

# **EuroPKI Certificate Policy**

***VERSIONE 1.1***

Gennaio 2004

**OID: 1.3.6.1.4.1.5255.1.1.1**

**© EuroPKI (2000-2004)**

## Revisione del documento

Data	Note editoriali
15 Ottobre 2000	Prima versione del documento
26 Febbraio 2004	Correzione di alcuni errori ortografici e sintattici.

# INDICE

<b>REVISIONE DEL DOCUMENTO .....</b>	<b>2</b>
<b>INDICE.....</b>	<b>3</b>
<b>1 INTRODUZIONE.....</b>	<b>7</b>
1.1 INFORMAZIONI GENERALI.....	7
1.2 IDENTIFICAZIONE .....	7
1.3 COMUNITÀ E APPLICABILITÀ .....	8
1.3.1 Autorità di Certificazione (CA) .....	8
1.3.2 Autorità di Registrazione (RA) .....	8
1.3.3 Entità finali.....	8
1.3.4 Applicabilità .....	8
1.4 DETTAGLI SUL CONTATTO .....	9
1.4.1 Specificazione – amministrazione - organizzazione .....	9
1.4.2 Referente.....	9
1.4.3 Persona addetta all'accertamento della conformità della CPS alla presente policy .....	9
<b>2 DISPOSIZIONI GENERALI.....</b>	<b>9</b>
2.1 DOVERI .....	10
2.1.1 Doveri della CA.....	10
2.1.2 Doveri delle RA .....	10
2.1.3 Doveri del sottoscrittore.....	10
2.1.4 Doveri di terze parti coinvolte.....	11
2.1.5 Obblighi per l'Archiviazione .....	11
2.2 RESPONSABILITÀ.....	11
2.2.1 Responsabilità della CA .....	11
2.2.2 Responsabilità della RA.....	11
2.3 RESPONSABILITÀ FINANZIARIA .....	11
2.3.1 Indennizzo da parte delle parti coinvolte .....	11
2.3.2 Relazioni fiduciarie .....	11
2.3.3 Processi amministrativi.....	11
2.4 INTERPRETAZIONE E APPLICAZIONE .....	12
2.4.1 Legge vigente.....	12
2.4.2 Divisibilità, sopravvivenza, fusioni, avvisi .....	12
2.4.3 Procedure di risoluzione di una disputa.....	12
2.5 COMMISSIONI.....	12
2.5.1 Commissioni per il rilascio o il rinnovo di certificati.....	12
2.5.2 Commissioni per l'accesso ai certificati.....	12
2.5.3 Commissioni per la revoca o l'accesso alle informazioni sullo status .....	12
2.5.4 Commissioni per altri servizi quali, a esempio, informazioni circa la policy .....	12
2.5.5 Rimborso .....	12
2.6 PUBBLICAZIONE E ARCHIVIAZIONE .....	12
2.6.1 Pubblicazione delle informazioni circa la CA.....	12
2.6.2 Frequenza delle pubblicazioni.....	13
2.6.3 Controlli di accesso.....	13
2.6.4 Archivi .....	13
2.7 CERTIFICAZIONE DI CONFORMITÀ .....	13
2.7.1 Frequenza dell'accertamento di conformità delle entità.....	13
2.7.2 Identità/qualifiche dell'addetto all'accertamento .....	13
2.7.3 Rapporti tra l'addetto all'accertamento e la parte accertata.....	13
2.7.4 Argomenti interessati dall'accertamento.....	13
2.7.5 Provvedimenti in caso di deficienza .....	13
2.7.6 Comunicazione dei risultati.....	13
2.8 CONFIDENZIALITÀ.....	14
2.8.1 Tipi di informazioni da ritenere confidenziali .....	14
2.8.2 Tipi di informazioni non considerate confidenziali .....	14
2.8.3 Divulgazione delle informazioni sulla revoca o sulla sospensione dei certificati .....	14

2.8.4 Rilascio delle informazioni ad ufficiali giudiziari .....	14
2.8.5 Rilascio delle informazioni per un processo giudiziario .....	14
2.8.6 Divulgazione delle informazioni su richiesta del titolare.....	14
2.8.7 Altri casi di divulgazione delle informazioni.....	14
2.9 DIRITTI DI PROPRIETÀ INTELLETTUALE .....	14
<b>3 IDENTIFICAZIONE E AUTENTICAZIONE.....</b>	<b>15</b>
3.1 REGISTRAZIONE INIZIALE .....	15
3.1.1 Tipi di nomi.....	15
3.1.2 Necessità di nomi significativi.....	15
3.1.3 Regole per interpretare diversi formati di nomi.....	15
3.1.4 Unicità dei nomi .....	15
3.1.5 Procedura per la risoluzione di dispute per il reclamo del nome.....	15
3.1.6 Riconoscimento, autenticazione e ruolo dei marchi.....	15
3.1.7 Metodo per verificare il possesso di una chiave privata .....	15
3.1.8 Autenticazione dell'identità di un'organizzazione.....	16
3.1.9 Autenticazione di identità singole.....	16
3.2 RINNOVO DELLE CHIAVI.....	16
3.3 RINNOVO DELLE CHIAVI DOPO LA REVOCA.....	16
3.4 RICHIESTA DI REVOCA .....	16
<b>4 REQUISITI OPERATIVI.....</b>	<b>17</b>
4.1 PROCEDURE DI RICHIESTA DI UN CERTIFICATO .....	17
4.2 RILASCIO DI UN CERTIFICATO.....	17
4.3 ACCETTAZIONE DI UN CERTIFICATO .....	17
4.4 SOSPENSIONE E REVOCA DI UN CERTIFICATO.....	17
4.4.1 Circostanze per la revoca.....	17
4.4.2 Chi può richiedere la revoca.....	18
4.4.3 Procedura per la richiesta di revoca.....	18
4.4.4 Periodo di attesa per la richiesta di revoca .....	18
4.4.5 Circostanze per la sospensione .....	18
4.4.6 Chi può richiedere la sospensione.....	18
4.4.7 Procedura per la richiesta di sospensione .....	18
4.4.8 Limiti al periodo di sospensione.....	18
4.4.9 Frequenza di rilascio di una CRL (se applicabile).....	19
4.4.10 Requisiti di controllo di una CRL.....	19
4.4.11 Disponibilità di revoca on-line e verifica dello status.....	19
4.4.12 Requisiti di verifica per la revoca on-line .....	19
4.4.13 Altre forme di avviso di revoca disponibili.....	19
4.4.14 Requisiti di verifica su altre forme di avviso di revoca .....	19
4.5 PROCEDURE DI ACCERTAMENTO DELLA SICUREZZA .....	19
4.5.1 Tipi di casi registrati .....	19
4.5.2 Frequenza nel controllo del registro degli eventi.....	19
4.5.3 Periodo di conservazione del registro degli accertamenti .....	19
4.5.4 Protezione del registro degli accertamenti.....	19
4.5.5 Procedure di salvataggio del registro degli accertamenti.....	19
4.5.6 Sistema di raccolta degli accertamenti (interno vs esterno).....	19
4.5.7 Notifica al soggetto causa dell'evento.....	20
4.5.8 Valutazione del livello di vulnerabilità.....	20
4.6 ARCHIVIAZIONE DELLE INFORMAZIONI .....	20
4.6.1 Tipi di eventi registrati .....	20
4.6.2 Periodo di conservazione in archivio .....	20
4.6.3 Protezione dell'archivio .....	20
4.6.4 Procedure di salvataggio dell'archivio .....	20
4.6.5 Requisiti per la marca temporale delle informazioni .....	20
4.6.6 Sistema di raccolta in archivio (interno o esterno).....	20
4.6.7 Procedure per ottenere e verificare le informazioni dell'archivio .....	20
4.7 CAMBIO DI CHIAVI.....	21
4.8 PROCEDURE DI RECUPERO IN CASO DI COMPROMISSIONI O CATASTROFI.....	21
4.8.1 Risorse del computer, software, e/o i dati corrotti .....	21
4.8.2 La chiave pubblica dell'entità viene revocata.....	21
4.8.3 La chiave dell'entità è compromessa .....	21

4.8.4 Sicurezza del sito dopo una catastrofe naturale o di altro tipo .....	21
4.9 CESSAZIONE DI ATTIVITÀ DELLA CA.....	21
<b>5 CONTROLLI DI SICUREZZA FISICA, PROCEDURALE E DEL PERSONALE.....</b>	<b>22</b>
5.1 CONTROLLI FISICI.....	22
5.1.1 Posizione e costruzione del sito.....	22
5.1.2 Accesso fisico.....	22
5.1.3 Alimentazione e climatizzazione.....	22
5.1.4 Esposizioni all'acqua.....	22
5.1.5 Protezione e prevenzione dagli incendi.....	22
5.1.6 Supporto di memorizzazione.....	22
5.1.7 Smaltimento dei rifiuti.....	22
5.1.8 Recupero.....	22
5.2 CONTROLLI PROCEDURALI.....	22
5.2.1 Ruoli fidati.....	22
5.2.2 Numero delle persone richieste per ogni compito.....	22
5.2.3 Identificazione e autenticazione per ogni ruolo.....	23
5.3 CONTROLLO DEL PERSONALE.....	23
5.3.1 Formazione, qualifiche, esperienza e requisiti per l'accesso.....	23
5.3.2 Procedure di controllo della formazione.....	23
5.3.3 Requisiti per la riqualificazione.....	23
5.3.4 Frequenza e requisiti di riqualificazione.....	23
5.3.5 Frequenza e sequenza dei turni di lavoro.....	23
5.3.6 Sanzioni per azioni non autorizzate.....	23
5.3.7 Requisiti di assunzione del personale.....	23
5.3.8 Documentazione fornita al personale.....	23
<b>6 CONTROLLI DI SICUREZZA TECNICA .....</b>	<b>23</b>
6.1 GENERAZIONE E INSTALLAZIONE DELLA COPPIA DI CHIAVI.....	23
6.1.1 Generazione della coppia di chiavi.....	23
6.1.2 Consegna di una chiave privata a un'entità.....	24
6.1.3 Invio della chiave pubblica presso l'ente certificatore.....	24
6.1.4 Consegna della chiave pubblica della CA agli utenti.....	24
6.1.5 Dimensioni delle chiavi.....	24
6.1.6 Parametri per la generazione della coppia di chiavi.....	24
6.1.7 Controllo della qualità dei parametri.....	24
6.1.8 Generazione di una chiave in hardware o in software.....	24
6.1.9 Ambito di utilizzo di una chiave (come previsto dal campo keyUsage nel formato X.509 v3).....	24
<b>CERTIFICATI DELLA CA.....</b>	<b>25</b>
6.2 CUSTODIA DELLA CHIAVE PRIVATA.....	25
6.2.1 Standard per i moduli crittografici.....	25
6.2.2 Controllo multi-persona della chiave privata (n su m parti).....	25
6.2.3 Deposito garantito della chiave privata.....	25
6.2.4 Copie di riserva della chiave privata.....	25
6.2.5 Archiviazione di chiavi private.....	25
6.2.6 Inserimento della chiave privata in un modulo crittografico.....	25
6.2.7 Metodo di attivazione della chiave privata.....	26
6.2.8 Metodo di disattivazione di una chiave privata.....	26
6.2.9 Metodo di distruzione di una chiave privata.....	26
6.3 ALTRI ASPETTI NELLA GESTIONE DELLA COPPIA DI CHIAVI.....	26
6.3.1 Archiviazione delle chiavi pubbliche.....	26
6.3.2 Periodi di utilizzo delle chiavi pubbliche e private.....	26
6.4 DATI DI ATTIVAZIONE.....	26
6.4.1 Generazione e installazione dei dati di attivazione.....	26
6.4.2 Protezione dei dati di attivazione.....	26
6.4.3 Altri aspetti dei dati di attivazione.....	26
6.5 CONTROLLI DI SICUREZZA DEL COMPUTER.....	26
6.5.1 Specifici requisiti tecnici per la sicurezza del computer.....	26
6.5.2 Valutazione del grado di sicurezza del computer.....	27
6.6 CONTROLLI TECNICI DEL CICLO DI VITA.....	27

6.6.1 Controlli per lo sviluppo del sistema.....	27
6.6.2 Controlli per la gestione della sicurezza.....	27
6.6.3 Valutazione del grado di sicurezza per il ciclo di vita.....	27
6.7 CONTROLLI DI SICUREZZA DELLA RETE.....	27
6.8 CONTROLLI SULLA PROGETTAZIONE DEL MODULO CRITTOGRAFICO.....	27
<b>7 PROFILI DEI CERTIFICATI E DELLE CRL.....</b>	<b>27</b>
7.1 PROFILO DEI CERTIFICATI.....	27
7.1.1 Numero(i) di Versione.....	27
7.1.2 Estensioni dei certificati.....	27
7.1.3 Codici identificativi dell' algoritmo.....	28
7.1.4 Formato dei nomi.....	28
7.1.5 Vincoli sui nomi.....	28
7.1.6 Codice identificativo della policy di certificazione.....	28
7.1.7 Utilizzo dell'estensione relativa ai vincoli sulle policy.....	28
7.1.8 Sintassi e semantica degli identificatori delle policy.....	28
7.2 PROFILO DELLE CRL.....	28
7.2.1 Numero(i) di Versione.....	28
7.2.2 CRL ed estensioni delle componenti delle CRL.....	28
<b>8 AMMINISTRAZIONE DELLE SPECIFICHE.....</b>	<b>29</b>
8.1 PROCEDURE PER IL CAMBIAMENTO DELLE SPECIFICHE.....	29
8.2 PUBBLICAZIONE E NOTIFICA.....	29
8.3 PROCEDURE DI APPROVAZIONE DELLA CPS.....	29
<b>APPENDICE 1: GLOSSARIO.....</b>	<b>1</b>
<b>APPENDICE 2: INTERPRETAZIONE DELLE PAROLE CHIAVE UTILIZZATE ALL'INTERNO DEGLI RFC.....</b>	<b>1</b>
<b>RIFERIMENTI.....</b>	<b>1</b>

# 1 Introduzione

EuroPKI è un'organizzazione no-profit nata per creare e sviluppare un'infrastruttura di certificazione a chiave pubblica di respiro europeo.

EuroPKI trae le sue origini dalle PKI stabilite nel progetto ICE-TEL e successivamente sviluppata dal progetto ICE-CAR. Entrambi i progetti sono stati finanziati dalla Commissione Europea nell'ambito del programma Telematics for Research.

Ulteriori informazioni sono disponibili sul sito <http://www.europki.org/ca/root/>

La struttura del presente documento è conforme all'RFC-2527 [1]. Di conseguenza sono presenti alcune sezioni per mera compatibilità anche se non si applicano specificamente ai servizi offerti da EuroPKI. L'Appendice 1 fornisce un glossario dei termini usati nel presente documento e basato principalmente sull'RFC-2527.

All'interno di questo documento, le parole "DEVE", "NON DEVE", "RICHiesto", "DOVRÀ", "NON DOVRÀ", "DOVREBBE", "NON DOVREBBE", "RACCOMANDATO", "PUÒ", "OPZIONALE" vanno interpretate in accordo con l'RFC-2119 [2] (cfr. Appendice 2).

L'espressione "CA conforme" è usata per indicare una CA il cui comportamento è conforme alle disposizioni specificate in tale documento.

## 1.1 Informazioni generali

Questo documento sancisce una serie di regole che stabiliscono l'applicabilità di un certificato rilasciato dalla CA alla propria comunità di utenti e/o classe di applicativi in possesso dei comuni requisiti di sicurezza.

Una Certificate Policy PUÒ essere usata dall'utente di un certificato come ausilio per decidere se un certificato, e suoi allegati, sia sufficientemente affidabile per una particolare applicazione. Un certificato basato sullo standard X.509 Versione 3, rilasciato da una CA conforme, DOVREBBE contenere un riferimento alla Policy utilizzata. Informazioni più dettagliate circa le modalità che una CA conforme adotta nelle sue operazioni di emissione dei certificati possono essere reperite nelle Certification Practice Statements (CPS).

Ogni CA conforme DEVE rilasciare la propria CPS, al fine di fornire informazioni ai potenziali clienti della CA circa i fondamenti tecnici, procedurali e legali che non sono specificati nella presente policy.

## 1.2 Identificazione

Questa Certificate Policy è identificata da un identificativo unico (OID) depositato e indicato qui di seguito:

### 1.3.6.1.4.1.5255.1.1.1

Tale OID si compone delle seguenti parti:

OID assegnato dall'ISO	1
Organizzazione riconosciuta dall'ISO	3
Dipartimento della difesa degli USA	6
Internet	1

Privato	4
Imprese private registrate dalla IANA	1
EuroPKI	5255
Root CA	1
Numero di Versione	1
Numero di Revisione	1

## 1.3 Comunità e applicabilità

Una CA conforme può scegliere liberamente la comunità e l'applicabilità dei certificati rilasciati, ma DEVE specificarle chiaramente nella propria CPS. In ogni caso, essa non deve rilasciare certificati alle entità che non appartengono alla propria comunità o per applicativi che non siano stati valutati accuratamente (per esempio, transazioni B2B ad alto valore). Inoltre, DOVRÀ rispettare tutte le limitazioni imposte dalle successive sezioni di questa policy.

### 1.3.1 Autorità di Certificazione (CA)

Una CA conforme, responsabile del rilascio, deve avere particolare cura nel decidere se una data organizzazione o individuo possa gestire una CA subordinata, attuando tutti i controlli e le verifiche dettagliate in questo documento.

Essa può usare un numero indefinito di RA (registration authorities) e svolgere il ruolo di RA, se l'autenticazione dell'entità può essere fatta dalla stessa CA. Le CA subordinate devono firmare un accordo con la CA addetta alla certificazione, in cui sia previsto l'obbligo di aderire alle sue procedure.

### 1.3.2 Autorità di Registrazione (RA)

Le Autorità di Registrazione (RA) sono necessarie per ottenere l'identificazione e autenticazione fisica delle entità. Le RA NON DEVONO essere autorizzate ad emettere certificati.

Una Registration Authority (RA) è un individuo, oppure un gruppo di persone facenti parte di un'organizzazione o di un'unità organizzativa, accreditati da una CA in qualità di referente per la registrazione di nuove entità finali che chiedono il rilascio di un certificato. Le RA hanno il compito di controllare in modo appropriato l'identità dei richiedenti.

Le RA devono firmare un accordo con la CA che rilascia i certificati, in cui è previsto l'obbligo di aderire alle sue procedure.

### 1.3.3 Entità finali

Le entità finali da certificare nell'ambito di tale policy possono essere persone fisiche (individui o rappresentanti di un'organizzazione) o entità informatiche (es. computer, router, applicazioni) in grado di compiere operazioni crittografiche.

Ogni CA conforme alla presente policy DEVE precisare nella propria CPS chi sono le entità finali che essa è disposta a certificare.

### 1.3.4 Applicabilità

Uno degli obiettivi di questa policy è promuovere un ampio uso dei certificati a chiave pubblica in molti applicativi differenti. Allo scopo di promuovere interoperabilità, la policy incoraggia fortemente le CA a supportare lo standard internazionale di sicurezza S/MIME per

garantire scambi di e-mail sicure. DOVREBBERO, inoltre, essere supportati anche IPsec (per garantire sicurezza di transito in rete) e SSL/TLS (per garantire sicurezza nelle comunicazioni durante il transito, al fine di proteggere i protocolli applicativi quali http, telnet, FTP). E' importante precisare che la policy, per principio, non vuole porre una limitazione a priori all'uso dei certificati, se non nei casi in cui i certificati siano usati in contrasto con la legislazione vigente nei paesi in cui operano le CA addette al rilascio. Tuttavia, al fine di valutare se i certificati rilasciati nell'ambito di tale policy siano adatti a un determinato applicativo, il capitolo 2 "Disposizioni generali" va letto attentamente ed opportunamente compreso.

## 1.4 Dettagli sul contatto

### 1.4.1 Specificazione – amministrazione - organizzazione

In nome della EuroPKI, la presente Policy è interamente gestita dal gruppo di sicurezza TORSEC (<http://security.polito.it>) del Politecnico di Torino, Dipartimento di Automatica e Informatica, Torino, Italia.

### 1.4.2 Referente

Per eventuali chiarimenti circa la presente policy, il referente da contattare é:

indirizzo	EuroPKI Root Certification Authority c/o Prof. Antonio Lioy Politecnico di Torino Dip. di Automatica e Informatica corso Duca degli Abruzzi 24 10129 Torino ITALIA
telefono	0115647021 0115647054
fax	0115647099
URL	<a href="http://www.europki.org/ca/root/">http://www.europki.org/ca/root/</a>
e-mail	<a href="mailto:ca@europki.org">ca@europki.org</a>

### 1.4.3 Persona addetta all'accertamento della conformità della CPS alla presente policy

Al fine di ottenere una valutazione della conformità delle CPS alla presente policy, le CA conformi devono contattare la persona menzionata al punto 1.4.2. Per ulteriori dettagli sulle procedure di approvazione delle CPS, vedere la sezione 8.3

## 2 Disposizioni generali

Questa sezione descrive i doveri delle rispettive parti e offre un prospetto delle responsabilità, e delle emissioni finanziarie ed economiche. Inoltre, una sottosezione affronta il tema della confidenzialità distinguendo le informazioni confidenziali da quelle pubblicamente disponibili e distribuibili. Compare anche un prospetto sulla verifica di conformità.

## 2.1 Doveri

### 2.1.1 Doveri della CA

Una CA DOVRÀ fornire un servizio di Certification Authority.

I principali doveri di una CA sono:

- gestire le richieste di certificazione e l'emissione di nuovi certificati:
  - accettare e confermare le richieste di certificazione da parte di entità richiedenti un certificato in accordo con le procedure previste dalla presente policy e dalla propria CPS;
  - autenticare le entità richiedenti un certificato, possibilmente con l'aiuto di RA separatamente designate;
  - rilasciare certificati sulla base delle richieste autenticate;
  - inviare ai richiedenti notificazione dei certificati rilasciati;
  - rendere pubblicamente disponibili i certificati emessi;
- occuparsi delle richieste di revoca dei certificati e della revoca degli stessi;
  - accettare e confermare le richieste di revoca da parte di entità richiedenti, secondo le procedure contenute nella CPS e nella policy;
  - autenticare entità richiedenti un la revoca di un certificato;
  - rendere le CRL pubblicamente disponibili.

### 2.1.2 Doveri delle RA

Una RA DEVE fornire un servizio di Autorità di Registrazione. Questo prevede:

- autenticazione dell'identità del soggetto;
- convalida della corrispondenza tra una chiave pubblica e l'identità del richiedente, attraverso un metodo di verifica opportuno;
- conferma di tale convalida nei confronti della CA;
- rispetto dell'accordo firmato con la CA.

### 2.1.3 Doveri del sottoscrittore

Un utente DOVRÀ comportarsi nel rispetto della CPS della CA addetta al rilascio di certificati. Tale accordo prevede:

- lettura e rispetto delle procedure concordate;
- opportuna custodia della propria chiave privata, in quanto unico possessore, nel caso in cui la sottoscrizione si riferisca a un singolo utente. Nel caso, invece, di una chiave privata rilasciata per un componente hardware o software, la custodia ed il controllo della chiave possono essere affidati alla responsabilità di più di una persona autorizzata;
- accettazione che nell'utilizzo dei certificati di chiave pubblica la responsabilità della CA sia limitata a quanto specificato nella sezione 2.2;
- autorizzazione al trattamento ed alla conservazione dei dati personali;
- immediata notifica alla CA in caso di compromissione della chiave privata.

### **2.1.4 Doveri di terze parti coinvolte**

Una parte coinvolta DEVE venire a conoscenza della CPS e della presente policy, prima di trarre alcuna conclusione sulla fiducia da riporre nell'utilizzo di un certificato emesso da una CA conforme. Essa, inoltre, DEVE controllare le CRL, al momento di convalidare l'utilizzo dello stesso certificato. In più DEVE utilizzare i certificati solo per gli applicativi proscritti e non DEVE utilizzarli per quelli proibiti.

### **2.1.5 Obblighi per l'Archiviazione**

Ciascuna CA conforme alla presente policy DEVE utilizzare un archivio pubblicamente accessibile dove conservare i certificati e le liste di revoca (CRL).

L'archivio DOVRÀ essere disponibile al pubblico quanto più possibile, compatibilmente con le caratteristiche dell'ente che gestisce tecnicamente la CA.

## **2.2 Responsabilità**

### **2.2.1 Responsabilità della CA**

Una CA conforme PUÒ accettare responsabilità. Considerando che questa policy si propone innanzitutto di promuovere l'adozione di certificati come strumento per aumentare la sicurezza dei computer e della rete per una vasta gamma di applicativi, la sottosezione 1.3.4 stabilisce che non sussistono limitazioni a priori all'utilizzo dei certificati rilasciati. La presente policy, tuttavia, prevede che la responsabilità della CA sia limitata a garantire che vengano effettuati i controlli opportuni per verificare l'identità di ogni richiedente, come descritto nella propria CPS, e ad adottare le minime misure di sicurezza necessarie a custodire la chiave privata della CA. In ogni caso, la lista completa delle responsabilità accettate DEVE essere specificata nella propria CPS.

### **2.2.2 Responsabilità della RA**

Cfr. la sottosezione 2.2.1

## **2.3 Responsabilità finanziaria**

Per quanto stabilito nelle sottosezioni 1.3.4, 2.2.1 e nella sezione 2.5, non è accettata alcuna responsabilità finanziaria per i certificati emessi nell'ambito della presente policy.

### **2.3.1 Indennizzo da parte delle parti coinvolte**

Nessuna specifica.

### **2.3.2 Relazioni fiduciarie**

Nessuna specifica.

### **2.3.3 Processi amministrativi**

Nessuna specifica.

## **2.4 Interpretazione e applicazione**

### **2.4.1 Legge vigente**

La presente policy va interpretata in base alla legge del paese di appartenenza della CA. Tale legge DEVE essere precisata nella propria CPS.

### **2.4.2 Divisibilità, sopravvivenza, fusioni, avvisi**

Nessuna specifica.

### **2.4.3 Procedure di risoluzione di una disputa**

Nessuna specifica.

## **2.5 Commissioni**

### **2.5.1 Commissioni per il rilascio o il rinnovo di certificati**

La presente policy non prevede il pagamento di alcuna commissione per il rilascio dei certificati. Tuttavia, la CA PUÒ riservarsi il diritto di applicarla. In tal caso, l'entità della commissione DEVE essere precisata nella CPS.

### **2.5.2 Commissioni per l'accesso ai certificati**

La presente policy non prevede il pagamento di alcuna commissione per l'accesso ai certificati. Tuttavia, la CA PUÒ riservarsi il diritto di applicarla. In tal caso, l'entità della commissione DEVE essere precisata nella CPS.

### **2.5.3 Commissioni per la revoca o l'accesso alle informazioni sullo status**

La presente policy non prevede il pagamento di alcuna commissione per l'accesso alle informazioni circa la revoca dei certificati o il loro status.

### **2.5.4 Commissioni per altri servizi quali, a esempio, informazioni circa la policy**

La presente policy non prevede il pagamento di alcuna commissione per l'accesso alle informazioni circa la policy e le CPS.

### **2.5.5 Rimborso**

Nessuna specifica.

## **2.6 Pubblicazione e Archiviazione**

### **2.6.1 Pubblicazione delle informazioni circa la CA**

Una CA conforme DOVRÀ rendere disponibile:

- la policy e la CPS in base alle quali opera;
- tutti i certificati emessi, eccetto quelli per i quali i sottoscrittori abbiano richiesto esplicitamente che non vengano divulgati pubblicamente;

- le liste dei certificati firmati ma ritenuti non più validi.

## **2.6.2 Frequenza delle pubblicazioni**

I certificati dovranno essere resi pubblici appena emessi. La frequenza delle pubblicazioni delle CRL è specificata al punto 4.4.9. Allo stesso modo, la policy e le CPS dovranno essere rese pubbliche non appena aggiornate.

## **2.6.3 Controlli di accesso**

NON DOVREBBE essere prevista nessuna politica di accesso alla presente policy, alle CPS e alle CRL. PUÒ essere previsto, invece, il controllo per l'accesso ai certificati (ad esempio, per evitare l'acquisizione di grosse quantità di dati quali indirizzi di e-mail o nel caso in cui la CA decida di applicare commissioni sui servizi di certificazione).

## **2.6.4 Archivi**

DOVRA' essere reso disponibile almeno un archivio per la pubblicazione delle informazioni sopra menzionate.

## **2.7 Certificazione di conformità**

Non è richiesto alcun accertamento di conformità da parte di enti esterni, è comunque prevista una auto-certificazione, da parte dell'organizzazione che svolge il ruolo di CA, che il suo operato sia conforme alla presente policy. In ogni caso, è consentito qualsiasi tipo di controllo di conformità da parte di esterni.

Ciascuna CA conforme può specificare nella propria CPS informazioni più dettagliate circa l'accertamento di conformità.

### **2.7.1 Frequenza dell'accertamento di conformità delle entità**

Nessuna specifica.

### **2.7.2 Identità/qualifiche dell'addetto all'accertamento**

Nessuna specifica.

### **2.7.3 Rapporti tra l'addetto all'accertamento e la parte accertata**

Nessuna specifica.

### **2.7.4 Argomenti interessati dall'accertamento**

Nessuna specifica.

### **2.7.5 Provvedimenti in caso di deficienza**

Nessuna specifica.

### **2.7.6 Comunicazione dei risultati**

Nessuna specifica.

## **2.8 Confidenzialità**

La CA raccoglie e conserva le informazioni personali sugli utenti (es. nome, organizzazione e indirizzo e-mail). Tali informazioni devono essere trattate in modo da assicurare la privacy in base alle leggi vigenti nel paese di appartenenza della CA.

### **2.8.1 Tipi di informazioni da ritenere confidenziali**

Tutte le informazioni sugli utenti, che non siano presenti nel certificato o nella CRL emessa da una CA conforme, sono considerate confidenziali e, pertanto, non devono essere rivelate a terze parti senza esplicita autorizzazione dell'utente.

### **2.8.2 Tipi di informazioni non considerate confidenziali**

Le informazioni incluse nei certificati e nelle CRL disponibili al pubblico ed emessi da una CA conforme non sono considerate confidenziali.

### **2.8.3 Divulgazione delle informazioni sulla revoca o sulla sospensione dei certificati**

Quando un certificato viene revocato o sospeso, un codice esplicativo PUÒ essere incluso nella CRL. Tale nota esplicativa non viene considerata confidenziale e può essere condivisa con tutti gli altri utenti e parti coinvolte. Tuttavia, non viene generalmente rivelato alcun altro dettaglio riguardante la revoca.

### **2.8.4 Rilascio delle informazioni ad ufficiali giudiziari**

Una CA conforme non rivelerà le informazioni personali del sottoscrittore o quelle correlate ai certificati a nessuna terza parte, tranne se richiesto dagli ufficiali giudiziari, dietro regolare mandato.

### **2.8.5 Rilascio delle informazioni per un processo giudiziario**

Nessuna specifica.

### **2.8.6 Divulgazione delle informazioni su richiesta del titolare**

Una CA conforme non rivelerà certificati o informazioni riguardanti i certificati ad alcuna terza parte, tranne su richiesta firmata da parte del titolare.

### **2.8.7 Altri casi di divulgazione delle informazioni**

Nessuna specifica.

## **2.9 Diritti di proprietà intellettuale**

Una CA conforme NON DEVE rivendicare alcun diritto di proprietà intellettuale sui certificati emessi.

Tuttavia, ognuno può copiare la policy e le CPS di EuroPKI a patto di includere un riferimento alla fonte.

## **3 Identificazione e autenticazione**

Questa sezione descrive le procedure utilizzate per l'identificazione e l'autenticazione del richiedente un certificato a una CA o RA prima del suo rilascio. La presente sezione, inoltre, descrive il modo in cui le parti richiedenti il rinnovo o la revoca vengono autenticate. Qui vengono altresì indicate le regole di denominazione, inclusi il riconoscimento della proprietà del nome e la risoluzione delle dispute sul nome.

### **3.1 Registrazione iniziale**

#### **3.1.1 Tipi di nomi**

Gli attributi di identificazione del sottoscrittore, richiesti per l'identificazione e autenticazione del richiedente, variano in base al tipo di certificato richiesto dal sottoscrittore.

Nella scelta dei tipi e del formato dei nomi utilizzati nei campi dei certificati, la policy di EuroPKI è conforme alla RFC 2459 [3].

Una CA conforme deve specificare nella propria CPS i tipi e il formato dei nomi utilizzati.

#### **3.1.2 Necessità di nomi significativi**

Il nome del Soggetto e dell'entità che rilascia un certificato DEVE essere significativo: la CA che rilascia il certificato deve avere una conoscenza appropriata dell'associazione esistente tra i nomi e le entità a cui essi appartengono.

Un indirizzo e-mail incluso nel certificato non deve necessariamente seguire una regola semantica che potrebbe essere utilizzata per identificare una persona e/o un'organizzazione.

#### **3.1.3 Regole per interpretare diversi formati di nomi**

Una CA conforme deve specificare nella propria CPS le regole per interpretare i diversi formati di nomi utilizzati nei certificati.

#### **3.1.4 Unicità dei nomi**

Il DN (Distinguished Name) DEVE essere unico per ogni singola entità certificata da una CA, come definita dal campo del nome dell'entità addetta al rilascio.

#### **3.1.5 Procedura per la risoluzione di dispute per il reclamo del nome**

Le dispute sono gestite ai sensi della legge del paese in cui la CA ha sede.

#### **3.1.6 Riconoscimento, autenticazione e ruolo dei marchi**

Nessuna specifica.

#### **3.1.7 Metodo per verificare il possesso di una chiave privata**

E' fortemente RACCOMANDATA l'adozione di un metodo appropriato per verificare il possesso, da parte del sottoscrittore, della chiave privata corrispondente alla chiave pubblica certificata.

Il metodo adottato DEVE essere descritto dettagliatamente nella propria CPS. Dopo aver scelto il metodo per la verifica del possesso, la CA conforme NON DEVE rilasciare i

certificati per i quali tale verifica sia fallita. La presente policy scoraggia il rilascio di chiavi private, da parte di una CA, come prova di possesso.

### **3.1.8 Autenticazione dell'identità di un'organizzazione**

Ogni volta che un sottoscrittore richiede che il nome di un'organizzazione venga incluso in un certificato, la CA responsabile DEVE avere conferma del fatto che l'organizzazione ne sia effettivamente a conoscenza. Al tal fine la CA DEVE richiederne relativa documentazione. In tutti i casi, i documenti legali probanti i dati da certificare devono essere scambiati utilizzando canali che non contemplino il trasferimento via rete informatica. La CA o l'RA POSSONO eseguire l'autenticazione. I dettagli DEVONO essere specificati nella propria CPS.

### **3.1.9 Autenticazione di identità singole**

In molti casi, i certificati a chiave pubblica costituiscono un mezzo per garantire una sicura autenticazione crittografica delle entità comunicanti. Partendo da tale premessa, la policy di EuroPKI stabilisce che è RICHIESTA l'autenticazione di identità singole. Il metodo di autenticazione RACCOMANDATO richiede che il singolo individuo si presenti personalmente dinanzi alla CA o RA addetta all'autenticazione, mostrando appositi documenti di identificazione (es. passaporto, patente, ecc.). In alternativa possono essere adottati altri metodi di identificazione come, ad esempio, videoconferenze. Se il soggetto da certificare è un componente software, la persona che presenta richiesta deve provare di avere la necessaria autorizzazione (come esempio, si può considerare la richiesta per il web server [www.europki.org](http://www.europki.org): solo le persone direttamente autorizzate dall'addetto alla registrazione del dominio europki.org può presentare tale richiesta). La procedura esatta DEVE essere specificata in dettaglio nella propria CPS.

## **3.2 Rinnovo delle chiavi**

La presente policy non prevede l'obbligo di generazione di una nuova chiave nel processo di rinnovo. Dopo la scadenza di un certificato la CA PUÒ rilasciarne uno nuovo sia per la stessa chiave, sia per una nuova. L'autenticazione della nuova chiave può essere effettuata con la stessa procedura indicata nella sezione 3.1 per la registrazione iniziale o usando richieste firmate digitalmente. Tali richieste devono essere inviate alla CA prima della scadenza del certificato.

Una CA può rilasciare più di un certificato per la stessa chiave.

## **3.3 Rinnovo delle chiavi dopo la revoca**

Una chiave pubblica, il cui certificato sia stato revocato a seguito della compromissione della corrispondente chiave privata, NON DEVE essere ri-certificata. La chiave pubblica PUÒ essere ri-certificata se la revoca è dovuta soltanto a sospensione del certificato. In quest'ultimo caso, l'autenticazione può essere effettuata con la stessa procedura indicata nella sezione 3.1 a proposito della registrazione iniziale o, in alternativa, usando richieste firmate digitalmente. Tali richieste DEVONO essere poi inviate alla CA prima della scadenza del certificato.

## **3.4 Richiesta di revoca**

Per poter accettare una richiesta di revoca, è necessario l'utilizzo di un appropriato metodo di autenticazione. La CA DEVE accettare come richiesta di revoca un messaggio firmato

digitalmente utilizzando un certificato rilasciato sotto la presente policy, non scaduto e non precedentemente revocato. Le stesse procedure adottate per l'autenticazione durante la registrazione iniziale sono considerate altrettanto valide per la richiesta di revoca. POSSONO essere supportate procedure alternative, come ad esempio, la comunicazione sicura del PIN (Personal Identification Number) di revoca.

Le esatte procedure supportate devono essere specificate in dettaglio nella propria CPS.

## **4 Requisiti operativi**

La presente sezione viene utilizzata per specificare i requisiti richiesti alle entità coinvolte nei processi di certificazione e di revoca.

### **4.1 Procedure di richiesta di un certificato**

La presente policy permette di adottare due procedure alternative per la certificazione:

- la certificazione delle entità viene eseguita interamente dalla CA. I dettagli di tale procedura devono essere specificati nella CPS;
- un'entità genera il proprio paio di chiavi e invia alla CA la chiave pubblica e gli altri dati richiesti. Fatto questo, la richiesta DEVE seguire attentamente le procedure specificate in questa policy e nella CPS per l'identificazione e autenticazione.

### **4.2 Rilascio di un certificato**

La CA e l'RA DEVONO accertare scrupolosamente la conformità e la validità dei documenti presentati dai sottoscrittori. Dopo che l'autenticazione è stata eseguita con i metodi specificati nella sezione 3.1, la CA DOVREBBE rilasciare il certificato. In tal caso, la CA DEVE notificare l'avvenuto rilascio al richiedente. Al contrario, nel caso in cui la CA, per qualsiasi ragione, decidesse di non rilasciare il certificato (nonostante i controlli e l'autenticazione risultino corretti), la stessa DOVREBBE notificare le ragioni di tale scelta al richiedente.

### **4.3 Accettazione di un certificato**

Nessuna specifica.

### **4.4 Sospensione e revoca di un certificato**

La CA è responsabile del rilascio e della pubblicazione delle CRL. Nonostante l'RFC 2459 non lo richieda esplicitamente, la CA DEVE rilasciare le CRL ad intervalli regolari. La CA aggiornerà la propria CRL con i dati dei certificati revocati.

#### **4.4.1 Circostanze per la revoca**

Un certificato SARÀ revocato se le informazioni contenute nel certificato appaiono sospette o compromesse. Sono tali le situazioni in cui:

- i dati del sottoscrittore risultino cambiati;
- la chiave privata del sottoscrittore risulti compromessa o sia sospettata di esserlo;
- le informazioni contenute nel certificato siano sospette di non essere accurate;

- il sottoscrittore non abbia rispettato i propri doveri.

#### **4.4.2 Chi può richiedere la revoca**

La CA DEVE accettare una richiesta di revoca effettuata dal titolare del certificato ritenuto non più valido. Tuttavia, la richiesta di revoca PUÒ essere effettuata anche dalla CA che ha rilasciato il certificato o da una RA associata.

Altre entità POSSONO richiedere la revoca, presentando una chiara prova di essere a conoscenza della compromissione della chiave privata o dell'avvenuto cambio dei dati del sottoscrittore.

#### **4.4.3 Procedura per la richiesta di revoca**

L'entità che chiede la revoca DOVRÀ essere opportunamente autenticata. Il metodo di autenticazione deve essere affidabile almeno come quello utilizzato nella procedura di rilascio. La CA DEVE accettare come richiesta di revoca un messaggio firmato digitalmente, utilizzando un certificato rilasciato sotto questa policy, non scaduto e non precedentemente revocato. Una procedura alternativa può prevedere che l'entità richiedente si presenti dinanzi alla RA o alla CA e presenti un documento di identità valido.

Nel caso in cui l'entità sia una CA, quest'ultima deve anche:

- informare i sottoscrittori e le CA mutuamente certificate;
- terminare il servizio di distribuzione dei certificati e delle CRL rilasciati utilizzando la chiave privata compromessa.

#### **4.4.4 Periodo di attesa per la richiesta di revoca**

La CA decide la durata del tempo necessario ad accettare la richiesta di revoca.

#### **4.4.5 Circostanze per la sospensione**

Una CA PUÒ sospendere temporaneamente un certificato su richiesta del sottoscrittore. Al contrario della revoca, la sospensione di un utente consente di riabilitarlo in seguito. In ogni caso ad una CA non è richiesto di offrire il servizio di sospensione.

Le informazioni sulle chiavi pubbliche degli utenti disabilitati POSSONO essere messe a disposizione tramite gli archivi della CA.

#### **4.4.6 Chi può richiedere la sospensione**

Nel caso in cui una CA offra il servizio di sospensione, la CA deve accettare una richiesta di sospensione effettuata dal titolare del certificato da sospendere.

#### **4.4.7 Procedura per la richiesta di sospensione**

L'entità che richiede la sospensione deve essere opportunamente autenticata. La CA deve accettare come richiesta di sospensione un messaggio firmato digitalmente con un certificato non scaduto e non precedentemente revocato rilasciato nell'ambito di questa policy. Una procedura alternativa può richiedere che l'entità si presenti dinanzi alla RA o CA e presenti un documento di identità valido.

#### **4.4.8 Limiti al periodo di sospensione**

Nessuna specifica.

#### **4.4.9 Frequenza di rilascio di una CRL (se applicabile)**

Le CRL devono essere rilasciate dalla CA conforme almeno ogni 40 giorni.

#### **4.4.10 Requisiti di controllo di una CRL**

La parte coinvolta DOVREBBE verificare un certificato alla luce della CRL più recente al fine di convalidare l'utilizzo del certificato.

#### **4.4.11 Disponibilità di revoca on-line e verifica dello status**

La CA può offrire servizio di revoca on-line e verifica dello stato del certificato. Partendo dalla premessa che la presente policy richiede che la CA rilasci una CRL, non è obbligatorio adottare servizi di revoca on-line e di verifica dello stato dei certificati. Tuttavia questa policy suggerisce di prendere in considerazione l'adozione del protocollo OCSP [4] per la fornitura di tale servizio.

#### **4.4.12 Requisiti di verifica per la revoca on-line**

Nessuna specifica.

#### **4.4.13 Altre forme di avviso di revoca disponibili**

Nessuna specifica.

#### **4.4.14 Requisiti di verifica su altre forme di avviso di revoca**

Nessuna specifica.

### **4.5 Procedure di accertamento della sicurezza**

La presente policy riconosce l'importanza delle procedure di accertamento della sicurezza suggerendo che la CA specifichi tutti questi tipi di disposizioni nella propria CPS.

#### **4.5.1 Tipi di casi registrati**

Nessuna specifica.

#### **4.5.2 Frequenza nel controllo del registro degli eventi**

Nessuna specifica.

#### **4.5.3 Periodo di conservazione del registro degli accertamenti**

Nessuna specifica.

#### **4.5.4 Protezione del registro degli accertamenti**

Nessuna specifica.

#### **4.5.5 Procedure di salvataggio del registro degli accertamenti**

Nessuna specifica.

#### **4.5.6 Sistema di raccolta degli accertamenti (interno vs esterno)**

Nessuna specifica.

#### **4.5.7 Notifica al soggetto causa dell'evento**

Nessuna specifica.

#### **4.5.8 Valutazione del livello di vulnerabilità**

Nessuna specifica.

### **4.6 Archiviazione delle informazioni**

La presente sezione specifica il tipo di eventi archiviati da parte della CA e dell'RA ed il metodo con cui tali dati vengono conservati. Per ulteriori dettagli non esplicitamente specificati si faccia il riferimento alla CPS.

#### **4.6.1 Tipi di eventi registrati**

La CA DOVREBBE archiviare:

- le richieste di certificazione corrispondenti ai certificati attualmente rilasciati;
- i certificati rilasciati;
- le CRL rilasciate;
- tutti gli accordi firmati con altre parti (es. RA);
- i documenti raccolti dal sottoscrittore durante la procedura di iscrizione;
- tutti i messaggi di interesse scambiati con l'RA;

Le RA DOVREBBERO archiviare:

- tutte le informazioni di validazione raccolte dal sottoscrittore;
- tutti i relativi messaggi scambiati con la CA.

#### **4.6.2 Periodo di conservazione in archivio**

Il periodo minimo di conservazione in archivio è di 2 anni.

#### **4.6.3 Protezione dell'archivio**

Nessuna specifica.

#### **4.6.4 Procedure di salvataggio dell'archivio**

Nessuna specifica.

#### **4.6.5 Requisiti per la marca temporale delle informazioni**

Nessuna specifica.

#### **4.6.6 Sistema di raccolta in archivio (interno o esterno)**

Nessuna specifica.

#### **4.6.7 Procedure per ottenere e verificare le informazioni dell'archivio**

Nessuna specifica.

## **4.7 Cambio di chiavi**

Nessuna specifica.

## **4.8 Procedure di recupero in caso di compromissioni o catastrofi**

Se la chiave privata di una CA è compromessa o sospettata di esserlo, la CA deve almeno:

- informarne i sottoscrittori, le CA mutuamente certificate e le parti coinvolte;
- terminare il servizio di distribuzione delle CRL e dei certificati rilasciati usando la chiave privata compromessa;
- richiedere la revoca del certificato della CA.

Se la chiave privata della RA è compromessa o sospettata di esserlo, l'RA deve almeno informarne la CA e richiedere la revoca del proprio certificato.

Se la chiave privata di un'entità è compromessa o sospettata di esserlo, l'entità deve almeno informarne le parti coinvolte e richiedere la revoca del proprio certificato.

### **4.8.1 Risorse del computer, software, e/o i dati corrotti**

Nessuna specifica.

### **4.8.2 La chiave pubblica dell'entità viene revocata**

Nessuna specifica.

### **4.8.3 La chiave dell'entità è compromessa**

Nessuna specifica.

### **4.8.4 Sicurezza del sito dopo una catastrofe naturale o di altro tipo**

Nessuna specifica.

## **4.9 Cessazione di attività della CA**

La cessazione di una CA è considerata alla stregua della cessazione permanente di tutti i servizi associati con una CA logica.

Prima che la CA termini il proprio servizio, devono essere completate almeno le seguenti procedure:

- informarne tutti i sottoscrittori, le CA mutuamente certificate, le CA di livello superiore, e le parti coinvolte con cui abbia accordi o altre forme di rapporti stabiliti;
- rendere disponibili al pubblico le informazioni sulla cessazione della propria attività;
- interrompere la distribuzione di certificati e CRL;

Una CA subordinata PUÒ cessare o continuare la propria attività in maniera autonoma.

# **5 Controlli di sicurezza fisica, procedurale e del personale.**

## **5.1 Controlli fisici.**

I requisiti di sicurezza imposti su una CA conforme sono indicati nella CPS. In ogni caso, questa policy stabilisce che la CA DEBBA essere installata su una stazione dedicata e che questa DEBBA essere fisicamente sicura.

### **5.1.1 Posizione e costruzione del sito**

Nessuna specifica.

### **5.1.2 Accesso fisico**

L'accesso fisico al sito nel quale la CA opera DEVE essere concesso soltanto a persone esplicitamente autorizzate.

### **5.1.3 Alimentazione e climatizzazione**

Nessuna specifica.

### **5.1.4 Esposizioni all'acqua**

Nessuna specifica.

### **5.1.5 Protezione e prevenzione dagli incendi**

Nessuna specifica.

### **5.1.6 Supporto di memorizzazione**

Nessuna specifica.

### **5.1.7 Smaltimento dei rifiuti**

Nessuna specifica.

### **5.1.8 Recupero**

Nessuna specifica.

## **5.2 Controlli procedurali**

Tutti i dettagli riguardanti i controlli procedurali, come la definizione dei ruoli di fiducia, devono essere specificati nella CPS.

### **5.2.1 Ruoli fidati**

Nessun accordo

### **5.2.2 Numero delle persone richieste per ogni compito**

Nessun accordo

### **5.2.3 Identificazione e autenticazione per ogni ruolo**

Nessun accordo

## **5.3 Controllo del Personale**

### **5.3.1 Formazione, qualifiche, esperienza e requisiti per l'accesso**

Il personale che opera all'interno della CA deve essere tecnicamente e professionalmente competente. Ogni CA conforme deve approfondire ulteriormente questi aspetti e quelli ad essi collegati nella propria .

### **5.3.2 Procedure di controllo della formazione**

Nessuna specifica.

### **5.3.3 Requisiti per la riqualificazione**

Nessuna specifica.

### **5.3.4 Frequenza e requisiti di riqualificazione**

Nessuna specifica.

### **5.3.5 Frequenza e sequenza dei turni di lavoro**

Nessuna specifica.

### **5.3.6 Sanzioni per azioni non autorizzate**

Nessuna specifica.

### **5.3.7 Requisiti di assunzione del personale**

Nessuna specifica.

### **5.3.8 Documentazione fornita al personale**

Nessuna specifica.

## **6 Controlli di sicurezza tecnica**

### **6.1 Generazione e installazione della coppia di chiavi**

Questa sezione è utilizzata per definire le disposizioni per la gestione delle chiavi e i corrispondenti controlli di sicurezza tecnica.

#### **6.1.1 Generazione della coppia di chiavi**

Le chiavi crittografiche della CA vengono generate dal software scelto per la gestione dei certificati.

Le chiavi crittografiche delle entità finali sono generate localmente dall'applicativo, durante il processo di richiesta, o dalla CA durante la procedura di registrazione. La presente policy suggerisce di adottare la prima procedura per firmare chiavi da utilizzare a scopi di non

ripudio. La seconda procedura può essere adottata per la certificazione di chiavi di cifratura o di mera autenticazione.

### **6.1.2 Consegna di una chiave privata a un'entità**

L'entità PUÒ generare la propria coppia di chiavi. E' importante osservare che nel caso della generazione effettuata dalla CA, la chiave deve essere consegnata all'entità finale in maniera sicura. Ulteriori dettagli DEVONO essere specificati nella CPS.

### **6.1.3 Invio della chiave pubblica presso l'ente certificatore**

Per la certificazione individuale, l'entità invia una richiesta di certificazione contenente la chiave pubblica generata alla CA o all'RA. Ogni CA conforme deve specificare nella propria CPS le esatte procedure di consegna della chiave pubblica.

Le CA conformi DEVONO supportare almeno i formati PKCS#10 e SPKAC. Se la chiave pubblica non viene generata dal sottoscrittore alla presenza del personale della CA/RA allora la CA NON DOVREBBE accettare formati che non forniscano prove di possesso della corrispondente chiave privata.

### **6.1.4 Consegna della chiave pubblica della CA agli utenti**

La CA deve fornire i meccanismi per consegnare la chiave pubblica di una CA agli utenti in maniera affidabile. Ulteriori dettagli devono essere specificati nella CPS.

In ogni caso, le chiavi pubbliche della CA DEVONO essere disponibili al pubblico in un archivio accessibile attraverso protocolli standard, quali HTTP o LDAP.

### **6.1.5 Dimensioni delle chiavi**

La lunghezza minima della chiave privata di un'entità finale da certificare deve essere decisa dalla CA responsabile del rilascio e non deve essere inferiore al valore di 512 bit. Si raccomanda che la chiave abbia una lunghezza minima di 1024 bit.

La coppia di chiavi di una CA deve avere la lunghezza minima di 1024 bit. Si raccomanda di utilizzare una lunghezza non inferiore ai 2048 bit.

### **6.1.6 Parametri per la generazione della coppia di chiavi**

Nessuna specifica.

### **6.1.7 Controllo della qualità dei parametri**

Nessuna specifica.

### **6.1.8 Generazione di una chiave in hardware o in software**

Le chiavi possono essere generate utilizzando una componente software o un dispositivo hardware (es. su un dispositivo crittografico) a seconda dei diversi strumenti disponibili da parte delle entità.

### **6.1.9 Ambito di utilizzo di una chiave (come previsto dal campo keyUsage nel formato X.509 v3)**

Gli scopi per i quali una chiave può essere utilizzata possono essere limitati da una CA attraverso l'inserimento dell'estensione keyUsage nel certificato. Questo campo indica lo scopo per il quale la chiave pubblica certificata viene utilizzata.

I certificati rilasciati nell'ambito di questa policy devono avere l'estensione keyUsage segnata come critica. Ciò significa che il certificato sarà utilizzato soltanto per uno scopo per il quale il corrispondente bit per l'uso della chiave sia fissato al valore uno.

### **Certificati della CA**

Nei certificati della CA l'estensione keyUsage deve contenere i seguenti bit fissati al valore uno:

digitalSignature – nonRepudiation – keyCertSign – cRLSign

Essa PUÒ contenere anche altri bit fissati al valore uno.

## **6.2 Custodia della chiave privata**

### **6.2.1 Standard per i moduli crittografici**

La presente policy non richiede l'adozione dell'utilizzo di un modulo crittografico aderente a standard pre-determinati. Ogni CA può dare nella propria CPS ulteriori dettagli sull'adozione di un modulo standard.

### **6.2.2 Controllo multi-persona della chiave privata (n su m parti)**

La chiave privata di un individuo NON DEVE essere sottoposta a controllo multi-persona (n su m).

Soltanto le chiavi private appartenenti a una CA, a un componente hardware o software POSSONO essere sottoposte a tale tipo di controllo: in tale caso DEVE essere specificato nella CPS.

### **6.2.3 Deposito garantito della chiave privata**

La presente policy scoraggia l'utilizzo di depositi garantiti della chiave privata, sia per le entità finali sia per una CA. Il loro utilizzo può essere autorizzato soltanto se la legge vigente nel paese di appartenenza della CA lo richiede esplicitamente.

### **6.2.4 Copie di riserva della chiave privata**

La presente policy suggerisce che tutte le parti conservino una copia di riserva della propria chiave privata allo scopo di recuperarla in caso di distruzione. Tale copia deve essere accuratamente custodita, specialmente nel caso in cui essa sia relativa ad una CA.

### **6.2.5 Archiviazione di chiavi private**

La presente policy suggerisce di utilizzare una procedura per l'archiviazione per le chiavi utilizzate per la cifratura o decifratura solamente. Infatti può essere necessario conservare una copia della chiave privata allo scopo di decifrare correttamente i messaggi anche nel caso in cui il corrispondente certificato a chiave pubblica sia scaduto.

### **6.2.6 Inserimento della chiave privata in un modulo crittografico**

La chiave privata di tutte le entità DOVREBBE essere conservata in forma cifrata. Tale procedura è particolarmente importante se l'entità è una CA.

### **6.2.7 Metodo di attivazione della chiave privata**

Dettagli specifici sulle procedure di attivazione della chiave privata DOVREBBERO essere presenti nella CPS. Come suggerimento generale, la presente policy raccomanda che, per l'attivazione di una chiave privata, siano inseriti alcuni dati specifici nel modulo crittografico. I dati sull'attivazione devono consistere, almeno, in un PIN o una frase chiave, ma per le chiavi private più importanti (es. quelle appartenenti alle CA) si consiglia l'utilizzo di dispositivi hardware o dati biometrici.

### **6.2.8 Metodo di disattivazione di una chiave privata**

Nessuna specifica.

### **6.2.9 Metodo di distruzione di una chiave privata**

Nessuna specifica.

## **6.3 Altri aspetti nella gestione della coppia di chiavi**

### **6.3.1 Archiviazione delle chiavi pubbliche**

La CA conforme DEVE archiviare tutti i certificati rilasciati. Possono essere utilizzati anche metodi differenti dalla firma digitale per garantirne l'integrità.

### **6.3.2 Periodi di utilizzo delle chiavi pubbliche e private**

Nessuna specifica.

## **6.4 Dati di attivazione**

### **6.4.1 Generazione e installazione dei dati di attivazione**

Le frasi chiave o i PIN devono essere selezionati secondo la "migliore modalità". Ciò significa che è necessario suggerire una lunghezza minima opportuna per le frasi chiave e migliorare i meccanismi per controllare che esse mostrino un elevato grado di entropia.

### **6.4.2 Protezione dei dati di attivazione**

Le frasi chiave, che proteggono le chiavi private, devono essere accessibili soltanto ad utenti autorizzati (ad es. titolare di certificati per uso personale, operatori delle CA per firmare le chiavi delle CA, ecc). Un'eccezione a tale indicazione è l'implementazione di un servizio sicuro di archiviazione/ripristino dei dati di attivazione. Tale meccanismo deve essere chiaramente definito nella CPS.

### **6.4.3 Altri aspetti dei dati di attivazione**

Nessuna specifica.

## **6.5 Controlli di sicurezza del computer**

### **6.5.1 Specifici requisiti tecnici per la sicurezza del computer**

Nessuna specifica.

## **6.5.2 Valutazione del grado di sicurezza del computer**

Nessuna specifica.

## **6.6 Controlli tecnici del ciclo di vita**

### **6.6.1 Controlli per lo sviluppo del sistema**

Nessuna specifica.

### **6.6.2 Controlli per la gestione della sicurezza**

Nessuna specifica.

### **6.6.3 Valutazione del grado di sicurezza per il ciclo di vita**

Nessuna specifica.

## **6.7 Controlli di sicurezza della rete**

La politica di certificazione EuroPKI suggerisce fortemente che la stazione, su cui viene utilizzato il modulo crittografico per le operazioni della CA, sia tenuta scollegata da qualsiasi rete dati per evitare tentativi di accesso non autorizzati. In ogni caso, l'accesso via rete al sistema della CA deve essere limitato per proteggere in modo appropriato la chiave privata della CA dal pericolo di compromissione.

## **6.8 Controlli sulla progettazione del modulo crittografico**

Nessuna specifica.

# **7 Profili dei certificati e delle CRL**

## **7.1 Profilo dei certificati**

Al fine di promuovere l'interoperabilità, la policy EuroPKI incoraggia fortemente la CA conforme a emettere certificati che abbiano il profilo previsto conforme all'RFC 2459. In ogni caso, la CPS deve specificare il profilo specifico adottato.

### **7.1.1 Numero(i) di Versione**

Il campo indicante la versione del certificato DOVRÁ recare almeno il valore 2, cioè una CA conforme DEVE emettere certificati X.509 versione 3 o successive.

### **7.1.2 Estensioni dei certificati**

In accordo con l'RFC 2459, si raccomanda l'inclusione nel certificato delle seguenti estensioni:

NOME DELL'ESTENSIONE	
SubjectKeyIdentifier	NON CRITICA

AuthorityKeyIdentifier	NON CRITICA
BasicConstraints	CRITICA
KeyUsage	CRITICA
CertificatePolicies	NON CRITICA

Si raccomanda, inoltre, l'utilizzo di altre due estensioni: CRLDistributionPoint, per fornire informazioni utili atte a recuperare le CRL e SubjectAltNames nel caso sia necessario includere un indirizzo e-mail RFC822 in un certificato. Entrambe le estensioni dovrebbero essere segnalate come NON CRITICHE.

### **7.1.3 Codici identificativi dell'algoritmo**

Nessuna specifica.

### **7.1.4 Formato dei nomi**

Tutti i problemi inerenti ai formati dei nomi devono essere specificate nella CPS.

### **7.1.5 Vincoli sui nomi**

Tutte i problemi inerenti ai vincoli sui nomi devono essere specificate nella CPS.

### **7.1.6 Codice identificativo della policy di certificazione**

E' possibile utilizzare altri codici identificativi per la policy di certificazione soltanto nel caso in cui le policy identificate risultino conformi alla presente. La CA conforme deve contattare i responsabili delle diverse policy per verificare il livello di conformità reciproca. Tuttavia, al fine di promuovere l'interoperabilità, in accordo con l'RFC 2459, si suggerisce di includere un solo codice di identificazione all'interno dei un certificati.

### **7.1.7 Utilizzo dell'estensione relativa ai vincoli sulle policy**

Tutte i problemi inerenti all'utilizzo dell'estensione relativa ai vincoli sulle policy devono essere specificate nella CPS.

### **7.1.8 Sintassi e semantica degli identificatori delle policy**

L'estensione relativa all'identificazione della policy permette di specificare, assieme a ciascun codice identificativo, alcune informazioni aggiuntive. La presente policy suggerisce che questo campo contenga un puntatore alla Certification Practice Statement (CPS) pubblicata dalla CA.

Il puntatore avrà il formato di un Uniform Resource Identifier (URI).

## **7.2 Profilo delle CRL**

### **7.2.1 Numero(i) di Versione**

Il campo indicante la versione delle CRL deve recare il valore 1, indicando CRL in formato X.509v2.

### **7.2.2 CRL ed estensioni delle componenti delle CRL**

Nessuna specifica.

## **8 Amministrazione delle specifiche**

### **8.1 Procedure per il cambiamento delle specifiche**

E' possibile apportare cambiamenti editoriali alla policy e alla CPS. Eventuali cambiamenti sostanziali della policy devono essere notificati in anticipo a tutte le CA ed agli utenti. Inoltre, tutte le CA devono aggiornare la propria policy in relazione ai cambiamenti apportati ai livelli superiori.

I cambiamenti che implicano modifiche tecniche minori devono essere notificati in anticipo.

### **8.2 Pubblicazione e notifica**

La presente policy è disponibile via Web su: <http://www.europki.org/ca/root/cps>

### **8.3 Procedure di approvazione della CPS**

Le CA DOVRANNO essere valutate in termini di conformità con la presente policy. Al fine di ottenere l'approvazione della CPS, le CA conformi possono sottomettere la propria CPS al referente specificato nella sezione 1.4.3. La CA DOVRÀ attendere la risposta. Il tempo massimo per completare la valutazione è fissato in 60 giorni. Potrebbe essere accettabile che una CA autocertifichi la sua conformità a questa policy; in questo caso se verrà riportata una qualsiasi forma di non conformità ad EuroPKI, il certificato della CA incriminata DOVRÁ essere revocato.

# APPENDICE 1: Glossario

**Certification Authority (CA)** – Un' autorità accreditata da uno o più utenti in relazione alla creazione e assegnazione di certificati a chiave pubblica. La CA può, a sua discrezione, creare le chiavi degli utenti. E' importante osservare che la CA è responsabile dei certificati a chiave pubblica durante tutto il corso della vita, non solo nel momento della loro emissione.

**CA-certificate** - Un certificato a chiave pubblica rilasciata da un'altra CA.

**Certificate policy (CP)** – Una serie di regole identificate che indicano l'applicabilità di un certificato a una particolare comunità e/o classe di applicativi con comuni requisiti di sicurezza. Per esempio, una particolare policy può indicare l'applicabilità di un tipo di certificati all'autenticazione delle transazioni di interscambio dei dati elettronici per il commercio di merci entro un dato intervallo di spesa.

**Certification path** – Una sequenza ordinata di certificati che, insieme con la chiave pubblica dell'oggetto iniziale, può essere elaborata per ottenere quella dell'oggetto finale.

**Certification Practice Statement (CPS)** – Una dichiarazione delle modalità che un' autorità di certificazione adotta nel rilascio dei certificati.

**Certificate revocation list (CRL)** - Una CRL è una lista temporanea su supporto cartaceo che identifica i certificati revocati firmati da una CA e resi liberamente disponibili in un deposito pubblico.

**Issuing certification authority (issuing CA)** – Nel contesto di un particolare certificato, l'issuing CA è la CA che ha emesso il certificato (vedi anche Subject certification authority).

**Public Key Certificate (PKC)** – Una struttura di dati contenente la chiave pubblica di un'entità finale e alcune ulteriori informazioni, digitalmente firmate con la chiave privata della CA che le ha rilasciate.

**Public Key Infrastructure (PKI)** – L'insieme dei componenti hardware e software, le persone, le policy e le procedure necessarie per creare, gestire, immagazzinare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.

**Registration authority (RA)** – Un'entità responsabile dell'identificazione e autenticazione dei certificati in oggetto, ma non della firma e rilascio dei certificati (es. a una RA vengono delegati dati compiti a nome di una CA). [Nota: L'espressione Local Registration Authority (LRA) è utilizzata altrove per indicare lo stesso concetto.]

**Relying party (RP)**– Il beneficiario di un certificato che agisce in fede di quel certificato e/o firme digitali autenticate utilizzando quel certificato. In tale documento, le espressioni "certificate user" e "relying party" sono usate in modo intercambiabile.

**Subject certification authority (subject CA)** – Nel contesto di un particolare CA certificate, la subject CA è la CA la cui chiave pubblica è autenticata nel certificato.

**IPR** – Diritti di proprietà intellettuale.

# Appendice 2: Interpretazione delle parole chiave utilizzate all'interno degli RFC

La RFC 2119 "Key words for use in RFCs to Indicate Requirement Levels", specifica il modo di interpretare le principali parole chiave usate nelle RFC.

Gli studiosi che seguono tali linee guida dovrebbero incorporare tale frase all'inizio dei propri lavori:

Le parole chiave "DEVE", "NON DEVE", "RICHIESTO", "DOVRÀ", "NON DOVRÀ", "DOVREBBE", "NON DOVREBBE", "RACCOMANDATO", "PUÒ", e "OPZIONALE" in questo documento vanno interpretate in accordo con la RFC 2119.

**DEVE** Tale termine, o i termini "RICHIESTO" o "DOVRÀ", significa che la definizione è un requisito assoluto della specificazione.

**NON DEVE** Tale frase, o la frase "NON DOVRÀ", significa che la definizione è una proibizione assoluta della specificazione.

**DOVREBBE** Tale termine, o l'aggettivo "RACCOMANDATO", significa che ci potrebbero essere buone ragioni in particolari circostanze per ignorare un dato elemento, ma le piene implicazioni devono essere comprese e accuratamente vagliate prima di scegliere un termine diverso.

**NON DOVREBBE** Tale frase, o la frase "NON RACCOMANDATO" significa che ci potrebbero essere buone ragioni in particolari circostanze in cui il comportamento particolare è accettabile o addirittura utile, ma le piene implicazioni dovrebbero essere comprese e il caso accuratamente vagliato prima di adottare qualsiasi comportamento descritto da tale frase.

**PUÒ** Tale termine, o l'aggettivo "OPZIONALE", significa che un elemento è davvero opzionale. Un venditore può scegliere di includere l'elemento perché un particolare mercato lo richiede o perché il venditore sente che valorizza il prodotto, mentre un altro venditore può omettere lo stesso elemento. Un'implementazione che non includa una particolare opzione deve essere pronta a interoperare con un'altra implementazione che non includa la stessa opzione, anche se forse dotata di minore funzionalità. Nello stesso senso, un'implementazione che includa una particolare opzione deve essere pronta a interoperare con un'altra implementazione che non includa la stessa opzione (eccetto, ovviamente, per il tipo di opzione).

# Riferimenti

[1] RFC 2527 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” March 1999 [ <ftp://ftp.isi.edu/in-notes/rfc2527.txt> ]

[2] RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels” March 1997 [ <ftp://ftp.isi.edu/in-notes/rfc2119.txt> ]

[3] RFC 2459 “Internet X.509 Public Key Infrastructure: Certificate and CRL Profile” January 1999 [ <ftp://ftp.isi.edu/in-notes/rfc2459.txt> ]

[4] RFC 2560 “Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP” June 1999 [ <ftp://ftp.isi.edu/in-notes/rfc2560.txt> ]