MODELLO DI FUNZIONAMENTO

DELLA CERTIFICATION AUTHORITY

Versione 1.0

Nome doc.:	**SPCoop-Modello FunzionamentoCertificationAuthority v1.0**	Versione:	**1.0**
Data emissione:	**5 marzo 2009**	Stato:	**Pubblicato**

INDICE

1. PREFAZIONE

1.1. Autori

Redatto da:	Laura Paoli Nazzareno Ticconi	RTI
Verificato da:	Nazzareno Ticconi	RTI
Revisione a cura di:	Stefano Fuligni	CNIPA
	Giovanni Olive	CNIPA
	Alessandro Vinciarelli	CNIPA
Approvato da:	Francesco Tortorelli	CNIPA

1.2. Modifiche Documento

Descrizione Modifica	Edizione	Data
Creazione documento	0.0	30 Settembre 2008
Aggiornamento documento relativamente a CA3	0.1	12 Ottobre 2008
Aggiornamento documento a seguito indicazioni CNIPA	0.2	31 Ottobre 2008
Aggiornamento documento dal CNIPA	0.3	3 Novembre 2008
Aggiornamento documento dal CNIPA	0.4	20 Febbraio 2009
Versione Pubblicabile	1.0	20 Febbraio 2009

1.3. Riferimenti

Codice	Titolo

1.4. Acronimi e Definizioni

Sigla	Descrizione
WebRao	Web Registration Authority Officer
CAO	Certification Authority Officer
RA	Registration Authority
WS	Web Service
CRUD	Create, Read, Update, Delete riferito ai dati di registrazione necessari alla produzione di un certificato
OCSP	Online Certificate Status Protocol
AC	Autorità di Certificazione
CRL	Certificate Revocation List
CA	Certification Authority (vedi)

Definizione	Descrizione
Amministratore CA	Persona interna al Centro di Gestione SICA che, oltre ad avere le facoltà dell'operatore CA (vedi) ha la facoltà di inserire registrazioni nel sistema e modificare le stesse per conto del richiedente
Certification Authority	Autorità considerata affidabile da uno o più utenti per creare e assegnare certificati In Italia si preferisce il termine Certificatore come definito dal CAD: :Soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.
Certificate Policy	Un insieme di norme, contraddistinto da un codice, che indica l'applicabilità di un certificato ad una particolare comunità e/o a una classe di applicazioni aventi comuni esigenze di sicurezza.
Certificate Revocation List	Un elenco firmato che riporta un insieme di certificati non più considerati validi dal Certificatore che li ha emessi.
Certificate Suspension List	Lista dei certificati sospesi che generalmente viene inclusa nella CRL
Certification Pratice Statement	Una dichiarazione delle prassi seguite da un Certificatore nell'emettere e gestire certificati.
CP	Certificate Policy (vedi).
CPS	Certification Practice Statement (vedi).
CRL	Certificate Revocation List (vedi).

Definizione	Descrizione
CSL	Certificate Suspension List (vedi)
End Entity	Il Titolare (vedi) di un certificato
HASH	Funzione che prende in input una stringa di lunghezza variabile e ritorna una stringa di lunghezza fissa
HSM	Hardware Security Module Dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione.
LDAP	Lightweight Directory Access Protocol.
Operatore CA	Persona interna al Centro di Gestione SICA che ha la facoltà di sottomettere richieste di certificati, autorizzare emissioni ed emettere I certificati interagendo con la Certification Authority
PKI	Public Key Infrastructure (vedi).
Public Key Infrastructure	Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
RA	Registration Authority (vedi)

Definizione	Descrizione
Registration Authority	Un'entità opzionale di una PKI, (separata dalla CA) che non firma né i certificati né le CRL, ma ha la responsabilità di registrare o verificare alcune o tutte le informazioni necessarie alla CA per emettere i certificati e le CRL e per effettuare altre operazioni di gestione dei certificati. Un'entità opzionale cui è data la responsabilità di effettuare alcune mansioni amministrative necessarie alla registrazione dei Titolari, quali: confermare l'identità del Titolare, confermare che il Titolare ha il diritto che sul suo certificato siano riportati i dati richiesti, verificare che è in possesso della chiave privata associata con la chiave pubblica di cui è richiesta la certificazione.
Referente PA	Figura di responsabile di una Pubblica Amministrazione locale o centrale nell'ambito del sistema SICA
Richiedente	La persona che richiede un certificato mediante i canali preposti. Nell'ambito del sistema SICA la figura del richiedente coincide con il responsabile di una Pubblica Amministrazione locale o centrale per quanto riguarda le operazioni verso la Certification Authority, indicato spesso nei sistemi come "referente PA". Anche un operatore interno SICA autorizzato ad interagire con la Certification Authority può svolgere le funzioni di richiedente-referente nei casi previsti.
RFC	Una RFC (Richiesta di Commenti) è un documento nel quale vengono descritti gli standard attraverso i quali viene regolamentato Internet.
SHA-1	Funzione di hash crittografico a 160 bit
Terzo Interessato	Persona fisica o giuridica, che dà il consenso a che il Titolare richieda che nel certificato siano specificati eventuali poteri di rappresentanza, titoli o cariche rivestite.

Definizione	Descrizione
Titolare	il soggetto intestatario del certificato, sia esso persona fisica o apparato.

2. OBIETTIVI E CONTESTO DI RIFERIMENTO

Il *Sistema Pubblico di Connettività e Cooperazione (SPC)* si colloca nel contesto definito dal Decreto legislativo n° 82 del 7 marzo 2005, pubblicato in G.U. del 16 maggio 2005, n. 112, recante il "**Codice dell'amministrazione digitale**" (C.A.D.) e successive modifiche ed integrazioni. Esso istituisce il SPC, definendone gli obiettivi, le funzionalità ed il modello di governance.

Il processo di regolamentazione normativa del SPC è proseguito nel tempo, arrivando alla pubblicazione del Decreto del Presidente del Consiglio dei Ministri n.1 del 1 aprile 2008, pubblicato in G.U. del 21 giugno 2008, n. 144, recante le **"Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettivita"**, previste dall'art. 71, comma 1-bis, del C.A.D, con il quale viene definito il quadro tecnico di riferimento per lo sviluppo dei servizi SPC e le regole per il funzionamento e l'adesione ai servizi SPC.

Parallelamente, come previsto dal modello condiviso di cooperazione applicativa per la P.A. italiana *SPCoop*, è stato avviato e portato a termine lo sviluppo dei *Servizi Infrastrutturali di interoperabilità, cooperazione ed accesso (SICA)* e del centro di gestione per l'erogazione di tali servizi (CG-SICA), infrastruttura condivisa a livello nazionale che abilita l'interoperabilità e la cooperazione applicativa fra le Amministrazioni pubbliche nonché l'accesso ai servizi applicativi da queste sviluppati e resi disponibili su SPC.

L'evoluzione dello scenario di riferimento e la disponibilità di servizi di infrastruttura per la cooperazione applicativa, hanno reso necessaria la definizione e pubblicazione di una serie di documenti che specificassero in dettaglio le modalità tecniche per l'interoperabilità e la cooperazione applicativa e l'utilizzo dei servizi SICA, come peraltro prevista dalle succitate regole tecniche.

Gli ultimi documenti tecnici relativi al SPCoop rilasciati alla fine del 2005, infatti, definivano un livello di condivisione che consentiva sia la stabilità del modello nel tempo rispetto al contesto organizzativo e tecnologico di riferimento, sia i necessari gradi di libertà per la sua implementazione; ciò a scapito del dettaglio tecnico necessario, invece, nel momento in cui si fa riferimento ad una specifica implementazione del modello ed a specifici servizi infrastrutturali.

I seguenti documenti sono stati redatti dal Raggruppamento Temporaneo di Imprese (IBM-Sistemi Informativi), incaricato dello sviluppo e dell'implementazione del Centro di Gestione dei servizi SICA, con la supervisione del CNIPA, ed hanno origine dalla documentazione sviluppata nel corso del progetto e nella fase di collaudo dei servizi stessi.

L'insieme di documenti prodotti specifica i modelli, le modalità, i dettagli tecnici di realizzazione, gestione ed utilizzo dei servizi SICA, le modalità di interfacciamento, le procedure qualificazione e gestione dei componenti infrastrutturali SPCoop, sulla base di quanto già previsto e definito nei documenti precedentemente condivisi e nel rispetto delle succitate regole tecniche.

Titolo Documento
1. Introduzione ai servizi SICA
2. Specifiche di nomenclatura in SPCoop
3. Specifiche di utilizzo del Servizio di Registro SICA
4. Modalità di funzionamento del Client SICA
5. Struttura dell'Accordo di Servizio e dell'Accordo di Cooperazione
6. Descrizione delle specifiche di sicurezza negli Accordi di Servizio
7. Aspetti di sicurezza applicativa nella cooperazione fra servizi
8. Modalità di funzionamento del Catalogo Schemi e Ontologie
9. Interfacce applicative tra Registro SICA generale e Registri SICA secondari
10. Modalità di Qualificazione del Registro SICA secondario
11. Modalità di Qualificazione della Porta di Dominio
12. Schema d'interoperabilità IndicePA
13. Guida ai servizi IndicePA
14. Modello di Gestione Federata delle Identità Digitali (GFID)
15. Modalità di accreditamento alla GFID
16. Modello di funzionamento dell'Indice dei Soggetti
17. Modello di funzionamento della Certification Authority

2.1. Scopo del documento

Obiettivo del presente documento è quello di illustrare il modello di funzionamento della Certification Authority presente all'interno del sistema SICA in termini di:

- Funzionalità
- Architettura Generale
- Modalità Operative

2.2. Note di lettura del documento

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE,

SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformità con [RFC2119]. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'e proibizione assoluta di implementazione di un determinato elemento di specifica.

2.3. Note sul Copyright

3. INTRODUZIONE

I Servizi SICA costituiscono la piattaforma infrastrutturale che abilita una Pubblica Amministrazione (di seguito PA), alla cooperazione applicativa in ambito SPCoop, offrendo servizi per

- L'accreditamento della PA in SPCoop e la successiva gestione dei dati dell'amministrazione (evoluzione dell'applicazione IPA già esistente).
- L'accreditamento e l'accesso degli utenti della PA ad SPCoop.
- La qualificazione della Porta di Dominio e del Registro Secondario di una PA.
- La pubblicazione e l'adesione agli Accordi di Servizio e di Cooperazione.
- La condivisione dei formati dei dati (rappresentati in schemi XML) utilizzati negli Accordi di Servizio.
- La pubblicazione di concetti (definiti in Ontologie) da associare agli Accordi di Servizio, per una ricerca più efficace degli stessi.
- Servizi di Certificazione digitale

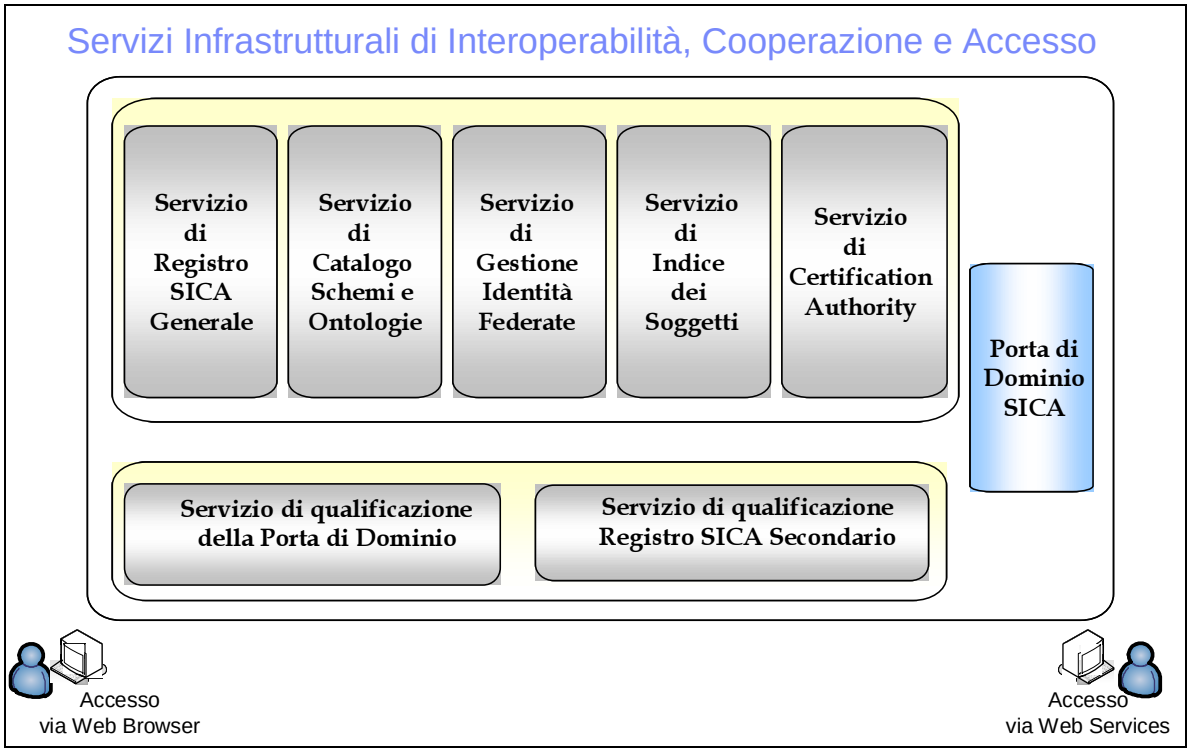

Figura 1 - Schematizzazione dei Servizi SICA

4. FUNZIONALITÀ

Il servizio di Certificazione, attraverso la gestione di due apposite infrastrutture a chiave pubblica denominate CNIPA CA3, il cui certificato radice è automaticamente riconosciuto dai browser di mercato, e CNIPA CA4, ha l'obiettivo di emettere e gestire diverse tipologie di certificati digitali per entità persona e non, da impiegare nei particolari contesti applicativi della Posta Elettronica Certificata e di SPCoop.

Le tipologie di certificati che è possibile emettere attraverso dette infrastrutture di CA, al momento sono:

CNIPA CA4:

- Certificati di SubCA per la certificazione delle AC operanti nel progetto SICA.
- Certificati per OCSP Responder.

- Certificati per l'autenticazione Server.
- Certificati per le PDD (porte di Dominio) e i Registri Secondari.
- Certificati per l'identificazione del Client.
- Certificati di firma XML.
- Certificati per la cifratura dei messaggi.
- Certificati di autenticazione "persona".

CNIPA CA3:

- Certificati di firma delle ricevute PEC.
- Certificati di autenticazione a IGPEC
- Certificati di Web Server.

Il servizio di Certificazione è costituito da:

Un sottosistema PKI: infrastruttura tecnologica di Certification Authority basata su coppie di chiavi asimmetriche e certificati digitali.

Un layer applicativo e di servizi per la CNIPA CA4: in grado di rendere i servizi di certificazione interoperabili e integrabili con il mondo dei servizi di cooperazionee e con il sottosistema PKI.

Il layer è costituito da :

- un Front-End di Registrazione.
- Web Services.

Il Servizio di Certificazione svolgerà principalmente funzionalità di

- Gestione dati di registration Authority .
- Gestione del ciclo di vita dei certificati.
- Gestione dello stato di validità dei certificati.
- Gestione di Sub CA.

Le modalità di utilizzo di tale Servizio possono essere pertanto classificate nelle seguenti tipologie di operazione:

- Registrazione dati nel repository RA.
- Emissione certificati digitali.
- Revoca/ Sospensione /Riattivazione certificati digitali.

- Disponibilità di CRL e OCSP.
- Accreditamento AC.

5. ARCHITETTURA GENERALE

La piattaforma applicativa scelta per realizzare le infrastrutture PKI che emettono i certificati digitali è denominata Unicert ed è fornita dalla Cybertrust Tech. Unicert è dotato di componenti specifiche ed avanzate per l'integrazione con applicazioni esterne sia di tipo sincrono sia di tipo asincrono.

Il sottosistema PKI è suddivisibile in alcune sottocomponenti logiche e infrastrutturali come schematizzato nella figura seguente:

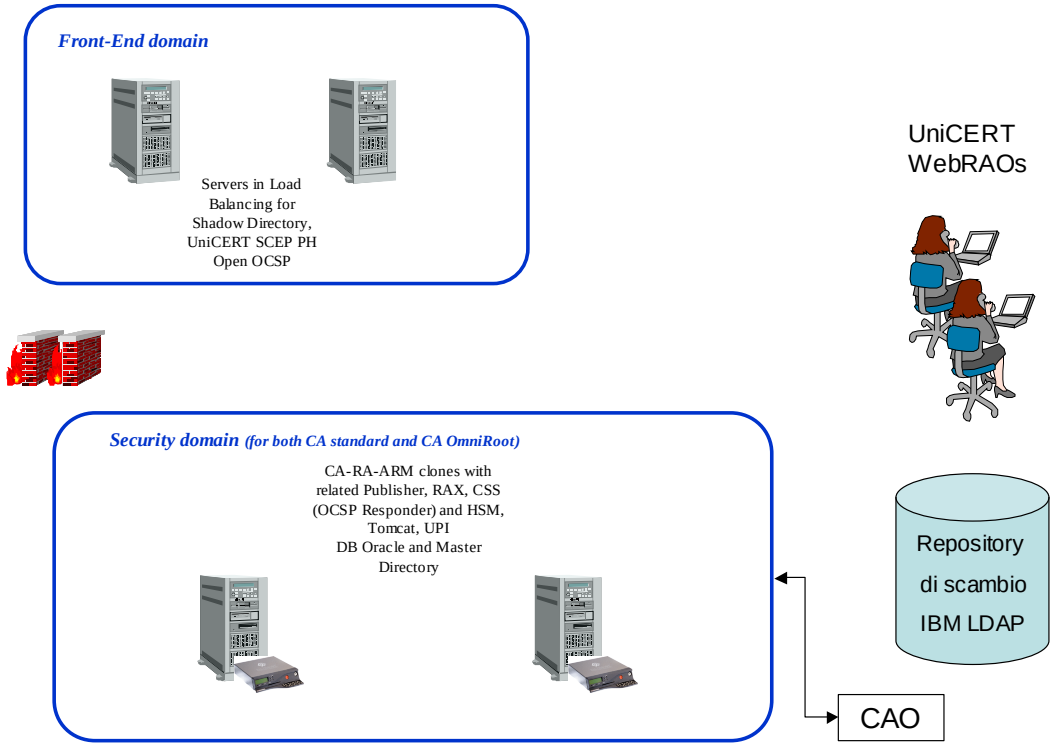

Figura 2 – PKI: Componenti Fisiche

La prima macrocomponente è denominata "Security Domain" e rappresenta il nucleo dei servizi PKI.

L'ambiente si compone della CNIPA CA4 (basata su certificato di root - self signed) che eroga i certificati definiti al cap.4 sulla base delle opportune policy definite, e la CNIPA CA3 che permette l'emissione di certificati web server riconosciuti dai browser più diffusi a livello mondiale, relativi alle funzionalità di PEC.

Le chiavi di certificazione saranno custodite in una coppia di apparati HSM AEP Sureware Keyper Professional.

Il «Security Domain» ospita anche le applicazioni di registrazione e gestione dei certificati:
Unicert RA e Unicert RA Exchange (che interfacciano le componenti WebRAO, UPI e Protocol Handler).

Key Archive Server (KAS).

Unicert Programmatic Interface - UPI (e relativo application server Tomcat) per le richieste di emissione e gestione dei certificati on line da parte dei servizi di front end (Web Services) via http post.

UniCert Publisher (per la pubblicazione dei certificati e delle CRL).

Unicert CSS (Responder OCSP Unicert) che si interfaccia direttamente con l'RDBMS Oracle della CA con funzione di responder interno.

5.1. Moduli Architetturali del Servizio di Certificazione

I moduli architetturali per l'erogazione dei servizi di certificazione e i macro componenti che realizzano tali moduli sono:

- Componente per la registrazione, validazione e archiviazione dei dati:
  - Front End Web/ Interfaccia client remota PA/ WebServices.
  - Repository LDAP.
- Componenti per l'emissione dei certificati, inclusa la profilazione.
  - Front End Web/ Interfaccia client remota PA/ WebServices.
  - Repository LDAP – UPI.
  - Unicert ARM e Unicert WebRAO.
  - Unicert CA e RA.
- Componenti per operazioni di revoca e/o sospensione e OCSP responder.
  - Front End Web / WebServices.
  - UPI.
  - Unicert WebRAO.
  - Unicert CA e RA.

- MS Active Directory (CRL/CSL).
- Unicert CSS (OCSP).
- Servizi di revoca e sospensione via OCSP (OCSP proxy e trasformazione da crl).

- Componenti per le operazioni di accreditamento delle AC.
  - CAO e Unicert per Cross Certification e Firma delle chiavi delle AC.
  - Front End per pubblicazione / upload della TCL prodotta.
- Componenti per la pubblicazione dei certificati.
  - Unicert CA - la pubblicazione dei certificati è definita al livello di policy della CA.
  - Unicert Publisher.
  - MS Active Directory Shadow (LDAP).
  - Front End Web (http / s) mediante allineamento con Directory Shadow.
- Componenti per key-recovery.
  - Unicert KAS.
  - RDBMS.

6. SOGGETTI COINVOLTI NELLA PKI

6.1. Certification Authority

La CA del progetto SICA ha il compito di adempiere alle funzioni di Autorità di Certificazione consistenti in:

- generare certificati contenenti la chiave pubblica dell'entità titolare;
- rendere disponibili i certificati all'entità certificata;
- registrare i certificati in un repository e renderli accessibili a tutti gli attori SICA;
- revocare il certificato, prima della sua scadenza, qualora ciò si renda necessario, inserendo definitivamente il certificato revocato in una lista dei certificati revocati;
- sospendere il certificato, prima della sua scadenza, qualora ciò si renda necessario, inserendo temporaneamente il certificato sospeso in una lista dei certificati sospesi;
- curare la pubblicazione e la distribuzione delle liste dei certificati sospesi e revocati.

6.2. Registration Authority

La funzione Registration Authority del CG-SICA ha il compito di adempiere alle funzioni di Autorità di Registrazione (RA) consistenti in:

- acquisire informazioni necessarie per l'identificazione del titolare di uno o più certificati;
- registrare gli attributi specificati nelle regole di registrazione e certificazione;
- assegnare ad ogni utente registrato un identificativo univoco (= passphrase).

6.3. Richiedenti

Il richiedente è la persona che richiede un certificato mediante i canali preposti. Nell'ambito del sistema SICA la figura del richiedente coincide con il responsabile di una Pubblica Amministrazione locale o centrale per quanto riguarda le operazioni verso la Certification Authority, indicato spesso nei sistemi come "referente PA". Anche un operatore interno SICA autorizzato ad interagire con la Certification Authority può svolgere le funzioni di richiedente-referente nei casi previsti.

6.4. Titolari

Il titolare è la persona fisica o l'apparato al quale è intestato il certificato. E' il soggetto che usa il certificato per gli usi consentiti e previsti dalla CA del CG-SICA (autenticazione per siti protetti, cifratura di file o mail, ecc.).

6.5. Utenti

Gli utenti sono coloro che ricevono file e comunicazioni da titolari di certificati.

Gli utenti possono verificare la validità del certificato usato dal titolare accedendo alle CRL pubblicate dal CG-SICA, nonché al servizio OCSP.

7. CONDIZIONI GENERALI APPLICATE ALLA CERTIFICATION AUTHORITY "CNIPA CA4"

7.1. Obblighi del Certificatore

Nello svolgimento delle sue attività la CA del CG-SICA deve operare con modalità conformi a quanto specificato nel documento "CG-SICA_Servizio_di_Certificazione-CPS certificati.doc".

7.2. Informazioni per i richiedenti

Le informazioni che il richiedente deve fornire sono differenti in base alla tipologia di certificato richiesto. Nel documento "CG-SICA Servizio di Certificazione - Policy dei certificati emessi" sono specificate, all'interno di ogni profilo del certificato, i campi che devono essere ricevuti dal richiedente. Le informazioni di base necessarie sono le seguenti:

CN = Common Name del titolare da inserire nel certificato

O = Organization di cui fa parte il titolare/apparato (codice della PA)

OU= Organization Unit Unità organizzativa della PA (solitamente opzionale).

Oltre alle informazioni necessarie alla produzione del certificato, il richiedente deve inserire in fase di registrazione i propri dati identificativi (Nome, Cognome) e l'indirizzo e-mail di notifica certificato, che sarà l'indirizzo al quale verrà spedito e notificato il certificato prodotto. Nel caso di certificato di autenticazione "persona" l'indirizzo e-mail di notifica deve essere necessariamente quello del titolare: sarà a lui infatti che dovranno essere inviate le due e-mail contenenti il certificato e la passphrase per l'installazione. All'indirizzo e-mail del richiedente verrà solo inviata notifica di emissione.

Viene fornita ai richiedenti una interfaccia utente per la registrazione dei dati necessari alla produzione di un certificato digitale. [1]

[1] Per i certificati di autenticazione persona e per altre fattispecie descritte al par.9.2 la registrazione della richiesta tramite interfaccia utente non è necessaria da parte del richiedente.

Tale interfaccia è il Front-end web del Servizio di Certificazione ed è raggiungibile da remoto, su rete SPC (Infranet), da parte dei richiedenti autorizzati, in possesso delle credenziali di accesso.

Prima di richiedere un certificato il richiedente deve inserire i dati tramite tale Front End, e quindi confermarli, ricevendo in output una passphrase che sarà necessaria nella fase di richiesta. I dati inseriti vengono salvati in un DB di registrazione apposito.

Prima della conferma dei dati inseriti l'utente può modificare/cancellare i dati presenti nel database (le cosiddette funzioni CRUD).

Dopo aver inserito i dati di registrazione e confermato gli stessi, l'utente potrà richiedere (da un'applicazione esterna al CG-SICA) il certificato, inserendo verso i web services predisposti dal CG-SICA, la passphrase ricevuta dal F/E di registrazione nel momento della conferma.

L'utente che ha accesso al DB di registrazione è la figura di Referente PA (oltre naturalmente all'Amministratore CA (vedi)- figura interna del SICA -) che ha la facoltà di inserire i dati di registrazione per altri utenti e apparati della propria PA.

7.2.1. Emissione, sospensione e revoca del certificato

Il Certificatore CG-SICA, durante il ciclo di vita dei certificati emessi nel presente ambito, opera in conformità con quanto specificato "CG-SICA_Servizio_di_Certificazione-CPS certificati.doc"

7.2.2. Notifiche ai Titolari

Il certificatore darà notizia della revoca o della sospensione ai Titolari interessati tramite posta Elettronica.

Nel caso di certificato di autenticazione "persona" verrà notificata l'emissione del certificato al richiedente, mentre al titolare (qualora fosse persona diversa dal richiedente) verrà inviato il certificato e la passphrase (in 2 e-mail separate).

7.2.3. Cross Certification

La CA del CG-SICA può gestire la Cross Certification con altre CA ritenute sicure dal CNIPA.

7.3. Obblighi del Titolare

Il Titolare è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (Art.32, comma 1, CAD).

7.4. Registro dei certificati

La copia di riferimento (MASTER) è collocata all'interno di una rete protetta da adeguati dispositivi,che permettono di controllare e limitare i flussi di accesso al server di emissione dei certificati, che vi registra i certificati emessi e le CRL/CSL.

L'accesso è possibile sulla copia SHADOW secondo il protocollo LDAP v2, come definito nello RFC 1777, o lo LDAP v3 come definito nello RFC 2251.

8. PROCEDURE DELLA CA "CNIPA CA4"

8.1. Chiave privata

La CA fornisce al titolare (persona fisica o apparato) una Coppia di Chiavi oppure soddisfa le richieste di certificazione pervenute in formato PKCS#10, in tal caso occorre una prova di possesso della chiave privata da parte del richiedente, che in questo caso ha generato autonomamente le chiavi necessarie al certificato stesso, come specificato nel seguente paragrafo.

8.2. Procedure di generazione chiavi

La generazione delle chiavi può avvenire da parte del certificatore o da parte del richiedente.

La generazione da parte del richiedente può avvenire nei seguenti casi:

- i certificati per l'autenticazione Server;
- certificati per le Porte di Dominio e Registri Secondari;
- i certificati per l'identificazione del Client;
- certificati per OCSP Responder;
- certificati di firma XML

In questi casi può essere utilizzata la procedura di generazione chiavi prevista dal software/dispositivo per creare una richiesta di certificato in formato PKCS#10 da allegare nell'apposito campo della richiesta.

Per quanto riguarda i certificati per OCSP Responder non sono previsti automatismi per motivi di sicurezza, quindi un operatore centrale del CG-SICA WebRAO (Registration Authority Opertor) procederà alla generazione del certificato interagendo direttamente con la Certification Authority.

La generazione da parte del richiedente deve avvenire nei seguenti casi:

- Certificato di certificazione delle AC

E questo è l'unico caso in cui viene gestito un PKCS#10 dal CAO (Certification Authority Officer)

La generazione da parte del richiedente non può avvenire nei seguenti casi:

- i certificati per la cifratura dei messaggi;
- i certificati di autenticazione "persona".

L'operatore CA (vedi § "Acronimi e Definizioni") autorizzerà la generazione interagendo con la Certification Authority.

8.3.Emissione certificato

Il sistema della CA è stato realizzato tenendo in considerazione le indicazioni contenute nel DPCM 13/01/2004.

8.4. Accettazione del certificato

I richiedenti sono tenuti a verificare la correttezza delle informazioni contenute nel Certificato loro consegnato e segnalare immediatamente eventuali errori al Certificatore.

In tal caso, il richiedente deve sottoscrivere una richiesta di Revoca per il Certificato contenente dati errati.

8.5.Rinnovo di un certificato

I certificati emessi dalla CA del CG-SICA hanno validità fino 02/12/2010.

Il Titolare che intende rinnovare il proprio certificato deve darne comunicazione tempestiva alla CA del SG-SICA mediante una nuova registrazione verso il Front-end web di registrazione (lo stesso applicativo usato per la richiesta del certificato), in modo da garantire la continuità del servizio.

Le procedure per l'ottenimento di un nuovo certificato non differiscono da quelle relative alla prima emissione.

Verrà emesso un nuovo certificato, che verrà inviato all'utente con una procedura identica alla prima emissione.

8.6. Revoca e sospensione di un certificato

La revoca o la sospensione dei certificati viene asseverata dal loro inserimento nella lista CRL

Il profilo delle CRL/CSL è conforme con lo RFC 3280.

La CRL, firmata dal Certificatore, viene aggiornata con periodicità prestabilita, e ad ogni revoca e sospensione.

La periodicità prevista per la CA "CNIPA CA4" è di 24 ore.

8.6.1. Revoca di un certificato

Un certificato viene revocato nei seguenti casi, ad ognuno dei quali corrisponde un codice detto CRLReason indicato tra parentesi:

1. sostituzione del certificato senza compromissione della chiave privata (CRLReason: Superceded);
2. compromissione (ovvero la perdita delle caratteristiche di sicurezza e univocità) della chiave privata del Titolare (CRLReason: Key Compromise);
3. i dati del certificato sono modificati o obsoleti; in questo caso ricade anche l'eventualità che un Titolare non accetti i certificati emessi a suo nome in quanto i dati sono errati (CRLReason: Affiliation Changed);
4. cessazione repentina, in condizioni di conflittualità o non, del Titolare dalle mansioni per le quali gli erano stati rilasciati i certificati (CRLReason: Cessation of Operation);
5. cessazione preventivata dalle mansioni per le quali sono stati rilasciati i certificati al Titolare (CRLReason: Cessation of Operation);
6. mancato rispetto da parte del Titolare degli obblighi specificati nelle CP, in misura tale che il Terzo Interessato o la CA ritengano necessario una revoca immediata (CRLReason: Unspecified);
7. altri casi aventi carattere d'urgenza a giudizio del Terzo Interessato (CRLReason: Unspecified);
8. altri casi non urgenti (CRLReason: Unspecified).

I casi indicati sono riassunti nella seguente tabella:

CRLReason	Codice numerico
Unspecified	0

Key Compromise	1
Affiliation Changed	3
Superceded	4
Cessation of Operation	5
CertificateHold	6

8.6.2. Sospensione di un certificato

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se debba essere revocato o no (ad esempio nei casi in cui si tema la compromissione della chiave privata, o si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

Per una sospensione il codice di CRLReason è certificateHold (cfr. tabella CRLReason) e ha come conseguenza l'emissione della lista aggiornata di sospensione/revoca.

8.6.3. Durata del periodo di sospensione di un certificato

I certificati rimarranno nello stato sospeso per 10 giorni, oltre i quali, in mancanza di altre comunicazioni, verranno revocati.

Sarà cura del richiedente comunicare all'Ufficio RA del CG-SICA, con modalità analoghe a quelle utilizzate per la richiesta di sospensione, la eventuale richiesta di riattivazione o di revoca del certificato precedentemente sospeso.

8.7. Gestione delle CRL e OCSP

I certificati revocati o sospesi verranno inseriti nelle CRL, cioè le liste di revoca, Il profilo delle CRL/CSL è conforme con lo RFC 3280.

La CA CNIPA CA4 gestisce inoltre la verifica della validità dei certificati anche tramite OCSP.

I punti di distribuzione delle CRL/CSL e agli OCSP responder sono indicati all'interno dei certificati all'estensione CRLDistributionPoints.

9. MODALITÀ OPERATIVE

Le modalità operative per la richiesta/gestione dei certificati emessi dalla CA "CNIPA CA4" possono essere attivate in modalità manuale o automatica, in dipendenza del tipo di certificato richiesto, del tipo di registrazione effettuata e della scelta del richiedente.

9.1. Modalità applicativa (Web Services)

La modalità applicativa, fruibile nel caso in cui la generazione delle chiavi sia effettuate da parte del richiedente (ad eccezione del certificato di certificazione di un'altra AC, dei certificati per OCSP Responder e dei certificati di autenticazione persona), è quella che prevede l'utilizzo di servizi (WebServices) messi a disposizione delle PA che potranno usufruirne attraverso le loro applicazioni.

9.1.1. Richiesta di certificato

Le modalità per la richiesta di un certificato in modalità automatica sono le seguenti:

- Mediante il Front-end web il richiedente sottomette la registrazione dei dati necessari alla emissione del certificato.
- Il richiedente, mediante un applicativo predisposto dalla PA, invia ai webservices l'identificativo univoco (passphrase) ricevuto in fase di registrazione. Tale identificativo servirà a collegare la richiesta di certificato con i dati registrati.
- Vengono letti i dati inseriti dall'utente all'atto della registrazione, tra i quali è presente anche il PKCS#10 (contenente la request di certificato firmata con la chiave privata generata dall'utente).
- Il PKCS#10 viene passato alle UPI (interfaccia fornita dalla CA verso i web services), mediante le quali la CA produce il certificato.

9.1.2. Modalità di invio certificato

Il certificato viene inviato all'indirizzo e-mail indicato dal richiedente durante la registrazione.

9.1.3. Richiesta di revoca di un certificato

Il Titolare (o il richiedente se trattasi di certificati per apparati) può richiedere la revoca del certificato. Le possibili cause di revoca sono indicati nella tabella CRLReason.

Il titolare invia la richiesta di revoca mediante apposito web service fornendo il numero seriale del certificato e la passphrase usata in fase di richiesta.

La CA notificherà la revoca al richiedente per e-mail.

9.1.4. Richiesta di sospensione di un certificato

Il Titolare (o il richiedente se trattasi di certificati per apparati) può richiedere la sospensione del certificato. Le possibili cause della sospensione sono indicati nella tabella CRLReason.

Il titolare invia la richiesta di sospensione mediante apposito web service usando il numero seriale del certificato.

La CA notificherà la sospensione al richiedente per e-mail.

9.1.5. Rinnovo di un certificato

Utente inserisce una nuova registrazione nel FE del servizio di Certificazione, quindi invia la richiesta di certificato tramite web services.

9.2. Modalità manuale

La modalità manuale di produzione di un certificato può essere attivata:

- Nel caso in cui nel DB di registrazione siano presenti solo i dati di registrazione e non il PKCS#10.
- Nel caso di alcuni tipi di certificati (persona, crittografia, OCSP , subCA).
- Nel caso in cui l'utente non possa usare applicativo di registrazione o applicativo per la richiesta.

9.2.1. Richiesta di certificato

La richiesta di certificato viene inviata tramite Fax o e-mail al Centro di Gestione SICA.

L'indirizzo e-mail è il seguente: helpdesk@spcoop.gov.it

Numero di fax: 06/41.90.981

L'operatore di CA registra i dati nel DB , produce il certificato in modalità manuale e lo invia per e-mail.

9.2.2.Modalità di invio certificato

L'operatore invia 2 e-mail separate: nella prima e-mail sarà presente il un file PKCS#12 (involucro protetto da passphrase, contenente il certificato e la coppia di chiavi) e in una e-mail successiva sarà presente la relativa passphrase di istallazione certificato.

Nel caso di certificato di autenticazione "persona" verrà inviata inoltre una terza e-mail al richiedente con la semplice notifica di emissione

9.2.3.Procedura per la richiesta di revoca di un certificato

Il Titolare (o il richiedente se trattasi di certificati per apparati) può richiedere la revoca del certificato. Le possibili cause di revoca sono indicate nella tabella CRLReason.

Le modalità per la richiesta di revoca di un certificato sono le seguenti:

- Il titolare invia la richiesta di revoca mediante fax o e-mail al Centro di gestione SICA (indirizzo e-mail: helpdesk@spcoop.gov.it, numero di fax: 06/41.90.981)
- L'operatore revoca il certificato.
- L'operatore notificherà la revoca al richiedente per e-mail.

9.2.4.Procedura per la richiesta di sospensione di un certificato

Il Titolare (o il richiedente se trattasi di certificati per apparati) può richiedere la sospensione del certificato. Le possibili cause di sospensione sono indicate nella tabella CRLReason.

Le modalità di sospensione sono le seguenti:

- Il titolare invia la richiesta di sospensione mediante fax o e-mail al Centro di gestione SICA (indirizzo e-mail: helpdesk@spcoop.gov.it, numero di fax: 06/41.90.981)
- L'operatore cambia lo stato del certificato in revocato con reason "CertificateHold".
- L'operatore notificherà la sospensione al richiedente per e-mail.

9.2.5. *Procedura per il rinnovo di un certificato*

Le modalità di rinnovo di un certificato non differiscono da quelle relative alla prima emissione.

---

10. FORMATO DEI CERTIFICATI E DELLE CRL

I Certificati e le CRL sono conformi a ISO 9594-8 (1997), alias ITU-T X.509v3.

Il loro formato soddisfa RFC 2459 e la Deliberzione CNIPA 4/2005.

10.1. Formato dei certificati

10.1.1. *Versione*

La versione del certificato è "ITU-T X.509 v3".

10.2. Struttura

I certificati emessi dalla CA del CG-SICA sono conformi allo standard X509v3. La struttura di tali certificati è descritta nel documento "CG_SICA_Servizio_di_Certificazione-policy_certificati_emessi "

10.3. Formato della CRL

Il formato della CRL è conforme alla RFC 2459, come da Delibera CNIPA 4/2005.

10.3.1. *Versione*

Il campo version è valorizzato come "v2".

10.4. Estensione della CRL e delle Entry

Come da Delibera CNIPA 4/2005, le estensioni richieste sono le seguenti:

- CRL/CSL: estensione cRLNumber, che indica il numero incrementale di CRL/CSL;
- entry delle CRL/CSL: estensione reasonCode, che indica la causale di revoca.

11. PROCEDURE DELLA CA "CNIPA CA3"

Il Servizio di Certificazione PEC si occupa di fornire certificati per i server dedicati ai server di Posta Elettronica Certificata. Questo servizio è inserito all'interno del Servizio di Certificazione ma è standalone rispetto agli altri servizi all'interno dell'SPCoop.

Viene usata una infrastruttura tecnologica di Certification Autohority analoga alla CNIPA CA4 ma dedicata alla funzione in oggetto. Il certificato di root ed i certificati emessi da questa Certification Authority sono automaticamente riconosciuti dai principali browser di mercato (IE, Mozilla, etc.)

11.1. Tipologie di certificati

Le tipologie di certificati emessi dalla CA CNIPA CA3 sono le seguenti:

- Certificati per la firma delle ricevute PEC.
- Certificati per l'autenticazione all'indice dei Gestori PEC.
- Certificati per Web Server PEC.

11.2. Condizioni generali

Per quanto riguarda le condizioni generali, gli obblighi, le informazioni ai richiedenti, le modalità di generazione chiavi e dei certificati si faccia riferimento al manuale operativo emesso dal CNIPA e reperibile al seguente indirizzo:

http://www.cnipa.gov.it/firmadigitale/manualeoperativoserver

Nel manuale sopra referenziato sono reperibili anche le informazioni relative alle modalità di gestione (revoca, ecc.) dei certificati emessi dalla CA "CNIPA CA3".

11.3. Modalità operative

La richiesta di emissione di un certificato verso la CA "CNIPA CA3" proviene al Centro di Gestione da parte del Responsabile della Registrazione CNIPA, mediante un tracciato record sotto forma di file di formato concordato firmato digitalmente. Tale file contiene in particolare le seguenti informazioni:

- dati dei Responsabili legali delle società gestori PEC;
- dati dei Responsabili del servizio PEC;
- dati dei Responsabili del server da certificare;
- dati da inserire nel certificato da produrre;
- richiesta PKCS#10 contenente la chiavi da certificare;

L'operatore WebRAO della CA provvederà a produrre il certificato, ad effettuare i controlli di coerenza con i dati forniti e a spedirlo, mediante form prestabilito, agli indirizzi e-mail specificati nel tracciato record della richiesta e per conoscenza al responsabile della registrazione CNIPA all'indirizzo e.mail: registrazione@cnipa.it