Aggiornamento dell'Infrastruttura per l'Utilizzo dei Certificati Digitali

Policy dei Certificati

Codice Documento: NPKI-CP-A-01

Controllo del documento

Identificazione documento

Nome documento:	NPKI-CP-A-01

Stato delle Revisioni

Rev.n°	Motivo della Revisione	Data
0.1	Revisione generale	01/09/2010
0.0	Prima stesura	27/12/2007

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. Scopo del documento

Il presente documento definisce i requisiti di sicurezza dell'infrastruttura PKI di TERNA S.p.A. nel rispetto dei quali i certificati emessi da TERNA possono essere utilizzati per garantire il non ripudio, l'autenticazione, l'integrità e la riservatezza dei dati scambiati tra entità che si avvalgono di tale PKI.

2. 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.
NPKI-TC-D-00a	Profilo dei Certificati	n.a.
NPKI-CPS-A-00a	Certificate Practice Statement	n.a.
NPKI-CVT-A-00	Procedure di Gestione dei Profili crittografici degli Utenti e delle Applicazioni.	SA

3. 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	
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	
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
TST	Time Stamp token	
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.

4. Introduzione

4.1. Sommario

Il presente documento di Policy (a cui di seguito si farà riferimento anche come CP) definisce le regole per l'applicabilità e l'utilizzo dei seguenti elementi da TERNA S.p.A.:

- Certificati di firma elettronica;
- Certificati di autentica;
- Certificati di cifratura;
- Certificati per il code signing;
- Certificati di autenticazione per procedure Applicative;
    - Certificati per accesso in VPN;
    - Certificati per MS Office Communication Server;
    - Certificati per applicazioni web based;
    - eccetera;
- Certificati di certificazione.

4.2. Identificazione

4.2.1. Identificatore alfanumerico

Il presente documento ha come identificatore alfanumerico: NPKI-CP-A-01

4.2.2. Identificatore oggetto

Policy OID: 1.3.76.41.1.1

4.3. Entità e applicabilità

La presente CP si applica:

1. alla CA di TERNA e cioè alle sue infrastrutture fisiche e logiche e al suo personale;
2. alle CA con cui TERNA abbia in vigore un accordo di mutua certificazione;
3. agli utenti a cui TERNA abbia rilasciato certificati in conformità con la presente CP;
4. a coloro che utilizzano i certificati rilasciati da TERNA in conformità con la presente CP per verificare l'autenticità e l'integrità di documenti a cui sia stata associata una firma elettronica supportata dai medesimi certificati.

Questa CP non si applica ad eventuali altri certificati o marche temporali emesse da TERNA sotto altre Policy.

4.3.1. Certification Authority (CA)

TERNA rilascia certificati al proprio personale dipendente ed ai dipendenti di società controllate o che utilizzano i servizi ed i sistemi di Terna stessa.
La Certification Authority provvede a:

- emettere i certificati degli addetti alla gestione dell'infrastruttura a chiave pubblica;
- emettere i certificati previsti dalle CP per gli utenti registrati e autorizzati;
- emettere i certificati previsti dalle CP per le applicazioni;
- pubblicare sulla directory i certificati delle chiavi pubbliche di cifra degli utenti;
- generare le coppie di chiavi di cifra e trasmettere in modo sicuro la chiave privata al titolare;

- mantenere una copia, protetta da accessi non autorizzati, delle chiavi private di cifra, a scopo di recovery;
- procedere al rinnovo delle chiavi secondo quanto previsto dalle rispettive CPS e dal presente CP;
- procedere al recovery dei profili utente, in caso di richiesta legittima del titolare, secondo quanto indicato nelle CPS e nel presente CP;
- generare e pubblicare le liste dei certificati revocati (CRL) con le modalità previste nel presente CP e nelle CPS.

La CA inoltre è responsabile di tutte le attività necessarie per garantire un corretto funzionamento della infrastruttura a chiave pubblica, deve quindi:

- garantire la sicurezza di tutti i sistemi hardware e software impiegati nel processo di certificazione;
- garantire la sicurezza delle reti su cui si appoggia la PKI;
- assicurare la continuità dei servizi critici, come la revoca e la sospensione dei certificati, l'emissione delle CRL.

4.3.2. Registration Authority (RA)

La RA è l'entità responsabile di verificare l'identità di coloro a cui possono essere assegnati i certificati siano essi titolari o referenti di applicazioni che richiedono per il loro funzionamento un certificato digitale.

La RA è essere coinvolta per:

- L''identificazione del titolare del certificato o del referente applicativo che lo richiede;
- Il recovery della chiave privata di cifratura e del profilo utente;
- La revoca o la sospensione di un certificato.

L'attività di RA può essere svolta da TERNA o da altre entità che abbiano concordato con TERNA le regole di erogazione del servizio. Nel caso in cui il servizio di RA venga svolto da un ente esterno, esso sarà disciplinato da un apposito contratto, le RA saranno attivate da TERNA che si riserva di verificare la rispondenza delle procedure applicate con quanto stabilito nelle CPS relative.

4.3.3. Titolari

4.3.3.1. Persone e dispositivi

I titolari sono le entità a cui vengono rilasciati i certificati.
Ogni titolare può disporre di più certificati, ogni certificato è relativo unicamente ad un titolare. Si suddividono in:

- Titolari interni: personale dipendente di Terna o equiparabile per compiti o mansioni a questo;
- Titolari esterni: afferenti a fornitori o a clienti di TERNA e di società da lei controllata e in generale a coloro a cui TERNA ritiene opportuno assegnare certificati per i propri fini aziendali.

Qualora i titolari siano persone fisiche, essi possono:

- Richiedere l'emissione dei certificati alla CA o alla RA per se stessi o per i dispositivi HW e SW di cui sono responsabili;
- Richiedere la revoca o la sospensione dei propri certificati e di quelli relativi ai dispositivi HW e SW di cui sono responsabili;
- Richiedere il recovery della chiave privata di cifratura e del profilo utente propri e di quelli relativi ai dispositivi HW e SW di cui sono responsabili.

4.3.3.2. Altre infrastrutture PKI (CA)

TERNA può sottoscrivere accordi di mutua certificazione con altre CA. A tali CA verranno rilasciati da TERNA i certificati delle chiavi pubbliche corrispondenti alle chiavi private da esse utilizzate per emettere certificati e liste di revoca.
Pariteticamente tali CA possono emettere i certificati delle chiavi pubbliche corrispondenti alle chiavi private utilizzate dalla CA di TERNA per emettere certificati e liste di revoca.
TERNA non riconosce validità ai certificati rilasciati da CA con cui non siano in essere accordi di mutua certificazione, anche se esse abbiano in vigore accordi di tale tipo con CA che a loro volta siano in rapporto di mutua certificazione con TERNA.

4.3.4. Applicabilità

4.3.4.1. Applicazioni previste

TERNA autorizza l'uso dei certificati rilasciati in conformità con la presente CP solo da parte di persone titolari di certificati rilasciati da TERNA o da altre CA con le quali TERNA abbia stipulato accordi di mutua certificazione.
I certificati emessi secondo le presenti policy possono essere utilizzati, a seconda della propria finalità come indicato ai capitoli successivi:

- per firmare elettronicamente documenti;
- per firmare elettronicamente codice sorgente;
- per cifrare:
    - comunicazioni e documenti tra personale dipendente e/o consulenti di TERNA
    - comunicazioni e documenti tra clienti o fornitori e TERNA.
- Per autenticarsi:
    - ad Applicazioni web
    - alla rete aziendale
    - ad applicazioni Client server

Le classi di applicazioni per le quali possono essere utilizzati i certificati sono:

- firma e cifra di messaggi di posta elettronica
- accesso sicuro ad applicazioni e siti web
- autenticazione ai sistemi, reti, ecc.
- firma e cifra di documenti.

4.3.4.2. Applicazioni non ammesse

Non è consentito l'uso dei certificati emessi da TERNA in conformità con la presente CP come indicato nella seguente tabella.

Se il titolare è	Non può
Una persona	Firmare certificati, liste di revoca, marche temporali.
Una CA cross-certified	Firmare altro che certificati e CRL

Non è consentito l'uso di applicazioni che:

1. richiedano TST in quanto il servizio non è previsto;
2. utilizzino algoritmi diversi da quelli stabiliti ai capitoli successivi;

4.3.4.3. Certificati

In accordo con le presenti policy la CA può emettere i tipi di certificati indicati di seguito.

Nel prosieguo del presente capitolo si intende per “corretto”: “conforme con quanto indicato in questo CP”.

4.3.4.3.1. Certificati di Firma e di autentica

Il loro utilizzo corretto consente di verificare l'identità del firmatario e l'integrità delle informazioni trattate nei limiti consentiti dagli standard utilizzati. Possono essere impiegati per:

- autenticazione del titolare;
- garantire l’integrità e l’autenticità delle informazioni scambiate tra diverse parti;
- garantire l’integrità e l’autenticità degli applicativi software.

L’utilizzo corretto dei certificati di firma previene, nei limiti consentiti dagli standard utilizzati, che la firma apposta possa essere ripudiata dal firmatario.

4.3.4.3.2. Certificati di cifratura

Il loro utilizzo corretto consente di proteggere la riservatezza dei dati sottoposti al processo di cifratura nei limiti consentiti dagli standard utilizzati.

4.3.4.3.3. Certificati Applicativi

Il loro utilizzo corretto, nei limiti consentiti dagli standard e dalle tecnologie utilizzate, consente di:

- Proteggere l’accesso alle applicazioni;
- Proteggere l’accesso alla rete aziendale;
- Autenticazione delle applicazioni;
- Firma e cifra di documenti mediante applicativi;
- Firma di applicazioni.

4.3.4.3.4. Certificati di certificazione

Loro titolare esclusivo è la CA di TERNA e non possono essere assegnati a nessuna altra entità. Sono utilizzati per verificare nei limiti consentiti dagli standard utilizzati l’autenticità dei certificati di sottoscrizione, di cifratura e del TSS e delle liste di revoca.

4.4. Riferimenti

4.4.1. Organizzazione

Le policy qui definite sono sotto la 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

4.4.2. Persone

Le persone responsabili per la gestione e aggiornamento del presente documento sono le seguenti.
Direzione Sicurezza Aziendale (di seguito denominata DSA)

Dott. Giuseppe Lasco
Via Arno 64
00156 ROMA
Telefono: +39-06-83138384
Fax: +39-06- 83138267
E-Mail: pki@terna.it

5. Condizioni generali

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

5.1. Obblighi

5.1.1. Obblighi della CA

TERNA ottempera agli obblighi che le derivano dal rispetto di questa CP.
La CA sostiene i diritti dei titolari che utilizzano i certificati nel rispetto delle presenti policy.

5.1.1.1. Informativa agli utenti

La CA informa preventivamente coloro che intendono richiedere certificati in merito a:

- Tipologie di certificati disponibili;
- Limitazioni all'uso di chiavi e certificati;
- Dati necessari per il rilascio dei certificati;
- Tipi di dati pubblicati nei certificati;
- Obblighi e responsabilità inerenti l'attribuzione e l'utilizzo di un certificato;
- Modalità per l'effettuazione della richiesta di certificazione;
- Modalità per l'effettuazione della revoca di un certificato;
- Modalità di accesso alle directory ove sono pubblicati certificati e CRL;
- Certificate Policy e Certification Practice Statement in vigore;
- Eventuali accordi di cross certification in vigore.

Tale informativa può essere di tipo elettronico o cartaceo, purché sia di tipo duraturo.

5.1.1.2. Identificazione delle entità

La CA deve identificare l'entità che richiede il certificato; l'identificazione è effettuata secondo quanto definito ai paragrafi successivi.

5.1.1.3. Emissione dei certificati

La CA è tenuta a:

- eseguire prima dell'emissione del certificato, la prova del possesso della chiave privata;
- non conservare copia delle chiavi private di firma e di autentica dei titolari;
- generare le chiavi di cifra mediante apparati e procedure che assicurino, in rapporto all'evoluzione delle tecnologie, la robustezza della coppia di chiavi generata, nonché la segretezza della chiave privata;
- rilasciare al titolare i certificati personali e qualora venisse richiesto il certificato pubblico della CA;
- pubblicare sulla directory il certificato pubblico di cifra.

A fronte della emissione di un certificato la CA deve:

- Notificarne l'avvenuta emissione al titolare e/o altra entità eventualmente indicata in specifici accordi. Tale notifica può essere sia di tipo elettronico che cartaceo;
- Rendere disponibili al titolare i suoi certificati e l'autocertificato della CA e rendere pubblico il certificato di cifratura mediante sua pubblicazione nella directory apposita.

5.1.1.4. Gestione dei certificati

A seguito della emissione di un certificato la CA è tenuta a:

- Gestire il rinnovo di certificati emessi e prossimi alla data di scadenza secondo quanto definito nei paragrafi successivi;
- Mantenere la storia delle chiavi private di cifra del titolare, garantendone la segretezza;
- Gestire il recovery delle chiavi private di cifratura e del profilo.

5.1.1.5. Revoca dei certificati

A fronte della revoca di un certificato emesso che sia da ritenere non più valido, la CA deve:

1. Notificare la revoca o sospensione del certificato al titolare e/o altra entità eventualmente indicata in specifici accordi. Tale notifica può essere sia di tipo elettronico che cartaceo;
2. Emettere e gestire le liste di revoca del certificato.

5.1.1.6. Obblighi riguardo CA in cross certification

La CA di TERNA può instaurare relazioni di cross certification con altre CA, dopo aver appurato che esse applicano misure di sicurezza e affidabilità compatibili con quanto esposto nel presente documento CP.
Alla data di stesura del presente documento non esistono relazioni di cross in essere con altre certification authority.

5.1.1.7. Altri adempimenti

Oltre a quanto precedentemente elencato la CA deve:

- Adottare tutte le misure organizzative e tecniche atte a garantire la sicurezza dei dispositivi hardware e software impiegati nell'attività di certificazione;
- Proteggere la riservatezza della propria chiave di certificazione;
- Custodire in modo inalterabile i log dei sistemi con cui è implementata la PKI;
- Gestire un archivio storico che preveda la memorizzazione dei certificati emessi e delle liste di revoca;
- Pubblicare regole pratiche per l'espletamento delle proprie attività (CPS) secondo quanto definito nel presente documento CP;
- Attenersi agli eventuali vincoli legislativi;
- Assicurare la continuità del servizio di emissione dei certificati, di revoca dei certificati e di emissione delle liste di revoca (CRL), ad eccezione dei periodi di indisponibilità per manutenzione straordinaria, secondo quanto stabilito in specifici accordi o procedure operative. Normalmente la disponibilità di tali servizi è nei giorni lavorativi nell'orario seguente:
-

TIPO DI SERVIZIO	GIORNI	ORARIO
Registrazione ed emissione di CERTIFICATI	LUN – VEN	08:00 – 17:00
Revoca/Sospensione	LUN – DOM	H24
Servizio di Verifica della Validità dei CERTIFICATI – CRL	LUN – DOM	H24
CALL CENTER	LUN – VEN	08:00 – 17:00

- Pubblicare i certificati di cifratura e le liste di revoca (CRL) su una directory accessibile mediante i protocolli LDAP v2 e v3 secondo quanto definito negli RFC 1777 e 2251. La disponibilità della directory per la consultazione dei certificati di cifratura e delle CRL è assicurato 24 ore su 24.
- Assicurare l'allineamento dell'orologio di sistema dei dispositivi utilizzati all'ora della rete TERNA.

- Comunicare ogni variazione del presente CP e delle relative CPS.

5.1.2. Obblighi della RA

La RA è l'entità attraverso la quale la CA espleta i propri doveri relativamente alla registrazione e certificazione degli utenti e a cui sono affidate alcune delle attività relative alla revoca/sospensione dei certificati. Essa pertanto deve operare secondo quanto definito al riguardo nelle presenti policy.
In particolare deve, in accordo a quanto descritto ai capitoli successi:

- identificare i richiedenti un certificato;
- svolgere i propri compiti relativi alla revoca/sospensione dei certificati;
- svolgere i propri compiti relativi al recovery dei certificati;
- attenersi agli obblighi che le competono in quanto titolare di certificato;
- notificare l'avvenuto recovery della chiave privata di cifratura e del profilo utente al titolare e/o ad altra entità eventualmente indicata in specifici accordi.

5.1.3. Obblighi delle aziende interessate alla PKI TERNA

Le aziende interessate alla emissione di certificati da parte della PKI di TERNA devono:

- Informare i titolari loro afferenti su obblighi e responsabilità inerenti l'attribuzione e l'utilizzo di un certificato;
- Esse, in conformità con specifici accordi stipulati con TERNA, hanno la facoltà, tramite appositi incaricati, di:
    - Abilitare le persone loro afferenti ad ottenere i certificati
    - Richiedere la revoca dei certificati relativi ai titolari loro afferenti
    - Richiedere il recovery delle chiavi di cifratura e del profilo utente per i titolari loro afferenti.

5.1.4. Obblighi dei titolari

Richiedendo un certificato l'entità accetta di conformarsi a quanto disposto dalle presenti policy, dichiara di avere fornito informazioni corrette per la sua identificazione e che il certificato sarà utilizzato esclusivamente per i fini autorizzati.
I titolari che possiedono certificati emessi da TERNA in accordo con le presenti policy devono:

- Prendere visone del presente documento CP e dei relativi CPS prima di richiedere l'emissione di un certificato;
- Conservare con la massima diligenza le chiavi private ed il dispositivo che eventualmente le contiene al fine di garantirne integrità e segretezza;
- Conservare il codice segreto di abilitazione all'uso delle chiavi private in luogo diverso da quello di conservazione delle chiavi stesse, in modo da garantirne la segretezza;
- Richiedere immediatamente la revoca di un certificato qualora:
    - il dispositivo che contiene la corrispondente chiave privata vada smarrito;
    - la chiave privata abbia perso le caratteristiche di segretezza, anche solo potenzialmente;
    - vengono le condizioni generali di uso dettate dalle presenti Policy;
- Utilizzare i certificati per i soli usi e per le sole applicazioni permesse dalla presente Certificate policy;
- Distruggere la propria chiave privata di firma qualora non abbiano più titolo a possederla;
- Informare prontamente TERNA di ogni eventuale variazione dei dati che li riguardano; se tali dati sono riportati in un certificato devono chiederne la revoca;

I titolari non devono:

- Tentare di estrarre la chiave privata dal dispositivo che la contiene o di duplicare il dispositivo;
- Rendere disponibile ad altri le proprie chiavi private;
- Utilizzare una chiave privata di firma che si presuma compromessa;
- Utilizzare una chiave privata firma relativa ad un certificato revocato o scaduto;
- Utilizzare un certificato di cifra revocato o scaduto;
- Violare alcuna norma sulla riservatezza delle informazioni personali, sulla proprietà intellettuale o eventuali disposizioni aziendali sulla riservatezza delle informazioni.

I titolari possono:

- Richiedere l'emissione dei certificati purché autorizzati da parte dell'organizzazione a cui afferiscono;
- Richiedere il recovery delle chiavi private di cifratura e del proprio profilo utente, ad esempio se hanno dimenticato i codici segreti di attivazione

5.1.5. Obblighi delle CA in cross certification

Una CA che abbia stipulato un accordo di mutua certificazione con la CA di TERNA qui descritta deve rispettare le proprie policy in base alle quali è stato sottoscritto l'accordo.
La CA di TERNA e l'altra CA si scambieranno le informazioni necessarie alla stipula del detto accordo.
Le due parti possono non comunicare le informazioni di cui ritengano di dover garantire la riservatezza. Il personale incaricato di quest'analisi sottoscriverà in ogni caso un impegno a non divulgare eventuali informazioni riservate concernenti la controparte di cui sia entrato in possesso.
Le due parti possono concordare ispezioni periodiche dell'altra parte per consentire la verifica del rispetto delle norme indicate nei documenti CP, CPS ed altri eventuali sulla cui base sia stato stipulato l'accordo.

5.1.6. Obblighi di altre entità

Le entità che fanno affidamento sui certificati emessi da TERNA per verificare la validità di firme digitali o la possibilità di cifrare dati per un titolare, sono tenute a verificare la validità dei certificati (rispetto al formato previsto dallo standard ISO 9594-8 1997 o successivo) avvalendosi delle liste di revoca/sospensione gestite da TERNA.

Qualora tali entità non possano ottenere una CRL:

1. formalmente valida;
2. di cui non sia trascorso il periodo di validità;
3. firmata dalla CA di TERNA con una chiave valida;

non sono autorizzate a ritenere valido il certificato in esame. Di conseguenza non sono autorizzate né a cifrare utilizzando tale certificato né a ritenere valida la firma digitale ad esso associata.

Esse devono inoltre:

- prendere visione delle garanzie e assicurazioni relative all'uso del certificato contenute nella CP di riferimento;
- qualora il certificato sia stato emesso da una CA diversa da TERNA, verificare l'esistenza di accordi di mutua certificazione tra le CA e i termini di tali accordi. Qualora non siano in atto accordi di questo tipo, le responsabilità relative all'utilizzo del certificato ricadono sull'utente.

Analogamente, prima di utilizzare un certificato emesso da CA riconosciute tramite cross certification, devono verificarne la validità tramite liste di revoca non scadute, la cui autenticità dovrà essere verificata utilizzando i certificati di cross certification.

Deve essere anche verificato il corretto uso dei certificati, avvalendosi del campo ***keyUsage*** dello standard ISO 9594-8 e se previsto di quello ***Extended KeyUsage***.
Le entità non certificate dalla CA di TERNA qui definita o la cui CA non sia riconosciuta mediante accordi di cross certification dalla stessa CA di TERNA si assumono in pieno la responsabilità di verificare la validità di un certificato e più in generale del suo utilizzo. Nei loro confronti TERNA non ha alcun obbligo al riguardo.

5.1.7. Obblighi relativi alla Directory

TERNA conserva in una zona logicamente e fisicamente protetta una copia master della directory su cui sono conservati i certificati, le liste di revoca/sospensione e altre informazioni necessarie per la operatività della CA. La copia master della directory è protetta da accessi non autorizzati.

Copie operative (slave) della predetta master copy sono rese liberamente disponibili all'accesso da parte degli utenti per accedere in sola lettura a certificati e liste di revoca/sospensione. Le copie operative della directory sono protette da accessi non autorizzati che ne possano alterare il contenuto.
L'accesso alle CRL e ai certificati emessi è garantito senza soluzione di continuità attraverso il sistema di directory slave ed attraverso il portale del certificatore.

5.2. Garanzie e limitazioni di responsabilità

5.2.1. Responsabilità della CA

5.2.1.1. Garanzie

La CA garantisce che userà le competenze e la diligenza ragionevolmente necessarie per assicurare che siano conformi alle presenti policy e alle procedure indicate nel documento CPS relativo:

- I servizi di certificazione ed i servizi di repository;
- La generazione delle coppie di chiavi di cifra;
- L'emissione dei certificati;
- La revoca e la sospensione dei certificati emessi;
- La gestione delle liste di revoca;
- L'effettuazione del servizio di recovery della chiave privata di cifratura e del profilo utente .

Essa, inoltre, garantisce che i documenti CP e CPS vengano aggiornati annualmente e comunque ogni qualvolta si renda necessario..

5.2.1.2. Limitazioni

Salvo quanto espresso nei paragrafi precedenti, la CA non risponde di:

- Informazioni false o errate che le siano state fornite e sulle quali non sia 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;
- Qualsiasi conseguenza derivante dall'utilizzo di certificati da parte di entità non appartenenti alla propria PKI o appartenenti ad infrastrutture PKI non riconosciute tramite cross certification;
- 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 atti di guerra, tumulti, 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 concordato in accordi di cross certification

Salvi restando gli obblighi di legge non risponde di:

- Richieste di indennizzo avanzate da terze parti nei confronti dei titolari o delle loro organizzazioni di appartenenza,
- Danni ad archivi o dati
- Danni indiretti, ivi inclusi mancati guadagni, derivanti da perdite di incassi, contratti, risparmi o profitti previsti

5.2.2. Responsabilità della RA

5.2.2.1. Garanzie

La RA garantisce che il processo di identificazione delle entità è conforme a quanto definito nelle presenti policy.

5.2.2.2. Limitazioni

Salvo quanto espresso ai punti precedenti, la RA non risponde di:

- Informazioni false o errate che le siano state fornite e sulle quali non sia 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.

5.3. Responsabilità finanziaria

5.3.1. Indennizzi

Non sono previsti indennizzi per incidenti legati a malfunzionamenti e/o errata applicazione delle procedure organizzative di tutte le componenti della PKI.

5.3.2. Relazioni fiduciarie

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

5.4. Interpretazione e competenze legislative

5.4.1. Riferimenti

Non si utilizzano riferimenti legislativi in quanto la CA di TERNA è esclusivamente ad uso interno.

5.4.2. Modifiche organizzative della CA

Eventuali modifiche organizzative che abbiano impatti sulla infrastruttura PKI e sulla CA stessa verranno comunicate a tutte le entità coinvolte con un anticipo di almeno due mesi rispetto all'attuazione delle variazioni stesse.

5.4.3. Risoluzione delle dispute

Qualsiasi reclamo dovrà essere fatto pervenire in forma scritta a TERNA, a

TERNA - Sicurezza Aziendale
Via Galbani 70
00156 ROMA
Telefono: +39-06-83138384
Fax: +39-06- 83138267
e-mail: pki@TERNA.it

Il foro competente sarà stabilito concordemente tra TERNA e le singole società clienti.

5.5. Tariffe

5.5.1. Generazione e rinnovo dei certificati

Le tariffe relative alla generazione ed al rinnovo dei certificati saranno definite in accordo con le strutture di appartenenza dei titolari.

5.5.2. Recovery della chiave privata di cifratura

Le tariffe relative al recovery della chiave privata di cifratura saranno definite in accordo con le strutture di appartenenza dei titolari.

5.5.3. Altri servizi

Nessun pagamento deve essere corrisposto per richiedere la revoca o la sospensione di un certificato né per richiedere la riattivazione di un certificato sospeso.
Nessun pagamento deve essere corrisposto per accedere a:

- Certificati di cifra;
- Liste di revoca;
- Il presente documento CP, purché pubblicato secondo quanto descritto nei paragrafi successivi;
- Il documento CPS, purché pubblicato secondo quanto descritto nei paragrafi successivi.

5.5.4. Rimborsi

Le tariffe e modalità per usufruire di eventuali rimborsi saranno definite in accordo con le strutture di appartenenza dei titolari.

5.6. Pubblicazione e repository

5.6.1. Pubblicazione di informazioni

Saranno pubblicati in forma elettronica i seguenti documenti:

- Il documento CP
- Il documento CPS, non comprensivo di informazioni riservate

I certificati di firma non vengono pubblicati sulla directory, ma sono allegati automaticamente ai documenti firmati.
E' gestita una struttura dati consultabile liberamente contente le liste di revoca. L'accesso sarà consentito tramite i protocolli LDAP ed http.

5.6.2. 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 è superiore ad 1 (una) ora.
Le liste di revoca sono pubblicate con la frequenza indicata ai capitoli successivi.
Versioni aggiornate del documento CP e del documento CPS vengono rilasciate nel più breve tempo possibile.

5.6.3. Controllo di accesso

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

5.7. Verifiche di conformità alle norme

TERNA effettua un auditing periodico e in alcuni casi particolari estemporaneo sulle norme esposte in questa CP e sulle procedure operative per verificarne:

1. il rispetto da parte del personale;
2. l'efficacia e l'aderenza alle effettive necessità;
3. l'effettiva possibilità che siano rispettate.

5.7.1. Frequenza

La verifica dei processi seguiti dalla CA è effettuata ogni mese, ogni sei mesi e ogni anno a seconda delle procedure interessate e comunque al verificarsi di eventi significativi.
La verifica dei processi seguiti dalla RA è effettuata almeno ogni anno e comunque al verificarsi di eventi significativi.

5.7.2. 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 infrastruttura PKI.
Le ispezioni vengono effettuate dal reparto di audit interno di TERNA.

5.7.3. 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 di lavoro in corso o pianificata che possa portare ad un conflitto di interessi.

5.7.4. 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;
- Recovery;
- Richiesta di revoca dei certificati;
- Revoca dei certificati.

I titolari interni e i titolari esterni possono essere soggetti ad azioni di verifica e controllo, se così è previsto negli specifici accordi. Per ulteriori dettagli si rimanda al documento CPS.

5.7.5. Azioni da intraprendere in caso di inadempienza

I risultati di azioni di verifica e controllo sono sottoposti all'attenzione di TERNA.
In base alle irregolarità riscontrate ed al loro impatto sulla infrastruttura PKI è possibile:

- Revocare eventuali certificati emessi dalla CA;
- Revocare i certificati della CA;
- Definire le azioni di correzione che la CA deve intraprendere entro un periodo di tempo convenuto.

Qualora si verificasse la compromissione della chiave privata della CA, entrerà in vigore quanto previsto al capitolo successivo.

Ove necessario potranno essere decise opportune azioni correttive, tendenti a modificare le procedure o l'infrastruttura. In tale caso saranno aggiornati i documenti CPS e CP che ad esse si riferiscono.

5.7.6. Comunicazione dei risultati

I risultati delle verifiche e dei controlli effettuati sono sottoposti all'attenzione della CA la quale è responsabile delle eventuali azioni correttive.
I risultati delle azioni di verifica e di controllo sono considerati riservati e gestiti secondo quanto definito nelle presenti policy.

5.8. Riservatezza

Tutte le informazioni raccolte, generate, trasmesse e gestite dall'infrastruttura PKI all'interno della quale opera la CA sono considerate riservate e trattate secondo quanto definito nelle presenti policy e del documento programmatico della Sicurezza di TERNA.

5.8.1. Informazioni riservate

Sono da considerare riservate tutte le informazioni relative a dati personali e, ove presenti, sensibili ai sensi della legge 675/96.
Sono altrettanto considerate riservate la informazioni che il titolare ha espressamente indicato di non voler riportare sul proprio certificato.
Per motivi di riservatezza le motivazioni della revoca dei certificati dei titolari sono limitate al minimo indispensabile a fornire informazioni utili agli utilizzatori dei certificati.

5.8.2. Informazioni non riservate

Non sono considerate informazioni riservate le informazioni contenute nei certificati né la revoca o la sospensione dei certificati stessi.

5.8.3. Comunicazione alle organizzazioni clienti

Ad eventuali referenti delle organizzazioni clienti a cui afferiscono i titolari vengono comunicate le seguenti informazioni:

- 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 indisponibilità del profilo utente memorizzato sul dispositivo crittografico;
- Notifica di revoca o sospensione dei certificati per i titolari loro afferenti;

La comunicazione può essere effettuata in forma elettronica o cartacea.

5.8.4. 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.

5.8.5. Comunicazione di informazioni ai titolari

In conformità con la legge 675/96 i titolari in qualsiasi momento possono chiedere l'accesso ai propri dati personali e, ove presenti, sensibili, conservati da TERNA o da organizzazioni eventualmente incaricate da TERNA del loro trattamento. L'esistenza e l'attività di tali organizzazioni viene portata a conoscenza dei titolari.

5.9. Copyright e leggi sulla proprietà intellettuale

I certificati, il presente documento CP, il documento CPS, ecc. sono di proprietà della società TERNA S.p.A.
Dispositivi hardware e software forniti da TERNA ai propri incaricati e titolari sono coperti da copyright.

6. Identificazione e autenticazione

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

- l'emissione dei certificati;
- il rinnovo dei certificati;
- la revoca o la sospensione dei certificati;
- il recovery dei certificati e del profilo utente;

6.1. Registrazione iniziale

6.1.1. Tipi di Nome

Il nome del titolare è indicato nel campo subject del certificato come Distinguished Name, come definito al capitolo 9.1 dello standard ISO 9594-1.
Il campo subjectAltNames del certificato contiene:

- l'indirizzo di posta elettronica e l'identificativo di dominio (UPN) per i titolari interni;
- l'indirizzo di posta elettronica per i titolari esterni;
- l'indirizzo di posta elettronica del referente per i certificati dei web server e della firma del codice applicativo;
- l'identificativo di dominio (UPN) per i certificati delle componenti server dell'applicativo MS Office Communication.
- L'indirzzo Ip o il nome DNS del terminatore VPN per i certificati IPSEC.

I tipi di nome che possono essere utilizzati nei certificati (nel campo subject) sono:

- Qualora il titolare sia una persona fisica: Nome e Cognome
- Qualora il titolare richieda un certificato per un dispositivo di cui è responsabile: Nome e Cognome del responsabile o Identificativo del dispositivo o del servizio (che contraddistingua Marca, modello, numero di serie o la tipologia di servizio che viene fornito).
- Pseudonimo. In questo caso TERNA conserva un opportuno archivio adeguatamente protetto per poter risalire dallo pseudonimo al titolare.

6.1.2. Significatività dei nomi

Il nome definito nel campo subject o nel subject alternate name è associato al titolare così che è possibile risalire a quest'ultimo. A fronte di una stessa entità con più certificati di medesimo tipo (ad esempio di firma) il campo subject può contenere un codice identificativo aggiuntivo in modo da rendere univoco tale campo. Per i Titolari interni ed esterni il codice identificativo univoco è rappresentato dal codice fiscale del titolare con in aggiunta un numero progressivo a tre cifre che consente di rendere unico il subject nel caso in cui un titolare dovesse aver più di un profilo assegnato.

6.1.3. Regole per l'interpretazione dei nomi

La modalità di composizione del nome del titolare nel campo subject viene definita nelle procedure operative di TERNA (CPS).
L'indirizzo di e-mail indica a quale indirizzo il titolare intende gli vengano inoltrate le comunicazioni in formato elettronico. L'indirizzo UPN rappresenta l'identificativo univoco del titolare nel domino Windows di TERNA.

6.1.4. Univocità dei nomi

Il nome riportato nel campo subject del certificato non può essere ambiguo ed è univoco nell'ambito di tutti i certificati emessi dall'infrastruttura PKI.

6.1.5. Risoluzione di conflitti sui nomi

La CA si riserva il diritto di prendere decisioni in merito alla risoluzione di omonimie per garantire l'univocità dei nomi, di comune accordo, ove ciò sia applicabile, con l'incaricato dell'organizzazione cliente che ha abilitato il titolare a richiedere il certificato.

6.1.6. Riconoscimento, autenticazione e ruolo dei marchi di fabbrica

Marchi di fabbrica possono essere presenti nei certificati usati da applicazioni.

6.1.7. 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, utilizzando modalità previste in standard ufficiali o in specifiche pubbliche RFC emesse dallo IETF del NIST.

6.1.8. Identificazione delle organizzazioni

TERNA ha predisposto un documento che identifica in modo univoco le organizzazione con le quale collabora/interagisce.

6.1.9. Identificazione delle singole entità

6.1.9.1. Addetti alla PKI

L'identificazione degli addetti alle operazioni di gestione della PKI e delle RA avviene da parte del proprio Management diretto o del Responsabile della Sicurezza all'atto dell'assegnazione dell'incarico.
A questi addetti viene consegnata anche specifica lettera di incarico.
Coloro che devono essere anche titolari di certificato utilizzeranno le procedure standard definite nell'ambito di queste policy e quanto descritto nel CPS.

6.1.9.2. Entità appartenenti a TERNA

Per i titolari interni ai quali debbano essere rilasciati certificati per se stessi o per i dispositivi di cui essi siano responsabili, possono applicarsi in alternativa le seguenti modalità operative:

1. le persone interessate si recano presso l'operatore di Registrazione a cui comunicano i dati necessari e, ove applicabile, anche quelli del dispositivo di cui sono responsabili per il quale intendono farsi rilasciare un certificato;
2. i rispettivi referenti inviano una e-mail, con i dati necessari sopra citati, alla specifica RA che provvede alla loro registrazione.

6.1.9.3. Entità appartenenti a Società clienti / fornitori

Per i dipendenti di Società clienti / fornitori ai quali debbano essere rilasciati certificati per se stessi o per i dispositivi di cui essi siano responsabili, si applica la seguente procedura:

- le persone, che nel singolo accordo saranno indicate come incaricate di fornire tale servizio, comunicheranno a TERNA, secondo le procedure dettagliate nell'accordo stesso, gli elenchi delle persone interessate dalla certificazione, indicando sotto la propria responsabilità gli estremi dei documenti di identità e di identificazione necessari.

6.2. Rinnovo dei certificati

TERNA emette due tipi di certificati: rinnovabili e non.
Per quelli rinnovabili TERNA rinnova automaticamente le chiavi e quindi i certificati in conformità con specifiche pubbliche RFC qualora il certificato da rinnovare sia ancora valido.
Se i certificati sono rinnovabili ne viene effettuato il rinnovo solo se sono stati utilizzati durante il periodo finale di validità.
I certificati scaduti non possono essere rinnovati. Le entità devono richiedere dei nuovi certificati eseguendo la procedura di recovery.
Per i certificati non rinnovabili il titolare, il referente dell'applicativo o gli incaricati prima della scadenza del certificato (per garantire la continuità operativa) o anche dopo la sua scadenza dovrà chiederne il rinnovo secondo le procedure di prima emissione descritte al passo precedente (in questo caso il subject resta invariato)

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

Il recovery delle chiavi private di cifratura e del profilo utente può essere richiesto dal titolare, dalle persone della organizzazione di appartenenza che li hanno autorizzati a richiedere i certificati o da altre entità eventualmente indicate negli specifici accordi. Il recovery avviene, con modalità operative sicure previste dalla specifica piattaforma tecnologica, dietro autorizzazione da parte degli incaricati delle organizzazioni di appartenenza dei titolari.

6.4. Richiesta di revoca dei certificati

La richiesta di revoca o sospensione dei certificati deve essere effettuata per iscritto secondo quanto definito ai punti successivi.
Il titolare e l'incaricato della singola Società saranno informati dell'avvenuta revoca o sospensione per posta elettronica e, ove previsto negli accordi, anche per posta normale.

7. Requisiti gestionali

In questa sezione vengono specificate le modalità operative impiegate nell'ambito della PKI di TERNA per la gestione del ciclo di vita dei certificati digitali

7.1. Richiesta di certificati

7.1.1. Richiesta da parte delle singole entità

In aggiunta a quanto definito al punto precedente, le persone che intendono fare richiesta di certificazione:

1. firmeranno il consenso all'elaborazione dei medesimi dati ai sensi delle vigenti normative;
2. riceveranno il materiale necessario per effettuare la certificazione e per operare quando saranno stati certificati;

7.2. Emissione dei certificati

Sono previste differenti modalità per l'emissione dei certificati in funzione dell'entità titolare.

7.3. Certificazione per Titolari Interni e Esterni

Dopo aver svolto quanto specificato ai paragrafi precedenti, per la generazione dei certificati i titolari installano, se richiesto dalle procedure, l'HW e il SW ricevuti e, come indicato nelle istruzioni ricevute, si autenticano al sistema e innescano il processo di certificazione.
A fronte dell'autenticazione del titolare, il processo di certificazione prevede che le coppie di chiavi asimmetriche di firma ed autentica siano sempre create dal titolare con il client o con il suo dispositivo di firma mentre la coppia di chiavi di cifratura viene creata centralmente dalla CA, che invia al titolare la chiave privata. La CA conserva copia di quest'ultima in modo sicuro, così da poterne fare il recovery.
La CA di TERNA verifica il possesso della chiave privata di firma da parte del titolare ed 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 da parte della CA, il processo non ha seguito.
Al termine del processo, il titolare sarà in possesso, all'interno del proprio dispositivo di firma o del proprio sistema client, del proprio profilo costituito delle chiavi private di firma, autentica e di cifratura, dei certificati di firma, di autentica e di cifratura.
Qualora il titolare riceva segnalazione di un'avvenuta precedente certificazione abusiva, attiva la revoca urgente dei certificati artefatti.
La CA di TERNA provvede a :

- pubblicare il certificato di cifratura emesso;
- notificare la generazione del certificato al titolare e/o altra entità eventualmente indicata in specifici accordi in forma elettronica o cartacea.

7.4. Accettazione dei certificati

Al termine del processo di emissione dei certificati il titolare deve:

1. verificare l'esattezza del certificato emesso dalla CA di TERNA.
2. Nel caso in cui riscontri che il certificato riporta dati errati, il titolare dovrà richiederne la revoca urgente. Fino al ricevimento di tale richiesta il certificato rilasciato verrà ritenuto accettato dal titolare.

7.5. Revoca dei certificati

7.5.1. Motivazioni per la revoca

7.5.1.1. Motivazioni per la revoca di un certificato di un titolare

Un certificato deve essere revocato nei seguenti casi:

1. sostituzione del certificato senza che ne sia stata compromessa la chiave privata;
2. non è più garantita la riservatezza della chiave privata;
3. le informazioni contenute nel certificato sono variate, sono diventate obsolete o sono errate;
4. il titolare cessa dall'incarico per adempiere al quale gli è stato rilasciato il certificato;
5. il titolare non ha rispettato gli obblighi di cui alle presenti policy;
6. non è più garantita la riservatezza della chiave privata di firma della CA di TERNA;
7. cessazione dell'attività della CA di TERNA.

In tutti i casi, tranne nel caso n. 7, la revoca può essere urgente.

7.5.1.2. Motivazioni per la revoca di un certificato della CA di TERNA

Un autocertificato della CA di TERNA deve essere revocato nei seguenti casi:

1. non è più garantita la riservatezza della chiave privata di firma della CA di TERNA;
2. cessazione dell'attività della CA di TERNA.

7.5.2. Entità idonee alla richiesta di revoca dei certificati

7.5.2.1. Chi può chiedere la Revoca di un certificato di un titolare

Le seguenti entità possono richiedere la revoca di certificati di un titolare:

- Il titolare e/o altra entità eventualmente indicata in specifici accordi;
- La CA;
- La RA.

7.5.2.2. Chi può chiedere la Revoca di un certificato della CA di TERNA

La revoca dei certificati della CA di TERNA può essere richiesta dal Direttore a cui risponde il Responsabile della CA di TERNA.

7.5.3. Procedura per la richiesta di revoca dei certificati

Tutte le richieste di revoca e le risultanti azioni devono essere archiviate e conservate per almeno 5 anni dopo la cessazione dei rapporti di collaborazione con il titolare del certificato.

7.5.3.1. Richiesta di Revoca del certificato di un titolare da parte del titolare stesso

Un titolare può richiedere la revoca o la sospensione del proprio certificato o del certificato del dispositivo di cui è responsabile:

- mediante un messaggio di posta elettronica, ove possibile, firmato in modo digitale
- contattando il Call Center per via telefonica, facendosi opportunamente identificare.

La revoca o sospensione di un certificato viene notificato, come previsto ai paragrafi precedenti.

7.5.3.2. Richiesta di Revoca del certificato di un titolare da parte del suo referente

L'incaricato della Società a cui afferisce il titolare può chiedere la revoca dei certificati di un titolare:

- mediante un messaggio di posta elettronica firmato in modo digitale, ove possibile
- presentandosi personalmente alla RA
- contattando il Call Center per via telefonica, facendosi opportunamente identificare.

7.5.3.3. Richiesta di Revoca del certificato della CA di TERNA

La revoca degli autocertificati della CA di TERNA deve essere richiesta con documento cartaceo opportunamente protocollato.

7.5.4. Periodo di tempo per revocare i certificati

La richiesta di revoca di un certificato viene verificata ed elaborata nel più breve tempo possibile e comunque non superiore ad 1 (una) ora dal momento in cui la richiesta perviene alla CA, nel caso si tratti di revoca urgente, purché la richiesta pervenga entro l'orario di servizio indicato nelle presenti policy.
Qualora la richiesta di revoca sia ricevuta nell'ultima ora prima dell'emissione di una CRL, è possibile che non vi sia il tempo materiale per elaborare la richiesta, che verrà comunque inserite nella CRL seguente indicando come momento di invalidità della chiave privata un momento non posteriore a quello in cui la richiesta è stata ricevuta.

7.5.5. Motivazioni per la sospensione

Un certificato viene sospeso quando sia necessario un ulteriore periodo di tempo per verificare la fondatezza della richiesta di revoca, cioè se il certificato debba essere effettivamente revocato.
La sospensione è sempre urgente.

7.5.6. Entità idonee alla richiesta di sospensione dei certificati

La sospensione dei certificati può essere richiesta dalle stesse entità abilitate a richiederne la revoca, con l'eccezione dei certificati di certificazione che non possono essere sospesi, ma, all'occorrenza, solo revocati.

7.5.7. Procedura per la richiesta di sospensione dei certificati

Le procedure per la richiesta di sospensione dei certificati sono le medesime previste per la loro revoca, con l'eccezione dei certificati di certificazione che non possono essere sospesi, ma, all'occorrenza, solo revocati.

7.5.8. Durata massima della sospensione dei certificati

La durata massima della sospensione è definita nelle procedure operative (CPS).
Se, prima della scadenza del periodo di sospensione, la CA di TERNA non riceve una richiesta di riattivazione del certificato, effettuata dalle stesse funzioni abilitate a richiederne la revoca e con le stesse modalità, il certificato viene revocato definitivamente con data di revoca pari alla data di inizio della sospensione.

7.5.9. Frequenza di emissione della CRL e loro disponibilità

Le liste di revoca sono pubblicate ogni 24 ore, indipendentemente dalla presenza di nuove revoche da pubblicare, e comunque nel più breve tempo possibile a fronte di revoche definite urgenti nel documento CPS interessato.
La disponibilità della directory o di un portale web per la consultazione delle CRL è assicurato 24 ore su 24.

7.5.10. Verifica della validità dei certificati avvalendosi delle CRL

La verifica della validità dei certificati viene eseguita accedendo con modalità on-line alle CRL emesse dalla CA di TERNA o emesse da CA cross-certified con TERNA.

7.5.11. Informazioni sulla validità dei certificati avvalendosi di informazioni on-line

Nessuna disposizione: non sono fornite informazioni sullo stato dei certificati altro che tramite CRL.

7.5.12. Verifica della validità dei certificati avvalendosi di informazioni on-line

Nessuna disposizione: non sono fornite informazioni sullo stato dei certificati altro che tramite CRL.

7.5.13. Altre modalità di informare sullo stato di validità dei certificati

Nessuna disposizione: non sono fornite informazioni sullo stato dei certificati altro che tramite CRL.

7.5.14. Verifica di altre modalità di informazione sullo stato di validità dei certificati

Nessuna disposizione: non sono fornite informazioni sullo stato dei certificati altro che tramite CRL.

7.5.15. Requisiti speciali nel caso di compromissione della chiave

In aggiunta a quanto esposto al capitolo "*Motivazioni per la revoca di un certificato di un titolare"* circa il punto 2, si applica quanto previsto ai capitoli successivi

7.6. Procedure di verifica e controllo

Tutti i sistemi componenti la PKI di TERNA interessati da quanto descritto in questa CP e nella CPS correlata registrano e conservano i record di log necessari.

7.6.1. Tipi di eventi registrati

Vengono effettuate tutte le registrazioni necessarie utili alla verifica e al controllo delle operazioni svolte nell'ambito della CA, dagli eventi relativi alla normale operatività dei singoli sistemi alle condizioni di allarme.
La CA registra 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 e dei log della CA
- Operazioni schedulate e non di manutenzione del sistema
- Aggiornamenti hardware e software

I record di log sono protetti contro manomissioni accidentali o intenzionali.

7.6.2. 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.

7.6.3. Conservazione dei log

I log sono conservati per un periodo di tempo non inferiore ai 5 anni.
Ne è consentita la rilettura in qualsiasi momento durante il periodo di conservazione.

7.6.4. 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.

7.6.5. 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.

7.6.6. Raccolta dei record di log

Gli eventi generati dal server ospitante la CA o dalla CA stessa sono registrati in file di log in modo automatico, eventi esterni possono essere registrati manualmente.
I log possono essere trasferiti in modo sicuro su supporti fisici esterni alla CA o al server ospitante.

7.6.7. Notifica ai soggetti che hanno causato eventi critici

Il responsabile della sicurezza della CA di TERNA viene informato degli eventi fuori linea e li comunica sia ai soggetti che li hanno causati sia ai loro capi. Nel caso il soggetto non sia dipendente o consulente di TERNA il responsabile della sicurezza ne informa la persona preposta a mantenere i contatti con l'azienda a cui il soggetto afferisce che provvede ad informare l'azienda stessa.

7.6.8. Valutazione delle vulnerabilità

TERNA ha in essere una sistematica attività di Risk Assessment and Management da cui scaturisce un'analisi delle possibili vulnerabilità e la individuazione delle opportune contromisure.

7.7. Informazioni archiviate

7.7.1. Tipi di informazioni archiviate

La CA archivia i seguenti tipi di informazioni:

- Eventi relativi a verifiche e controlli;
- Certificati e CRL emessi;
- Chiavi private di cifra dei titolari, in forma protetta, per consentire la gestione della key history,
- Accordi di cross certification;
- Documentazione cartacea ed elettronica: corrispondenza, richieste di certificazione, richieste di recovery del profilo o della chiave privata di cifratura, richieste di revoca integrate della documentazione necessaria, report di independent audit, verbali di generazione delle chiavi della CA, descrizione della configurazione dei vari sistemi della PKI, ecc.
- Richieste di accesso alle informazioni archiviate.

7.7.2. Periodo di conservazione degli archivi

Le chiavi, i certificati e le CRL sono conservate per un periodo di tempo non inferiore ai 5 anni.
Documentazione relativa ad accordi di cross certification e la corrispondenza sono mantenuti per un periodo di tempo non inferiore ai 5 anni.
Qualora TERNA decidesse di interrompere la propria attività di CA la documentazione verrà gestita come indicato ai capitoli successivi.

7.7.3. 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 e magnetismo, oltre che da tentativi di manomissione e di accesso non autorizzato.
Ne è consentita la rilettura in qualsiasi momento durante il periodo di conservazione.

7.7.4. Copie di riserva degli archivi

Giornalmente sono effettuate copie di riserva dei log, dei certificati, e delle chiavi, mantenendo valida la tutela dell'integrità e della riservatezza delle informazioni.
Settimanalmente 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.

7.7.5. Indicazione del tempo nei record di log

Tutti i record di log contengono l'indicazione del momento in cui sono stati presi. La fonte di tempo con cui sono sincronizzati i clock dei sistemi della CA è una fonte affidabile.

7.7.6. Sistema di raccolta dei record archiviati

L'archivio delle informazioni è interno alla base dati della Certification Authority

7.7.7. Procedura per verificare ed ottenere informazioni archiviate

Le richieste per accedere ad informazioni archiviate sono sottoposte alla CA in forma scritta.

7.8. Rinnovo delle chiavi

7.8.1. Rinnovo delle chiavi dei titolari

7.8.1.1. Rinnovo normale delle chiavi dei titolari

La durata dei certificati dei titolari è indicata nel riferimento "Profilo dei Certificati".
I certificati emessi da TERNA possono essere rinnovabili o non.
Per quelli rinnovabili, trascorsa una percentuale della vita del certificato da definire negli accordi con le aziende clienti, il portale Terna, non appena attivato, innesca la procedura di sostituzione della coppia di chiavi del titolare e quindi del suo certificato.
Se il titolare non utilizza il portale nell'ultimo periodo di vita del proprio certificato, quest'ultimo scadrà e, qualora il titolare volesse continuare ad operare in seno alla PKI di TERNA, dovrà eseguire nuovamente il processo di registrazione e certificazione.
La procedura di rinnovo dei certificati non rinnovabile è equiparabile alla procedura descritta nel paragrafo: 7.8.1.2.

7.8.1.2. Rinnovo in condizioni anomale delle chiavi dei titolari

Nel caso in cui il titolare smarrisca il proprio dispositivo crittografico o i relativi codici di attivazione o in cui esso risulti difettoso o, ancora, nel caso in cui sia stata compromessa una sua chiave privata, il titolare, a seconda dei casi, avvalendosi del dispositivo preesistente o di un altro attiverà con la collaborazione della propria RA di riferimento il recupero della copia di chiavi di cifra, o la generazione di una nuova coppia, e/o la generazione di una nuova coppia di chiavi di firma.
A seguito di questo processo il titolare disporrà sul proprio dispositivo crittografico di un profilo basato su una nuova coppia di chiavi di firma, sulla vecchia chiave privata di cifra e (ove necessario) su una nuova coppia di chiavi di cifra.

7.8.1.3. Rinnovo delle chiavi della CA

In condizioni di normalità la chiave di firma della CA ha durata di 10 anni e il rinnovo suo 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.
Il verbale dell'operazione viene conservato per 5 anni.

7.9. Procedure di emergenza e disaster recovery

7.9.1. Gestione dei disastri ambientali

In caso di disastro viene attivato un piano di disaster recovery che prevede quanto segue.

1. le CRL già emesse restano disponibili senza soluzione di continuità;
2. il ritardo massimo nell'emissione di nuove CRL e di nuovi certificati è di 12 ore qualora debba essere messo in operatività il sito di back up;

In caso di disastri di particolare gravità si applica una specifica Operational Security Policy.
I dati riservati sono protetti in modo che, anche se i loro supporti venissero asportati nei momenti successivi al disastro non possono essere letti.

7.9.2. Compromissione delle chiavi di TERNA

In caso di compromissione di una chiave di firma della CA, TERNA notificherà 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.

7.9.2.1. Compromissione della chiave di firma della CA di TERNA

Entro 8 ore dalla scoperta dell'evento TERNA ne informerà i propri utenti e le CA cross-certified.
La coppia di chiavi della CA di TERNA verrà sostituita, come esposto al capitolo 7.8.1.3.
I certificati emessi saranno revocati e sostituiti. La sostituzione di tutti i certificati, ancorché estremamente onerosa, è indispensabile, perché solo in questo modo sarà possibile distribuire a tutti i titolari di certificati emessi dalla CA di TERNA (singoli individui e CA cross-certified) il nuovo autocertificato della CA di TERNA relativo alla chiave privata di firma con la quale viene emessa la nuova CRL in cui sono elencati tutti i certificati revocati.

7.10. Termine dell'attività della CA

Qualora TERNA intenda terminare la propria attività di CA, con un anticipo di almeno 6 (sei) mesi svolgerà le seguenti attività preliminari.

7.10.1. Attività preliminari

1. La prevista data di cessazione delle attività verrà comunicata ai titolari e alle CA cross certified;
2. verrà incaricata un'altra Società di rilevare la documentazione e, qualora tale Società operi come CA, di rilevare anche la directory ove verrà pubblicata l'ultima CRL;
3. qualora tale Società non intenda operare come CA, TERNA conserverà attiva la directory, su cui verrà pubblicata l'ultima CA, fino allo scadere dell'ultimo certificato revocato.

7.10.2. Attività al momento della chiusura delle attività

Al sopraggiungere della data di cessazione delle attività TERNA revocherà i certificati ancora in vigore.

8. 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.

8.1. Sicurezza ambientale

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

8.1.1. Luoghi ed edifici

I dispositivi utilizzati dalla CA per il proprio funzionamento si trovano in un ambiente isolato, ad accesso controllato, all'interno di edifici sui quali TERNA 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.

8.1.2. Accesso fisico

8.1.2.1. CA

L'accesso ai locali ove sono ospitati i sistemi della CA (CA, Master Directory, infrastrutture di rete interna) è limitato alle persone autorizzate. 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.

8.1.2.2. RA

La RA deve espletare almeno le seguenti funzioni di controllo:

- Il computer della RA non deve essere utilizzato da altre entità, se non in presenza e sotto il diretto controllo della RA stessa
- Sono messe in atto misure di sicurezza che impediscano intrusioni all'interno dei computer ed evidenzino eventuali tentativi.
- L'eventuale dispositivo crittografico utilizzato, viene riposto in una cassetta di sicurezza durante i periodi di inutilizzo.
- L'utilizzo del computer viene tutelato da adeguati sistemi di identificazione della RA stessa

8.1.2.3. Titolari

I titolari devono proteggere i codici di attivazione del dispositivo di firma dall'accesso di altre persone. Questi codici non devono essere scritti su supporti leggibili liberamente, a meno che non vengano custoditi in modo da garantire l'accesso al solo titolare.

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

Sono in atto misure che assicurano un sistema di condizionamento di aria sicuro e un adeguato sistema di alimentazione elettrica che consente il funzionamento dei sistemi della CA in modo ininterrotto almeno sufficiente a permettere una chiusura ordinata dei sistemi.

8.1.4. Esposizione all'acqua

Gli edifici che ospitano la CA di TERNA sono situati in posizione soprelevata rispetto a corsi d'acqua di grande portata attuale e potenziale (fiumi e torrenti).
La rete di scarico è dimensionata in modo da assicurare lo smaltimento delle acque anche in condizioni critiche, purché non disastrose.

8.1.5. Misure di prevenzione e protezione dagli incendi

Le misure antincendio sono conformi con la normativa di legge.

8.1.6. Dispositivi di memorizzazione

I supporti dati sono conservati in locali sicuri e ad accesso controllato ed esistono procedure che ne regolamentano la movimentazione.

8.1.7. Gestione dei rifiuti

L'eliminazione del materiale avviene in modo da impedire che i dati riservati possano essere rivelati:

1. i supporti cartacei od ottici contenenti tali dati vengono distrutti;
2. i supporti magnetici vengono smagnetizzati o distrutti;
3. i rifiuti tossici vengono smaltiti nel rispetto delle norme di legge.

8.1.8. Salvataggi in altri luoghi

I log, i dati archiviati e quanto è necessario per garantire la ripartenza in altro sito in caso di disastro viene copiato e conservato in siti remoti e sicuri.

8.2. Sicurezza procedurale

Gli addetti alle mansioni della CA devono essere autenticati per accedere ai sistemi.

8.2.1. Profili

Per non permettere ad una sola persona di effettuare azioni dannose, le responsabilità devono essere suddivise tra più profili ed individui in modo da assicurare che non vi siano conflitti di interessi o di mansioni.
Ogni profilo deve avere capacità proporzionali al proprio ruolo.

8.3. Sicurezza sul personale

8.3.1. Addetti

Il personale addetto ai differenti compiti relativi alla PKI è verificato e controllato dai responsabili della rispettiva struttura organizzativa aziendale.
Il personale addetto alla PKI di TERNA ha le seguenti caratteristiche:

- E' personale dipendente di TERNA 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;
- Ha ricevuto una adeguata formazione relativa al ruolo ricoperto nella PKI;
- Ha sottoscritto una dichiarazione in cui afferma di essere a conoscenza dei propri compiti e delle sanzioni disciplinari previste in caso di violazione dei propri obblighi;
- Ha qualifiche aziendali tali da garantire un'adeguata autonomia decisionale;
- Ha maturato una esperienza almeno quinquennale nell'ambito della conduzione di sistemi informatici.

8.3.2. Formazione del personale

Il personale addetto riceve un'adeguata formazione in funzione dei profili ed in particolare:

- sull'utilizzo delle componenti software e hardware utilizzate;
- sulle misure di sicurezza da adottare in funzione del proprio profilo;
- sulle varie procedure operative;
- sulle procedure da seguire in caso di emergenza.

8.3.3. Frequenza degli aggiornamenti

Almeno ogni anno è predisposto un aggiornamento delle conoscenze degli addetti.

8.3.4. Documentazione

Gli addetti sono forniti di documentazione che espone in modo dettagliato le procedure da seguire per i processi che li vedono coinvolti.

9. Sicurezza tecnica

9.1. Generazione e memorizzazione delle chiavi

9.1.1. Generazione delle chiavi

9.1.1.1. Certification Authority

Le coppie di chiavi della CA vengono generate per via software e memorizzate in modo cifrato nel database della Certification Authority

9.1.1.2. Titolari

La generazione delle chiavi di firma viene effettuata dai titolari con dispositivi crittografici hardware (e.g. Smart Card) o su file protetto da password .
Le coppie di chiavi di cifratura sono generate dalla CA con applicazione certificata FIPS 140-1 al livello 3.

9.1.1.3. Applicativi

La generazione delle chiavi di firma o di autentica viene effettuata dai titolari su file protetto da password o in un formato proprietario relativo all'applicativo che la utilizza.

9.1.2. Rilascio della chiave privata al titolare

Nel caso della coppia di chiavi di firma o di autentica non è applicabile: ogni titolare genera la proprio coppia di chiavi all'interno del dispositivo di firma, su un file o in modo proprietario a seconda dell'applicazione che la utilizza..
La coppia di chiavi di cifra è generata dalla CA e la chiave privata viene inviata al client dell'utente lungo un canale sicuro (RFC 2510).

9.1.3. 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

- nel caso di titolari interni o esterni rispetta un protocollo RFC (PKIX-CMP) di gestione dei certificati;
- nel caso di applicativi avviene con il download della richiesta di certificato in formato PKCS10;
- nel caso di apparati IPSEC rispetta il protocollo SCEP.

9.1.4. Rilascio della chiave pubblica della CA ai titolari

Le metodologie di rilascio della chiave pubblica di certificazione possono essere una tra quelle indicate di seguito:

- durante la sessione di certificazione utilizzando il protocollo PKIXCMP;
- durante la sessione di certificazione utilizzando il protocollo SCEP;
- download tramite protocollo http dal sito del Certificazione;
- download tramite protocollo LDAP dalle directory Shadow;
- replica attraverso i meccanismi di distribuzione propri del dominio microsoft.

9.1.5. Dimensione delle chiavi – Algoritmi

L'algoritmo asimmetrico adottato di firma e cifra è lo RSA, utilizzato come specificato nello RFC 2313.
La lunghezza delle chiavi asimmetriche è di almeno 1024 bit.
L'algoritmo di hashing adottato è SHA-1, come da ISO/IEC 10118-3:1998.
Il formato di firma è conforme con la specifica pubblica RFC 2315.

9.1.6. Generatore dei parametri delle chiavi

I parametri delle chiavi di firma sono generati dai microprocessori dei dispositivi di firma, certificati come indicato al capitolo 6.1.1. Quelli delle chiavi di cifra sono generati dalla CA con un'applicazione certificata FIPS 140-1 al livello 3.

9.1.7. Controllo della qualità dei parametri

Si veda quanto detto al punto precedente.

9.1.8. Generazione delle chiavi in hardware

Si veda quanto indicato nei paragrafi precedenti.

9.1.9. Utilizzo dei certificati

L'uso dei certificati è previsto come segue:

- certificati di firma: per la sottoscrizione non ripudiabile ed autenticazione
- certificati di cifra: per la cifratura
- certificati di firma della CA: per la firma dei certificati e delle CRL

9.2. Protezione delle chiavi private

9.2.1. Standard per il modulo di cifratura

L'eventuale dispositivo crittografico utilizzato dai titolari è certificato FIPS
La chiave privata della CA è conservata registrata cifrata con algoritmo affidabile.
Se la chiave di firma della CA viene esportata, per motivi di backup/recovery, viene cifrata con un algoritmo e lunghezza di chiave affidabile.

9.2.2. Escrow delle chiavi private

Non è effettuato escrow delle chiavi private di firma o autentica dei titolari e degli applicativi.

9.2.3. Backup delle chiavi private

Non è effettuato backup delle chiavi private di firma o autentica dei titolari e degli applicativi.
Per le chiavi private di cifratura dei titolari viene effettuata una copia di backup che consente sia di recuperare la chiave di cifratura in vigore (ad esempio per lo smarrimento dei codici 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 sia intervenuta la sostituzione della coppia di chiavi di cifratura del titolare.
Le chiavi private della CA sono memorizzate in modo sicuro nel db della CA stessa. Le policy di backup seguono quelle della base dati della CA stessa.

9.2.4. Archiviazione delle chiavi private di cifratura

In aggiunta a quanto specificato al paragrafo precedente si chiarisce che, proprio perché le chiavi di cifra dei titolari sono conservate dalla CA per motivi di backup, esse vengono anche archiviate insieme con gli altri dati della CA.

9.2.5. Inserimento della chiave privata nei moduli crittografici

La chiave privata di firma dei titolari viene generata all'interno del dispositivo di firma.
La chiave privata di cifra dei titolari viene generata dalla CA e comunicata in modo sicuro al client software dei titolari, il quale lo inserisce in modo sicuro nel dispositivo di firma.
La CA non adottano dispositivi crittografici.

9.2.6. Attivazione della chiave privata

Le chiavi private vengono utilizzate esclusivamente dal Sistema Operativo dei dispositivi crittografici a fronte di un processo di login dove la passphrase del titolare è richiesta e convalidata.
Per attivare la chiave privata della CA è richiesto almeno il dual control.

9.2.7. Disattivazione della chiave privata

La disattivazione della chiave privata è una componente del processo di logout. Il logout deve avvenire automaticamente a fronte di un periodo di inattività di durata predefinita.

9.2.8. Distruzione della chiave privata

I titolari sono tenuti a restituire i dispositivi di firma assegnati loro e comunque ad azzerare le chiavi private in essi contenute.

9.3. Altri aspetti di gestione delle chiavi

9.3.1. Archiviazione delle chiavi pubbliche

Si rimanda ai paragrafi precedenti.

9.3.2. Ciclo di vita delle coppie di chiavi

La durata delle coppie di chiavi di firma, autentica e cifra è definita nel riferimento "Profilo dei Certificati"
La durata delle chiavi di firma della CA è stabilita nella CPS.

9.4. Dati per l'attivazione delle chiavi

9.4.1. Generazione e installazione dei dati di attivazione

9.4.1.1. Certification Authority

Gli addetti di TERNA stabiliscono autonomamente i codici per l'attivazione della CA.

9.4.1.2. Titolari

Ai titolari vengono comunicati in modo sicuro i codici per attivare il processo di certificazione, durante il quale essi stabiliscono autonomamente i codici per la successiva attivazione del proprio profilo crittografico.

9.4.2. Protezione dei codici di attivazione

Sono previste norme per la gestione protetta dei codici di attivazione da parte degli addetti alla CA e dei titolari.

9.5. Sicurezza dei computer

9.5.1. Requisiti specifici per la sicurezza dei computer

Sui sistemi di CA e sugli altri sistemi della PKI sono installati prodotti per la protezione contro i virus. Sono inoltre previste specifiche procedure per il change management.

9.5.2. Valutazione della sicurezza dei computer

Il sistema operativo dei sistemi di elaborazione utilizzati per la generazione delle chiavi, la generazione dei certificati e la gestione del registro dei certificati è sottoposto a procedure di Hardening che ne consentono di aumentare i livelli di sicurezza.

9.6. Controlli sul ciclo di vita

Tutti i sistemi della PKI sono svuotati di ogni dato riservato quando vengono dismessi dalle funzioni di PKI.

9.7. Sicurezza della rete

I sistemi della PKI sono protetti tramite firewall configurati in modo tale da accettare solamente i protocolli ed i comandi richiesti per i servizi necessari alla CA e sono controllati mediante sistemi IDS costantemente monitorati.

9.8. Controlli sullo sviluppo dei dispositivi crittografici

Nessuna disposizione.

10. Profili di Certificati e CRL

10.1. Profilo dei certificati

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

10.1.1. Versione

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

10.1.2. Extension dei certificati

Sono ammesse extension previste dallo RFC 2459.

10.1.3. OID degli Algoritmi utilizzati

Gli OID degli algoritmi di firma, basati sugli algoritmi asimmetrici e di hashing elencati di seguito, sono quelli indicati nello RFC 2459 o in suoi aggiornamenti.
L'algoritmo asimmetrico utilizzato è:

- RSA (Rivest-Shamir-Adleman) utilizzato come da PKCS#1 (RFC 2313).

Gli algoritmi di hashing utilizzati sono:

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

Gli OID degli algoritmi di cifratura simmetrici utilizzati sono:

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

10.1.4. Formato dei nomi

Il DN prevede l'uso dei seguenti componenti: Country, Organization, Organization Unit, Common Name, Serial Number. Si faccia riferimento al documento "Profilo dei Certificati" per ulteriori informazioni.

10.1.5. Restrizioni sui nomi

I nomi debbono essere assegnati in modo compatibile con lo specifico DIT subtree attribuito.

10.1.6. Certificate Policy OID

Nessuna disposizione.

10.1.7. Uso della extension Policy Constraints

Questa estensione può essere utilizzata per limitare la validità dei certificati solo a quelli rilasciati da CA con le quali TERNA abbia in vigore un accordo di mutua certificazione.

10.1.8. Altre Estensioni

Si faccia riferimento al documento “Profilo dei Certificati” per ulteriori informazioni.

10.2. Profilo della CRL

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

10.2.1. Versione della CRL

La versione della CRL X.509 v2, o successivi aggiornamenti.

10.2.2. CRL ed extension della CRL

Sono ammesse extension previste dallo RFC 2459.

11. Amministrazione delle policy

Questa CP è rivista almeno ogni anno, a meno di eventi particolari che ne richiedano una revisione non pianificata.

11.1. Procedure per l'emissione di nuove versioni

E' consentita l'emissione di nuove CP a fronte di nuove tipologie di certificati, di titolari, di applicazioni per le quali siano utilizzabili i certificati.
E' previsto venga assegnato un nuovo codice identificativo alle policy modificate qualora l'impatto delle variazioni sia di natura rilevante.

11.1.1. Elementi modificabili senza preavviso

Sul presente documento CP è possibile effettuare solo le seguenti modifiche senza avvisare le entità interessate:

- Editoriali;
- Correzioni tipografiche;
- Riferimenti a persone o organizzazioni.

11.1.2. Elementi che possono essere modificati solo con preavviso

1. Ogni elemento presente in questo documento può essere modificato con 90 giorni di preavviso;
2. Variazioni ad elementi che non hanno un impatto sostanziale sull'infrastruttura PKI possono essere effettuate con 30 giorni di preavviso;
3. A seguito di circostanze eccezionali possono essere effettuate delle variazioni con l'obbligo di notificarle entro 5 giorni dalla data di aggiornamento.

11.2. Notifica delle variazioni

11.2.1. Destinatari dell'informativa

Tutte le variazione proposte devono essere portate a conoscenza di:

- CA con cui sia in vigore un accordo di cross certification
- Titolari

Le informazioni sono pubblicate su Web server all'indirizzo www.nunloso.it e possono essere trasmesse per posta elettronica.
I Titolari che non accettino la nuova CP dovranno chiedere la revoca dei propri certificati. Finché tale richiesta non verrà ricevuta, le modifiche alle CP si riterranno accettate dai titolari.

11.2.2. 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 1 del capitolo 11.1.2;
- entro 15 giorni nel caso di variazioni di cui al punto 2 del capitolo 11.1.2;

11.2.3. Gestione dei commenti

I commenti alle variazioni sono sottoposti all'attenzione delle figure responsabili della definizione dei documenti CP e CPS indicate ai paragrafi precedenti, le quali sono libere di applicare o meno i suggerimenti forniti dagli utenti.
I commenti ricevuti archiviati secondo quanto definito ai paragrafi precedenti.

11.2.4. Applicazione delle correzioni

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

11.3. Approvazione delle CP

Nessuna disposizione.