiesta i codici che permettono di realizzare l'autenticazione con la CA, conformemente allo standard RFC 2510.
3. L'applet genera la coppia di chiavi di autentica. Questa operazione può essere eseguita tramite l'applet o tramite un dispositivo hardware, tipicamente una smart-card interfacciabile con le CAPI di Microsoft;
4. l'applet invia alla portale del certificatore la richiesta di certificazione della chiave pubblica in formato RFC 2511 o RFC 2314 o RFC 2986.
5. il portale inoltra la richiesta di certificazione alla Certification Authority

La CA :

6. genera la coppia di chiavi di cifra, della cui chiave privata conserva una copia, protetta in modo da essere attivabile solo dalla CA o dal titolare, per poter effettuare il recovery
7. alla ricezione della chiave pubblica di firma inviata dal titolare, esegue la prova del possesso; se questa termina con esito positivo, genera i certificati di cifra e di firma e li invia al titolare insieme con il proprio certificato. Al titolare viene inviata in modo sicuro su un canale di comunicazione cifrato anche la chiave privata di cifra.
8. Se la prova del possesso non va a buon fine la CA non rilascia i certificati e ne dà avviso al titolare sotto forma di messaggio di errore.

Il processo di emissione della chiave di firma è speculare a quello della chiave di autentica

Al termine del processo il titolare interno sarà in possesso di tre coppie di chiavi e dei relativi certificati quello esterno di due coppie di chiavi e relativi certificati.
La CA inoltre provvede a:

1. Pubblicare il certificato di cifra sulla directory X.500
2. A rendere i codici di attivazione non utilizzabili.

Qualora il titolare riceva segnalazione di una certificazione abusiva deve provvedere a richiedere la revoca del certificato alla RA che informa l'incaricato interessato.

5.3. Accettazione dei certificati

Alla ricezione dei certificati, il titolare ha l'obbligo di controllare l'esattezza delle informazioni ivi riportate e in caso di discordanza con i dati dichiarati deve procedere alla revoca immediata del certificato

5.4. Revoca dei certificati

5.4.1. Motivazioni per la revoca

La revoca di un certificato deve essere richiesta se si verifica una delle condizioni indicate al corrispondente capitolo della CP di riferimento.
L'incaricato può richiedere la revoca dei certificati dei titolari a lui sottoposti per ogni caso che a suo giudizio abbia carattere di urgenza.
Ai certificati revocati viene assegnato un codice di revoca (CRLReason) che viene inserito nella CRL e serve per identificare la motivazione.
I codici utilizzati dalla PKI di TERNA fanno parte dello standard X.509 e sono:

1. Key Compromise: indica la compromissione della chiave privata
2. CA Compromise: indica la compromissione della chiave privata della CA
3. Unspecified: raccoglie tutte le motivazioni non comprese nelle precedenti quattro
4. CessationOfOperation: cessazione dell'attività dalla CA

Nel caso di compromissione della chiave privata del titolare (CRLReason: Key Compromise), viene anche richiesto di indicare la data in cui si era certi che la chiave fosse ancora valida; questo si riflette nella valorizzazione della extension invalidityDate della entry di CRL relativa al certificato in questione).
Vengono utilizzati solo i codici sopra elencati per non violare la privacy dei titolari.

5.4.2. Entità idonee alla richiesta di revoca dei certificati

Possono richiedere la revoca dei certificati:

1. il titolare
2. una terza parte eventualmente indicata negli accordi interaziendali
3. la RA
4. la CA

Nella tabella seguente è indicato chi può richiedere la revoca, in quali casi e se la revoca è di tipo urgente ("U") o normale ("N").

Motivazione	Titolare	RA	CA
Recovery del profilo o aggiornamento dei certificati		N	
Compromissione della chiave privata o perdita di controllo del dispositivo di firma	U	U	U
Dati del certificati obsoleti o errati	U + N	U + N	U + N
Cessazione dall'incarico per cui è stato rilasciato il certificato	U + N	U + N	U + N
Violazione degli obblighi del titolare		U	U
Compromissione della chiave della CA			U
Cessazione dell'attività della CA			N

5.4.3. Procedura per la richiesta di revoca dei certificati

La procedura per la richiesta della revoca è distinta in base all'identità di chi la effettua.
I tempi per dare seguito alla richiesta sono indicati nei paragrafi di competenza.
Notifica dell'avvenuta revoca deve essere inoltrata al titolare e a chi ha presentato la richiesta.

Revoca richiesta dal titolare

Il titolare può richiedere la revoca dei propri certificati nei casi indicati nella tabella al capitolo precedente.
La richiesta deve essere gestita in accordo a quanto descritto nella documentazione disponibile sul Portale di Certificazione.:
L'operatore deve:

1. verificare la correttezza delle informazioni contenute nella richiesta
2. eseguire la revoca.
3. in caso di revoca urgente, richiedere l'emissione immediata della CRL.

Revoca inoltrata da terze parti

Ove esplicitamente previsto dagli accordi, la richiesta di revoca dei certificati di un titolare può essere inoltrata alla RA da una terza parte, che adduca valide motivazioni quali:

1. accertata compromissione della chiave privata del titolare
2. provato utilizzo dei certificati e delle chiavi non conforme alle policy

La richiesta deve essere presentata presso gli uffici della RA, l'operatore ha l'obbligo di verificare l'identità del richiedente mediante i meccanismi concordati sulla base di specifici accordi o secondo quanto indicato nella documentazione disponibile sul Portale di Certificazione.

Revoca attivata dalla RA

La RA, ove giunga a conoscenza dei casi previsti nella tabella di cui al capitolo 5.4.2, provvede ad attivare la procedura di revoca (Urgente o Normale), compilando l'apposito modulo di revoca.
Deve in seguito dare comunicazione dell'avvenuta revoca al titolare e al relativo incaricato tramite un messaggio di posta firmato.

Revoca attivata dal responsabile dei certificati

Il responsabile dei certificati può revocare i certificati di tutti i titolari, siano essi utenti finali o incaricati, in tutti i casi urgenti previsti nel punto 5.4.1.
Deve in seguito darne comunicazione al titolare e al relativo incaricato tramite un messaggio di posta.

5.4.4. Periodo di tempo per elaborare le richieste di revoca

Nei casi in cui la richiesta di revoca abbia carattere di urgenza, deve essere verificata ed eseguita nel più breve tempo possibile e comunque entro 1 (una) ora dal momento in cui viene presentata alla RA o al responsabile dei certificati.
Nei casi non urgenti, la richiesta deve essere soddisfatta entro un arco di tempo sufficiente a far comparire l'informazione nella CRL che verrà pubblicata successivamente al momento della presentazione della richiesta.
Qualora la richiesta pervenga nell'ultima ora prima della pubblicazione della successiva CRL, la revoca potrà slittare alla CRL ancora successiva. In questo caso, se il richiedente la revoca non richiede anche la valorizzazione dell'extension "invalidityDate", in quest'ultima sarà indicato il momento della richiesta.

5.4.5. Motivazioni per la sospensione

In aggiunta a quanto indicato all'analogo capitolo della CP di riferimento si specifica che la sospensione è una particolare forma di revoca in cui il ReasonCode è onHold.

5.4.6. Entità idonee alla richiesta di sospensione

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

5.4.7. Procedure per la richiesta di sospensione

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

5.4.8. Durata massima della sospensione dei certificati

In aggiunta a quanto indicato all'analogo capitolo della CP di riferimento, si specifica che la sospensione può avere una durata massima di 30 giorni lavorativi, trascorsi i quali senza comunicazione diversa, viene attuato quanto previsto nella CP di riferimento.

5.4.9. Frequenza di emissione della CRL e loro disponibilità

In aggiunta a quanto indicato all'analogo capitolo della CP di riferimento, si specifica che nel caso di revoche urgenti può essere richiesta l'emissione immediata della CRL. In tal caso questa avverrà nel più breve tempo possibile e si inserirà nella numerazione progressiva senza alterare la normale periodicità di emissione programmata in origine.
Le liste di revoca vengono scaricate collegandosi alla directory X.500 tramite il protocollo LDAPv3, il software in dotazione ai titolari è in grado di collegarsi direttamente alla directory. Le CRL saranno disponibili anche su protocollo http sia da rete Internet che da rete Intranet. Le CRL saranno disponibili anche su protocollo http sia da rete Internet che da rete Intranet.

5.5. Procedure di verifica e controllo

5.5.1. Tipi di eventi registrati

In aggiunta alle informazioni indicate all'analogo capitolo della CP di riferimento, al fine di permettere la verifica ed il controllo di tutte le operazioni svolte all'interno dell' infrastruttura, esse vengono opportunamente registrate in file di log, generati automaticamente dalla CA stessa.
Eventi esterni che non coinvolgono direttamente la CA vengono registrati autonomamente dai sistemi interessati.

Eventi del software CA

Gli eventi registrati dal software della CA sono relativi sia all'accesso fisico che logico a tutte le componenti del sistema, essi vengono classificati in base al livello di criticità in:

- *"log"*: è il livello minimo, correlato alle attività normali (per esempio: richiesta di certificato, emissione di una nuova CRL);
- *"event"*: è il livello intermedio, legato ad eventi non usuali o comunque ad eventi per cui sono richieste una o più autorizzazioni e che, pur non essendo causa di allarme, vanno verificati per controllarne la legittimità;
- *"alarm"*: è il massimo livello ed è relativo ad eventi critici: tentativi di eseguire operazioni non autorizzate o malfunzionamenti HW o SW.

Ad ogni evento è sia associato un codice identificativo che l'identità dell'operatore che ha autorizzato l'operazione.
La CA verifica e controlla direttamente i seguenti insiemi di eventi:

1. Attivazione e chiusura dei servizi della CA
2. Eventi di creazione, modifica, rimozione, disattivazione, attivazione, e ripristino dei profili dei titolari
3. Eventi di creazione, modifica, rimozione, disattivazione, attivazione e recovery di profili relativi a personale addetto alla CA
4. Eventi di generazione, aggiornamento e recovery delle chiavi
5. Eventi di creazione, aggiornamento revoca e recovery dei certificati

6. Esecuzione di backup e restore degli archivi della CA
7. Esecuzione di backup, restore e cancellazione dei log
8. Operazioni di manutenzione del sistema programmate e non
9. Aggiornamenti hardware e software

Eventi registrati al di fuori del controllo del software della CA

Vengono registrati i seguenti eventi:

1. Aggiornamenti del software: automatico per alcuni eventi, manuale per altri;
2. Manutenzione programmata ed estemporanea dei sistemi e dei locali: automatico per alcuni eventi, manuale per altri
3. Accesso ai locali: automatico nei casi in cui si utilizzano controlli accessi automatici, manuale negli altri
4. Giornale di bordo del personale incaricato della vigilanza: idem
5. Variazione del personale che ricopre i ruoli di gestione della PKI; manuale

5.5.2. Analisi dei log

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP.

5.5.3. Conservazione dei log

I log sono conservati in accordo alle politiche di backup in esercizio presso TERNA.

5.5.4. Protezione dei log

I record sono numerati progressivamente, e riportano la data e l'istante della loro registrazione, sono inoltre protetti da eventuali modifiche successive alla loro registrazione tramite MAC o firma digitale.
La verifica dell'integrità dei file di log viene fatta automaticamente dal sistema ad ogni accesso in lettura da parte di un operatore.
L'integrità dei log provenienti da sistemi diversi da quello della CA è garantita da procedure operative adeguate.
L'accesso ai log è protetto fisicamente mediante la conservazione in armadi a cura dello specifico responsabile.

5.5.5. Copia di riserva dei log

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP.

5.5.6. Raccolta dei record di log

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP.

5.5.7. Notifica ai soggetti che hanno causato eventi critici

Oltre alla registrazione sui file di log, il sistema segnala immediatamente all'operatore quando l'esecuzione di una operazione non va a buon fine, indicando anche la possibile causa del malfunzionamento.

5.5.8. Valutazione delle vulnerabilità

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP.

5.6. Informazioni archiviate

5.6.1. Tipi di informazioni archiviate

A maggior dettaglio di quanto indicato all'analogo capitolo della CP la CA archivia e conserva i seguenti tipi di informazioni:

1. Dati relativi ai titolari forniti all'atto della registrazione dell'utente.
2. Documentazione cartacea od elettronica sottoscritta al momento della richiesta o del rilascio di un certificato
3. Richieste di recovery di chiavi e profili, richieste di revoca o sospensione
4. Chiavi di cifra degli utenti
5. Certificati emessi
6. Documenti di cross certificazione

5.6.2. Periodo di conservazione degli archivi

I dati di back della Certification Authority sono conservati per 10 anni.
La documentazione cartacea viene conservata per 10 anni.
I documenti di cross certificazione vengono conservati per 10 anni.

5.6.3. Protezione degli archivi

La protezione delle informazioni di tipo cartaceo e degli archivi elettronici è garantita dalle normali policy di sicurezza e procedure già predisposte in azienda.
I certificati, le chiavi e le CRL archiviati sono protetti tramite cifratura con meccanismi implementi direttamene dal prodotto di CA scelto.

5.6.4. Copie di riserva degli archivi

Il database contenente le informazioni registrate viene sottoposto a backup completo una volta al giorno. Sono prodotte 2 copie di backup di cui la prima conservata presso il sito di produzione, la seconda presso il sito di Disaster Recovery. inoltre mensilmente una ulteriore copia di backup del sito di produzione viene archiviata in armadio ignifugo.
Le informazioni cartacee sono redatte originariamente in duplice / triplice copia, le copie vengono conservate in archivi separati.

5.6.5. Indicazione del tempo nei record di log

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

5.6.6. Procedura per verificare ed ottenere informazioni archiviate

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento

5.7. Rinnovo delle chiavi

5.7.1. Rinnovo delle chiavi dei titolari

In aggiunta a quanto specificato all'analogo capitolo della CP di riferimento, si specifica che in caso cui il profilo sia memorizzato su dispositivo crittografico e nel caso di malfunzionamento di quest'ultimo, il titolare, una volta attivato il recovery del profilo su un nuovo dispositivo, curerà la distruzione di quello guasto. Qualora si tratti di una smart card provvederà a tagliare il chip. Il dispositivo distrutto verrà consegnato al Responsabile dei dispositivi crittografici che dovrà verificarne la reale inutilizzabilità.

5.7.2. Rinnovo delle chiavi della CA

Le chiavi della CA vengono rinnovate periodicamente almeno ogni 10 anni, 3 mesi prima della loro effettiva scadenza, e in caso di guasto del dispositivo di firma, guasto che comunque non derivi da tentata o riuscita manomissione delle chiavi.

Il processo di rinnovo consiste nella generazione di una nuova coppia di chiavi e nell'emissione e pubblicazione sulla directory di tre nuovi certificati:

1. Certificato contenente la nuova chiave pubblica, firmato con la nuova chiave privata
2. Certificato contenente la nuova chiave pubblica firmato con la vecchia chiave privata
3. Certificato contenente la vecchia chiave pubblica firmato con la nuova chiave privata

Si tratta di un processo di cross-certification che permette di dare validità alle nuove chiavi come eredi delle vecchie, senza interrompere la catena di fiducia.
In ognuno dei certificati il campo "Issuer" contiene sempre lo stesso distinguished name mentre l'authoritykeyIdentifier è specifico per ogni coppia di chiavi, perché è dato dall'impronta SHA-1 della chiave pubblica della CA, questo consente di risalire lungo la catena delle sostituzioni e identificare sempre la chiave pubblica corretta per la verifica dei certificati.
La procedura viene eseguita dalla medesima tipologia di persone indicata al capitolo 0 e ne viene redatto un verbale firmato dai presenti e conservato dall'auditor.

5.8. Procedure di emergenza e disaster recovery

TERNA ha sviluppato procedure di emergenza e disaster recovery, di cui vengono indicate le informazioni non riservate e comunque non soggette a variazioni frequenti. Del documento di disaster recovery sono depositate copie su carta nei punti strategici per la gestione dell'emergenza.
I principali casi di disastro contemplati sono i seguenti:

1. Gestione dei disastri ambientali
2. Compromissione della chiave della CA;
3. Guasti Hardware and software;

5.8.1. Gestione dei disastri ambientali

Il piano di disaster recovery di TERNA prevede siti di backup.
Di seguito un breve elenco delle fasi per previste per i fail back.

1. Gestione dell'emergenza – le CRL già emesse continuano ad essere disponibili; l'emissione di nuove CRL e di nuovi certificati può essere ritardata fino al ritardo massimo indicato all'analogo capitolo della CP di riferimento, se è necessario attivare il macchinario di backup;
   Quanto sopra non si applica in casi di catastrofi di estrema gravità ed ampiezza. In tali situazioni saranno operative specifiche Operational Security Policies.
2. Gestione del transitorio – le funzionalità saranno normalmente operative sulle apparecchiature principali o su quelle di back up; in quest'ultimo caso si attiveranno le attività per riportare le operazioni sul macchinario principale, sia esso quello originale o un altro sostitutivo;
3. Ripristino della operatività normale – il macchinario originale o un altro sostitutivo diventeranno regolarmente operativi.

Per attuare il piano sono stati redatti manuali estremamente dettagliati per riattivare i servizi su nuove apparecchiature che normalmente possono diventare operative nel tempo indicato all'analogo capitolo della CP di riferimento.
I dati personali conservati su supporti che possano essere trafugati nel periodo immediatamente al disastro sono cifrati.

5.8.2. Compromissione della chiave della CA

Se la chiave di firma dei certificati viene compromessa si procede alla sua revoca e verrà generata una nuova coppia di chiavi di certificazione come indicato ai capitoli precedenti. I certificati emessi con la chiave compromessa verranno revocati per CACompromise.
La revoca del certificato della CA rende automaticamente non validi anche tutti i certificati da lei emessi.
In caso di revoca per compromissione la CA deve notificare per iscritto (o con altro mezzo) l'accaduto a tutti i titolari e ai responsabili delle CA con cui esistono accordi di cross certificazione, e, nel caso intenda riprendere l'attività di certificazione, deve indicare le modalità di proseguimento della stessa.

Qualora si proceda alla generazione di una nuova coppia di chiavi, verranno emessi di nuovo anche tutti i certificati utente attivi al momento della revoca e ancora validi e i certificati di mutua certificazione.

5.8.3. Guasti HW e SW

Nel caso di guasti HW o SW si applica un opportuno sottoinsieme delle misure di recovery descritte ai paragrafi precedenti.

5.9. Termine dell'attività della CA

Nel caso in cui la CA smetta di erogare il servizio di certificazione deve:

1. informare per iscritto, con l'anticipo previsto all'analogo capitolo della CP di riferimento, sulla data prevista di cessazione dell'attività i responsabili delle CA con cui esistono accordi di mutua certificazione e i titolari dei certificati; questi ultimi per e-mail e, ove previsto esplicitamente dagli accordi, per posta ordinaria;
2. comunicare se è stato predisposto che l'attività di certificazione venga rilevata da un'altra CA e indicare i termini di tale subentro;
3. indicare in ogni caso quale organizzazione conserverà la documentazione fino a scadenza, le modalità con cui sono resi disponibili gli archivi e per quanto tempo dopo la cessazione dell'attività verranno mantenuti;
4. revocare tutti i certificati ancora validi al momento della cessazione dell'attività
5. generare e pubblicare l'ultima CRL che dovrà rimanere accessibile alla consultazione almeno finché non sarà trascorsa la scadenza naturale di tutti i certificati revocati;
6. distruggere le chiavi di firma della CA.

Tutte le operazioni saranno effettuate in presenza delle persone previste per la generazione delle chiavi della CA e verrà redatto un verbale, firmato dai presenti, che sarà conservato dalla organizzazione subentrante.

6. Sicurezza ambientale, procedurale e del personale

6.1. Sicurezza ambientale

6.1.1. Luoghi ed edifici

Tutti i sistemi informatici dei servizi di certificazione si trovano in un'area protetta, il cui accesso è limitato solo ad un gruppo ristretto di operatori e viene controllato da sistemi di sicurezza operanti con continuità .
I locali si trovano in un edificio controllato 24 ore su 24 da un circuito di telecamere collegato alla centrale operativa di emergenza.

Sede principale

L'edificio esterno è cinto da un perimetro invalicabile, gli unici punti di ingresso sono protetti da porte a bussola attivabili con l'uso di un apposito tesserino magnetico, dotate di vetri antisfondamento e controllo del peso.
I locali dove sono installati i server, all'interno della sede sopra individuata, sono chiusi, senza affacci verso l'esterno, con accesso controllato, dotato di aria condizionata le cui caratteristiche, così come quelle delle condutture elettriche e dei cablaggi di rete.
I locali dei server sono dotati delle misure antincendio, sono sotto allarme e le pareti sono antisfondamento.

6.1.2. Accesso fisico

L'accesso all'edificio principale è sorvegliato da guardie giurate che consentono l'ingresso secondo le seguenti regole:

1. Presentazione del tesserino aziendale da parte dei dipendenti interni di TERNA
2. Riconoscimento e registrazione del personale interno che si trovi sprovvisto del tesserino e consegna di un tesserino provvisorio
3. Nel caso di persone in visita, presentazione di un documento di identità valido, registrazione delle credenziali e del nominativo della persona che riceve la visita e rilascio di un tesserino temporaneo. Il visitatore una volta all'interno dell'edificio dovrà essere accompagnato dal dipendente che riceve la visita.

CA

L'accesso alla sala macchine è consentito solo al personale autorizzato. L'accesso è controllato da tesserino magnetico, smart/card.
Nei locali ad accesso riservato non deve essere presente un solo operatore alla volta.
Il personale che esegue manutenzione straordinaria deve essere scortato e sorvegliato per tutto il tempo di permanenza all'interno dei locali riservati da personale autorizzato in modo permanente.
L'ingresso e l'uscita dai locali viene registrata, manualmente e le registrazioni vengono controllate periodicamente.

RA

Le RA durante l'orario di ufficio operano in locali che non prevedono meccanismi di controllo degli accessi aggiuntivi rispetto a quelli utilizzati per l'accesso all'edificio principale.
Le protezioni che devono essere implementate sui dispositivi in dotazione alle RA sono i seguenti:

1. il computer della RA non deve essere utilizzato da altre persone se non sotto il controllo diretto del titolare e da personale autorizzato, nel caso si eseguano operazioni di manutenzione
2. è previsto il log-out automatico dall'applicativo nel caso non vengano eseguite operazioni per un periodo di tempo prestabilito

3. vengono utilizzati strumenti che permettono di bloccare ed evidenziare tentativi di intrusione nel sistema
4. si usano accorgimenti particolari per evidenziare tentativi di manomissione dell' hardware dei computer
5. la smart/card e il relativo lettore vengono custoditi separatamente durante i periodi di inutilizzo
6. la password di sblocco del profilo è protetta da accessi non autorizzati

È inoltre disposta l'installazione di software anti-virus che deve essere aggiornato periodicamente.

Titolari

I titolari sono responsabili personalmente della custodia dei dispositivi e degli applicativi a loro affidati, devono proteggere le password per l'accesso al profilo, senza trascriverla su supporti liberamente accessibili o comunque conservandola in modo che sia leggibile solo dal titolare.
Qualora le chiavi siano memorizzate su supporti esterni (es.floppy disk) questi ultimi non devono essere lasciati incustoditi all'interno del lettore o comunque depositati in luoghi facilmente accessibili.
Gli applicativi che fanno uso delle chiavi sono programmati in modo tale da eseguire il log-out automatico dopo alcuni minuti di inattività da parte dell'utente, questo per evitare l'uso non autorizzato nel caso il computer sia lasciato incustodito.
È inoltre disposta l'installazione di software anti-virus che deve essere aggiornato periodicamente.

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

In aggiunta a quanto esposto all'analogo capitolo della CP di riferimento, le procedure di sicurezza e di manutenzione della rete elettrica e di condizionamento dell'aria sono conformi alle procedure aziendali già previste in materia.

6.1.4. Esposizione all'acqua

Si rimanda integralmente a quanto esposto all'analogo capitolo della CP di riferimento.

6.1.5. Misure di prevenzione e protezione dagli incendi

Descrivere brevemente le misure antincendio, le frequenze dei controlli dei dispositivi

6.1.6. Dispositivi di memorizzazione

I dispositivi utilizzati per la memorizzazione delle informazioni conservate dalla CA e dalla RA vengono mantenuti in locali ad accesso controllato e in condizioni ambientali idonee. La loro gestione è fatta a partire dalle procedure di acquisto, volte ad ottenere supporti esenti da virus di qualsiasi tipo, fino allo smaltimento che prevede la smagnetizzazione o la distruzione fisica, a seconda del supporto.

6.1.7. Gestione dei rifiuti

Le procedure per lo smaltimento della documentazione cartacea contenente informazioni sensibili sono conformi alle procedure aziendali già previste in materia .

6.1.8. Salvataggi in altri luoghi

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

6.2. Sicurezza procedurale

Sono indicate di seguito le regole utilizzate per l'attribuzione delle responsabilità tra gli addetti alla gestione della PKI, vengono definiti i ruoli e il numero di autorizzazioni richieste per l'esecuzione delle diverse operazioni

6.2.1. Profili

Profili per la CA

Esistono più profili funzionali tra i quali sono suddivise le responsabilità legate alla gestione della CA, per attivare le operazioni più delicate alcuni di essi devono operare contemporaneamente:

- Responsabile della sicurezza
- Responsabile della generazione e custodia delle chiavi della CA
- Responsabile della generazione dei certificati
- Responsabile della gestione del registro dei certificati
- Responsabile della registrazione degli utenti
- Responsabile della sicurezza dei dati
- Responsabile dell'auditing

Alcuni di questi profili funzionali possono essere assegnati alla stessa persona, secondo quanto indicato nella tabella seguente:

Attribuzioni / Profili	sicurezza	gener. & cust. Chiavi	generaz. Certificati	gest. reg. certificati	registr. Utenti	sicur. Dati	auditing
Sicurezza	X				----	----	----
Gener. & cust. Chiavi		X	Sì		----	Sì	----
Generazione Certificati		Sì	X			Sì	
Gest. reg. certificati				X	Sì	Sì	
Registr. Utenti				Sì	X	Sì	
Sicur. Dati		Sì	Sì	Sì	Sì	X	
Auditing							X

6.2.2. Numero di persone necessarie per azione

Per lo svolgimento di alcune delle funzioni della CA è necessaria la presenza di più persone, nella tabella seguente viene specificato il numero massimo di autorizzazioni richieste per le operazioni critiche associate al ruolo indicato.

Ruolo	N. di persone abilitate	N. minimo di persone necessarie contemporaneamente
Master User	3	1
First Officer	1	1
Security Officer	5	2
Directory administrator	3	--

6.2.3. Riconoscimento degli addetti

Gli addetti alla CA si autenticano alla PKI secondo quanto indicato ai paragrafi precedenti

6.3. Sicurezza sul personale

In aggiunta a quanto disposto all'analogo capitolo della CP di riferimento si applicano le seguenti disposizioni.
Al personale addetto alla PKI non possono essere assegnate mansioni incompatibili con il rispettivo incarico di PKI, in ottemperanza alle regole seguenti:

1. una mansione non deve controllare l'altra;

2. una mansione non deve essere in grado di limitare l'esecuzione dell'altra;
3. le due mansioni non devono congiuntamente controllarne una terza;
4. al personale della PKI non possono essere assegnati altri incarichi estranei alla PKI in contrasto con gli incarichi di PKI.

Al momento dell'assegnazione dell'incarico gli addetti alla PKI devono dichiarare per iscritto di essere stati informati compiutamente dei propri doveri e delle relative responsabilità, dei ruoli per i quali sono responsabili e delle conseguenze di eventuali mancanze.

6.3.1. Addetti

Il personale addetto alla gestione della PKI è controllato dai propri responsabili all'interno della struttura organizzativa aziendale. I responsabili non sono autorizzati alla esecuzione delle attività assegnate al personale addetto.

6.3.2. Qualifiche ed esperienza

Gli addetti alla CA e alla RA vengono scelti tra indicare la qualifica all'interno dell'organigramma della società dei diversi addetti, in base a quali criteri viene assegnata (anni di esperienza, titoli di studio ecc) e quali responsabilità comporta.
Oltre alle qualifiche indicate al punto precedente, gli addetti alla CA e RA hanno maturato una esperienza di almeno 5 anni nella conduzione di sistemi informativi aziendali e hanno seguito dei corsi di formazione specifici sulla gestione del sistema di PKI implementato

6.3.3. Formazione

Le competenze del personale addetto alla CA e alla LRA, vengono arricchite mediante periodici corsi di aggiornamento in funzione dei ruoli ricoperti e riguardanti in particolare le seguenti aree:

1. utilizzo delle componenti software della PKI
2. utilizzo delle componenti hardware utilizzate dalla PKI, compresi i dispositivi crittografici.
3. misure di sicurezza da adottare in funzione del proprio profilo
4. procedure operative indicate in questo documento
5. procedure da seguire in caso di emergenza.

6.3.4. Frequenza degli aggiornamenti

I corsi di aggiornamento sono programmati annualmente in funzione della variabilità dei ruoli e degli aggiornamenti all'infrastruttura stessa e verranno attivati sia presso le sedi di TERNA che presso enti esterni.

6.3.5. Sequenza e variabilità dei profili

Per evitare che la permanenza di un addetto nello stesso ruolo possa creare, in caso di assenza del personale, difficoltà di gestione all'infrastruttura, i profili vengono fatti ruotare con frequenza annuale.
La tabella seguente mostra i criteri di scambio che possono essere applicati:

6.3.6. Sanzioni per azioni non autorizzate

Le sanzioni per azioni non autorizzate sono definite dal responsabile del personale nell'ambito delle proprie responsabilità.

6.3.7. Documentazione

Gli addetti alla CA e alla RA sono forniti di tutta la documentazione che espone in modo dettagliato le norme impiegate nei processi che li vedono coinvolti: manuali dei prodotti, CP, CPS, procedure specifiche, piano delle situazioni di emergenza.

7. Sicurezza tecnica

Questa sezione descrive le misure di sicurezza adottate dalla Certification Authority di TERNA per la protezione delle chiavi, dei certificati e di tutte le informazioni utilizzate nell'attività di certificazione

7.1. Generazione e memorizzazione delle chiavi

7.1.1. Generazione delle chiavi

CA

Le chiavi della CA vengono generate alla presenza di almeno 2 operatori, Master User o Security Officer, che devono abilitare la procedura autenticandosi al sistema.
La chiavi private sono memorizzate sul DB della Certification Authority in modo cifrato
Il verbale della procedura viene firmato dai presenti e conservato dall'auditor.

Titolari

I titolari generano personalmente dalla propria postazione di lavoro la coppia di chiavi di firma e di autentica, la chiave privata viene conservata nel profilo dell'utente protetta tramite cifratura.
I titolari possono memorizzare il proprio profilo su File o all'interno del dispositivo crittografico (e.g. Smart Card).
Le chiavi di cifra vengono generate dalla CA che conserva una copia della chiave privata a scopo di recovery, questa copia è memorizzata cifrata nel database della CA. Le chiavi private di cifra vengono poi inviate in modo sicuro al client del titolare che le registra nel dispositivo di firma.

7.1.2. Rilascio della chiave privata al titolare

La CA rilascia la chiave privata di cifra al titolare trasferendola all'interno del profilo; la chiave viene inviata su un canale di comunicazione protetto, secondo il protocollo indicato nell' RFC 2510.
Il canale viene creato al momento dell'autenticazione del titolare alla PKI.

7.1.3. Rilascio della chiave pubblica di firma alla CA

La chiave pubblica di firma del titolare viene inviata alla CA lungo il canale protetto già indicato al punto precedente, all'interno della richiesta di certificazione, secondo il protocollo indicato nell' RFC 2510.

7.1.4. Rilascio della chiave pubblica della CA ai titolari

La chiave pubblica della CA ed il relativo auto-certificato vengono propagati tramite i meccanismi i propagazione messi a disposizione del Dominio Microsoft o pubblicati sul portale del certificatore.

7.1.5. Dimensione delle chiavi

Le dimensioni delle chiavi della CA e dei titolari sono riportate nel documento NPKI-TC-A-03

7.1.6. Generatore delle chiavi

Le chiavi della CA vengono generate tramite applicativo software.
Le coppie di chiavi di firma dei titolari possono essere memorizzate o su file o su dispositivi crittografici quali Smart Card. Nel caso di uso di dispositivi questi dovranno essere certificati ITSEC.

7.1.7. Utilizzo dei certificati

Di norma in ogni certificato viene indicato lo specifico utilizzo che deve esserne fatto, secondo quanto indicato nella Certificate Policy associata, mediante la valorizzazione delle "Limitazioni d'uso" e dell'estensione *keyUsage.* I valori che può assumere sono riportati nel documento NPKI-TC-A-03.

7.2. Protezione delle chiavi private

7.2.1. Standard per il modulo di cifratura

Tutte le operazioni di cifratura effettuate dalla CA, dalla RA e dai titolari sono effettuate tramite moduli software o dispositivi hardware.

7.2.2. Gestione delle chiavi private

L'attivazione delle chiavi di firma della CA avviene secondo un meccanismo "m di n" del tipo dello Shamir Shared Scheme basato sull'immissione di password da parte degli addetti.
Il recovery delle chiavi di cifra e del profilo dei titolari si rende necessario nei casi seguenti:

1. Il titolare dimentica la password di sblocco del profilo
2. Il profilo è danneggiato o non è più utilizzabile perché scaduto
3. L'eventuale smart-card su cui sono memorizzate le chiavi è stata danneggiata o smarrita

Il recovery deve essere richiesto dal titolare o dal suo incaricato secondo le modalità indicate in precedenza.
La RA consegna al titolare i nuovi codici di attivazione, con cui avviare il processo di recovery, questo consiste in:

1. generazione di una nuova coppia di chiavi di firma da parte del titolare
2. emissione del nuovo certificato di firma da parte della CA .
3. invio al titolare da parte della CA della storia delle sue chiavi private di cifra (*key history*)
4. ricostruzione del profilo del titolare

Nel caso ci sia il sospetto che la password di sblocco o il profilo siano in possesso di un entità diversa dal titolare, è necessario procedere alla revoca dei certificati prima di effettuare il recovery, in questo caso sarà generata dalla CA una nuova coppia di chiavi di cifra, che verrà inviata al titolare insieme alla *key history*.

7.2.3. Key escrow delle chiavi private di sottoscrizione

Le chiavi private di firma sono in possesso esclusivamente del titolare, per garantire il non ripudio, non deve esserne fatta perciò nessuna copia.

7.2.4. Backup delle chiavi private

Per rendere possibile il recovery delle chiavi private di cifra dei titolari, la CA ne conserva una copia nel proprio database in una lista associata al titolare, detta *key history,*che contiente tutte le chiavi private dell'utente che si sono succedute nel tempo.
La *key history* è protetta tramite cifratura.e l'accesso è permesso solo alla CA e ai titolari ed esclusivamente durate il processo di key recovery.
Le chiavi private della CA non vengono duplicate, al verificarsi di qualsiasi evento che ne possa minacciare la segretezza, devono essere rinnovate e in casi estremi revocate.

7.2.5. Archiviazione delle chiavi private

Si faccia riferimento a quanto descritto ai paragrafi precedenti

7.2.6. Inserimento della chiave privata nei moduli crittografici

Nessuna ulteriore disposizione rispetto all'analogo capitolo della CP di riferimento.

7.2.7. Attivazione della chiave privata

Le chiavi private sono attivate in seguito all'accesso al profilo da parte del titolare (valido solo nel caso in cui il profilo è memorizzato su file).

La password inserita permette lo sblocco della credenziali, successivamente, se è disponibile il collegamento con la directory, viene verificata la validità dei certificati. Se anche questo controllo va a buon fine, il titolare è abilitato all'uso delle chiavi. In caso contrario il profilo non viene sbloccato.

7.2.8. Disattivazione della chiave privata

L'utilizzo della chiave privata viene disattivato quando il titolare si sconnette dal profilo valido solo nel caso in cui il profilo del titolare è memorizzato su file in formato proprietario Entrust (.epf)

La disattivazione avviene anche automaticamente dopo alcuni minuti di inattività, per evitare che le chiavi restino attive anche in assenza del titolare.

7.2.9. Distruzione della chiave privata

Dispositivo crittografico

Al termine della operatività di un dispositivo crittografico tipo smart-card, le chiavi private in esso memorizzate devono essere distrutte.
Si può procedere in due modi:

1. Reinizializzando il dispositivo crittografico
2. Distruggendo fisicamente la smart-card.

Profilo su disco del sistema utente

Nel caso in cui il profilo sia memorizzato sul disco fisso del sistema utente si deve procedere alla cancellazione sicura.

7.3. Altri aspetti di gestione delle chiavi

7.3.1. Archiviazione delle chiavi pubbliche

Le chiavi pubbliche ed i relativi certificati vengono conservati dalla CA secondo le procedure indicate in precedenza.

7.3.2. Ciclo di vita delle coppie di chiavi

Le chiavi della CA hanno un tempo di vita di 10 anni dopo i quali avviene il rinnovo automatico, il certificato auto-emesso associato alla chiave pubblica ha invece un tempo di vita di 7 anni.
Le chiavi private di cifra ed i relativi certificati hanno un tempo di vita di almeno 3 anni.
Le chiavi private di firma e di autentica hanno un tempo di vita di 2 anni ed il relativo certificato scade dopo 3 anni.
Il rinnovo di entrambe le coppie di chiavi avviene automaticamente, come indicato ai paragrafi precedenti.

7.4. Dati di attivazione

7.4.1. Generazione dei dati di attivazione e installazione

CA

Gli addetti alla CA di TERNA ricevono I codici di attivazione per installare almeno in due la CA.

Titolari

Ai titolari vengono comunicati in modo sicuro I codici con cui si autenticano alla CA nella fase di certificazione.

Durante il processo di certificazione i titolari scelgono una password di sblocco del dispositivo di firma, che potranno a loro piacimento modificare, con la quale attivarlo.

7.4.2. Activation Data Protection

Ogni entità della PKI, addetti alla CA, adotteranno tutte le misure per mantenere segreti I codici di attivazione.

7.5. Sicurezza dei computer

I sistemi di elaborazione utilizzati nell'attività di certificazione sono dislocati in locali protetti e ad accesso controllato
Il sistema operativo degli elaboratori utilizzati per la generazione delle chiavi è sottoposto a procedure di Hardening volte a limitare i servizi attivi sui sistemi
L'accesso agli applicativi da parte degli utenti è soggetto ad autenticazione forte tramite i certificati.

7.6. Sicurezza della rete

La protezione della rete di accesso alla CA e alla directory x.500, sono riportate nel documento di Architettura Fisica relativo all'intera infrastruttura PKI.

8. Certificati e CRL

8.1. Profilo dei Certificati dei Titolari della CA

Si faccia riferimento a quanto indicato nel documento “NPKI-TC-A-03”

8.2. Profilo della CRL

La CRL è conforme allo standard ITU-T X.509v3 , la versione è del tipo X.509 v2,
La extension reasonCode può essere impostata secondo quanto definito al punto 5.4.1 e solo per i seguenti CRLReason:

1. unspecified
2. keyCompromise
3. superseded
4. cessationOfOperation.

Nel caso di sospensione del certificato il reasonCode è :

5. onHold

È possibile inoltre valorizzare il campo invalidityDate, per indicare l’ultima data nella quale la chiave privata risultava non essere ancora compromessa. Esso può anche essere utilizzato come indicato al capitolo 5.4.4.

9. Amministrazione delle policy

9.1. Nuovi Practice Statements

Nuovi documenti CPS possono essere emessi a fronte di significative variazioni nelle modalità di emissione e gestione dei certificati, nella tipologia dei certificati stessi o nella organizzazione e gestione della PKI
I nuovi CPS verranno pubblicati allo stesso indirizzo dei precedenti e potranno aggiungersi o sostituire quelli già pubblicati, secondo il tipo di variazioni effettuate.

9.2. Variazione delle CPS

9.2.1. Elementi modificabili senza preavviso

Gli elementi che possono essere modificati senza che sia necessario darne preavviso ai titolari sono: Correzioni grafiche e ortografiche e modifiche alle persone di riferimento.

9.2.2. Elementi modificabili con preavviso

Se le modifiche apportate al presente CPS rendono necessaria la riemissione del documento, deve esserne dato preavviso entro i seguenti termini:

1. Modifiche alle procedure di gestione del ciclo di vita dei certificati: entro 10 giorni
2. Modifiche alla struttura organizzativa della PKI: entro 20 giorni
3. Modifiche al profilo dei certificati: entro 20 giorni

9.2.3. Notifica delle variazioni

I titolari, gli addetti alla PKI e i responsabili delle CA con cui sono in atto accordi di mutua certificazione devono ricevere notifica delle variazioni.
La notifica può avvenire tramite posta elettronica firmata, nella quale si deve indicare dove è possibile reperire gli aggiornamenti o il nuovo documento.

9.2.4. Periodo utile per ricevere commenti

Le entità interessate dalle variazioni possono inviare i propri commenti e suggerimenti alle persone responsabili.
I commenti devono prevenire entro due giorni dal termine del preavviso

9.2.5. Gestione dei commenti

I commenti alle modifiche vengono sottoposti all'attenzione dei responsabili dei documenti CPS e CP che hanno l'autorità di prendere in considerazione o meno i suggerimenti pervenuti.
I commenti verranno archiviati secondo le procedure indicate.

9.2.6. Applicazione delle correzioni

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

Appendice A: Verifica della validità dei certificati

Quando un utente verifica la validità di un certificato deve accertarsi che:

1. il certification path sia valido

2. il certificato non sia stato revocato o sia scaduto
3. Il *certification path* è costituito dai seguenti elementi che devono essere esaminati in sequenza da parte degli utenti :
    a. Auto-certificato della chiave pubblica della CA consegnato al titolare all'atto della certificazione
    b. certificati di cross certificazione tra la CA di TERNA e la CA che ha emesso il certificato da verificare.

A questi elementi in caso di rinnovo delle chiavi della CA, si aggiungono, conformemente all' RFC 2510, i seguenti certificati:

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

La verifica che il certificato di cifra non sia revocato avviene accedendo alla CRL presente sulla directory.
Si deve controllare che il momento indicato nel campo "nextUpdate" della CRL in esame non sia superato, cioè non sia anteriore al momento in cui si sta facendo la verifica.
Una firma digitale non va ritenuta affidabile qualora:

1. non sia possibile accedere ad una CRL valida, ossia di cui non sia possibile verificare la firma o che non sia scaduta, relativa al certificato associato alla firma digitale;
2. il certificato associato al documento firmato risulti scaduto e non sia possibile stabilire il momento di apposizione della firma;
3. il certificato associato al documento firmato risulti revocato e non sia possibile stabilire il momento di apposizione della firma
4. il certificato associato al documento firmato risulti revocato.