Bollettino Ufficiale della Regione Campania n. 38 del 09 agosto 2004

Allegato A2

Regione Campania

Manuale operativo della Regione Campania per la gestione di una PKI ad uso interno

MANUALE DI GESTIONE DEI DOCUMENTI ELETTRONICI CON VALIDITA' GIURIDICA INTERNA ED ESTERNA

SOMMARIO

DEFINIZIONI

DEFINIZIONE	DESCRIZIONE
AIPA	Autorità per l'Informatica nella Pubblica Amministrazione. Trasformata in "Centro Nazionale per l'informatica nella pubblica amministrazione" in attuazione di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato sul supplemento ordinario n. 123 alla Gazzetta Ufficiale n. 174 del 29 luglio 2003.
Certificato	Documento informatico in formato ITU X.509 v.3 o successive contenente informazioni relative al Titolare e la sua chiave pubblica di firma, firmato dal Certificatore con la propria chiave privata di certificazione.
Certificato qualificato	Ai sensi dell'articolo 2, comma 1, lettera e), del decreto legislativo 23 gennaio 2002, n. 10, è il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva ed avente le caratteristiche fissate dall'art. 11 del D.P.C.M. 13 gennaio 2004 in G.U. del 27/04/2004..
Certificatore	Ente che svolge le attività di generazione, emissione, conservazione, revoca e sospensione dei certificati.
Certificatore accreditato	Certificatore iscritto nell'albo tenuto dal CNIPA, ai sensi degli artt. 3 e 4 della direttiva n. 1999/93/CE
Certificazione	Il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto Titolare cui essa appartiene.
Chiave privata	Elemento della coppia di chiavi asimmetriche, destinato ad essere utilizzato soltanto dal Titolare. Essa è utilizzata per firmare digitalmente.
Chiave pubblica	Elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico. Essa è utilizzata per la verifica della firma.
CNIPA	Centro Nazionale per l'informatica nella pubblica amministrazione (vedi AIPA).
Coppia di chiavi	Coppia di chiavi asimmetriche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di firma digitale di documenti informatici.
CRL (Certificate Revocation List)	Vedi Liste di revoca dei certificati.
Destinatario	Destinatario di un documento informatico firmato digitalmente.

DEFINIZIONE	DESCRIZIONE
Dispositivo di firma	Un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali.
Dispositivo per la creazione di una firma	L'apparato strumentale, usato per la creazione di una firma elettronica.
Distinguished Name (Dname)	Identificativo univoco del Titolare presso il Certificatore.
Firma elettronica avanzata	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
Lista di revoca dei certificati (CRL)	Lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contrassegnata da una marca temporale, contenente i certificati emessi dallo stesso e successivamente revocati.
Manuale operativo	Documento pubblico depositato agli atti della Regione Campania che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.
PIN (Personal Identification Number)	Numero di identificazione personale.
PKCS (Public Key Cryptographic Standard)	Standard tecnici per applicazioni crittografiche, realizzati dalla RSA Data Security Inc.
PKI (Public Key Infrastructure)	Infrastruttura a Chiave pubblica.
RA - I	Autorità di Registrazione per l'identificazione dei Soggetti Titolari. Nello specifico la RA-I è il Soggetto che ha emesso l'atto di organizzazione interna che identifica i Titolari (Coordinatore D'Area o Dirigente di Settore delegato).
RA - R	Autorità di Registrazione per le attività di registrazione. Nello specifico la RA-R è l'AGC Ricerca Scientifica ed Informatica.
Registrazione	Attività d'acquisizione, verifica e archiviazione dei dati dei richiedenti.
Registro dei certificati	Registro contenente i certificati emessi dal Certificatore, la lista dei certificati revocati e la lista dei certificati sospesi, accessibile anche telematicamente.
Revoca del certificato	Operazione con cui il Certificatore annulla la validità del certificato da un dato momento in poi.
Titolare	Soggetto a favore del quale è stato emesso un Certificato

DEFINIZIONE	DESCRIZIONE
Token di firma	Supporto per la conservazione della chiave privata e per la generazione della firma. Può essere di due tipologie: token sw e token hw.
Validazione temporale	Risultato della procedura informatica con cui si attribuiscono, ad una evidenza informatica, una data ed un orario opponibili ai terzi.

1 INTRODUZIONE

Scopo del documento

Questo documento definisce le procedure seguite dalla Regione Campania nello svolgimento dell'attività di certificatore ad uso interno. Esso si riferisce ai servizi di:

- Certificazione delle chiavi pubbliche dei dipendenti della Regione Campania e di tutti coloro che sono espressamente autorizzati dalla Regione Campania.

Il presente documento definisce inoltre gli obblighi e le responsabilità del Certificatore, del Titolare e di quanti accedono per la verifica della firma.

Riferimenti normativi

Il Manuale Operativo è conforme a quanto previsto dalla normativa italiana e dalle Direttive dell'UE e in particolare:

- Direttiva 13 dicembre 1999 n. 1999/93/CE
- Decreto Legislativo 23 gennaio 2002 n. 10
- Art. 15, comma 2, Legge 15 marzo 1997 n. 59
- D.P.R. 28 dicembre 2000 n. 445
- D.P.C.M. 13 gennaio 2004, pubblicato in G.U. del 27/04/2004
- Circolare AIPA 19 giugno 2000 n. AIPA/CR/24
- Circolare AIPA 16 febbraio 2001 n. AIPA/CR/27
- Testo Unico Sulla Privacy (D.lgs. del 30.06.2003 n. 196)
- D.P.R 7 aprile 2003 n. 137

Si precisa che i riferimenti normativi indicati in precedenza e nel prosieguo del presente manuale dovranno intendersi anche relativi alle norme in corso di emanazione in materia, modificative o sostitutive delle precedenti.

DATI IDENTIFICATIVI DEL CERTIFICATORE

I dati identificativi relativi al Certificatore della Regione Campania sono i seguenti:

Denominazione e Ragione sociale:	**Sede legale**:
Rappresentante legale:	
Telefono:	**Fax**:
Sede operativa:	**Indirizzo E-mail:**
Indirizzo Internet:	**Call Center**:

MANUALE OPERATIVO

Dati identificativi del Manuale operativo

Il presente Manuale operativo, è identificato col nome "**Manuale operativo della Regione Campania per la gestione di una PKI ad uso interno**" ed è consultabile per via telematica all'indirizzo Internet:
http://www.regione.campania.it
Il presente documento è identificato con il numero di versione 1.0

Responsabile del Manuale operativo

Il Responsabile del Manuale operativo è il Coordinatore dell'Area Generale di Coordinamento Ricerca Scientifica ed Informatica.

Tipologia delle utenze

Il Certificatore ad uso interno della Regione Campania (nel prosieguo indicato come "Certificatore") certifica esclusivamente le chiavi pubbliche utilizzate dai dipendenti nell'esercizio delle loro funzioni e dai soggetti autorizzati espressamente dall'Ente.

Il Certificatore della Regione Campania rilascia esclusivamente a tal fine firme elettroniche avanzate.

L'eventuale utilizzo per scopi diversi è ammesso solo se autorizzato espressamente dalla REGIONE CAMPANIA.

OBBLIGHI DEL CERTIFICATORE, DEL TITOLARE E DI QUANTI ACCEDONO PER LA VERIFICA DELLE FIRME

Obblighi del Certificatore

Nello svolgimento della sua attività, il Certificatore:

1) adotta tutte le misure organizzative e tecniche idonee a garantire la sicurezza dei processi e ad evitare danno ad altri;
2) emette e gestisce i certificati in modo conforme alla normativa italiana ed europea, con le procedure descritte nel presente Manuale Operativo;
3) identifica con certezza i soggetti titolari richiedenti ed il fatto che siano regolarmente in esercizio presso la Regione Campania;
4) informa espressamente, in modo compiuto e chiaro, il Titolare riguardo agli obblighi in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma, nonché sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
5) rilascia e rende pubblico, nel dominio di esercizio, il certificato;
6) si attiene alle regole tecniche emanate con D.P.C.M. 13 gennaio 2004, in quanto applicabili alla tipologia di firma rilasciata;
7) si accerta dell'autenticità della richiesta di certificazione;
8) verifica il corretto funzionamento della coppia di chiavi, con la sottoscrizione di uno o più documenti di prova;
9) si attiene alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi del Testo Unico Sulla Privacy (D.lgs. del 30.06.2003 n. 196);
10) genera le coppie di chiavi dei Titolari, all'interno del dispositivo di firma nell'ipotesi di cui al par. Procedure per la generazione e la certificazione delle chiavi pubbliche di firma;
11) genera la coppia di chiavi mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata;
12) procede tempestivamente alla revoca del certificato in tutti i casi previsti dal presente Manuale Operativo;
13) comunica le richieste di revoca ai Soggetti previsti dal presente Manuale Operativo;
14) dà tempestiva pubblicazione, nel dominio di esercizio, della revoca della coppia di chiavi asimmetriche.

Obblighi del Titolare

Il Titolare è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

Il Titolare della chiave deve, inoltre:

1) fornire tutte le informazioni richieste dal Certificatore, garantendone, sotto la propria responsabilità, l'attendibilità;
2) conservare la chiave privata e l'eventuale dispositivo che la contiene al fine di garantirne l'integrità e conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dall'eventuale dispositivo contenente la chiave;
3) richiedere tempestivamente la revoca dei certificati relativi alle chiavi di cui abbia perduto il possesso o malfunzionanti;
4) dare corso senza indugio alla richiesta di revoca, specificando la motivazione e la sua decorrenza;

E' vietata la duplicazione della chiave privata e dei dispositivi che la contengono.

Obblighi dei Responsabili RA-I

I Responsabili sono tenuti a :
1) individuare, mediante un atto di organizzazione interna, i soggetti Titolari;
2) predisporre la lista di certificati da rilasciare;
3) consegnare, previa verifica dell'identità, la busta ed il dispositivo di firma ai Titolari, nelle ipotesi di procedura centralizzata di cui al par. 6.7.1. Dell'avvenuta consegna dovrà essere conservata opportuna ricevuta;
4) consegnare, previa verifica dell'identità, la busta contenente il PIN ai Titolari, nelle ipotesi di procedura centralizzata per il rilascio del token sw per procedure di firma su server remoto di cui al par. 6.7.2. Dell'avvenuta consegna dovrà essere conservata opportuna ricevuta;
5) richiedere tempestivamente la revoca dei certificati per le ipotesi previste dal par. 9.2.1;
6) dare corso senza indugio alla richiesta di revoca;

Obblighi dei Responsabili RA-R

I Responsabili di registrazione RA-R sono tenuti a :
1) effettuare la registrazione del soggetto titolare;
2) inviare la richiesta di certificazione al Certificatore;
3) identificare mediante la verifica dei documenti di riconoscimento, annotandone gli estremi, i soggetti esterni alla Regione Campania espressamente autorizzati all'uso della firma elettronica;
4) consegnare la busta ed il dispositivo di firma ai Responsabili RA-I, nelle ipotesi di procedura centralizzata di cui al par. 6.7.1;
5) consegnare la busta contenente il PIN ai Responsabili RA-I, nelle ipotesi di procedura centralizzata per il rilascio del token sw per procedure di firma su server remoto di cui al par. 6.7.2.

Obblighi dei destinatari

Per l'accettazione dei documenti informatici firmati, i destinatari degli stessi devono verificare:
1) la validità del certificato;
2) l'assenza del certificato dalle Liste di Revoca (CRL) dei certificati;
3) l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare.

RESPONSABILITÀ

Responsabilità del certificatore ad uso interno

Il Certificatore ad uso interno della Regione Campania è responsabile nei confronti di qualunque soggetto faccia ragionevole affidamento sui certificati emessi dallo stesso, nei limiti di cui all'art. 28 bis del D.P.R. 445/2000, come introdotto dal D.Lgs. 23 gennaio 2002 n. 10. L'esistenza e la validità del certificato non dispensano però l'utente dall'eseguire ogni altra verifica che appaia opportuna secondo criteri di oculata prudenza, anche in relazione al rilievo, economico o d'altra natura, degli interessi coinvolti. La responsabilità del CERTIFICATORE è comunque rigorosamente circoscritta a:

- l'esattezza delle informazioni contenute nel certificato alla data di rilascio e la loro completezza rispetto ai requisiti fissati per i certificati;
- l'esecuzione della procedura di revoca nei termini e con le modalità previste dal presente manuale operativo.

E' esclusa qualunque responsabilità del Certificatore, anche di natura sussidiaria, in relazione a fatti diversi da quelli sopra enunciati, ed in particolare per fatti riconducibili alla sfera operativa del soggetto titolare, ivi compresi, a titolo esemplificativo, il mancato rispetto delle procedure, vizi formali o sostanziali relativi al documento firmato ed al suo contenuto, lo smarrimento o la sottrazione o l'incauto affidamento ad altro soggetto del dispositivo di firma, l'erronea identificazione del documento sottoposto alla procedura di firma.
E' altresì esclusa qualsivoglia responsabilità del Certificatore laddove i terzi non si attengano alle prescrizioni stabilite dal presente documento ed in particolare non rispettino le procedure stabilite per la verifica delle firme e delle marche temporali o facciano affidamento su di esse al di fuori dei casi e dei limiti previsti dal relativo certificato.
Ogni responsabilità è comunque esclusa laddove il Certificatore provi d'aver agito senza colpa, ed in ogni caso in cui la responsabilità è esclusa dall'art. 28 bis del D.P.R. 445/2000, come introdotto dall'art. 7 del D.Lgs. 10/2002

INDIVIDUAZIONE E REGISTRAZIONE

Individuazione

L'individuazione dei soggetti titolari richiedenti, dipendente della Regione Campania, viene effettuata da un responsabile RA-I ovvero il Responsabile dei titolari (Coordinatore d'Area o Dirigente di Settore delegato) che prepara una lista contenente tutti i certificati da rilasciare. La lista contiene informazioni relative al nome, cognome e funzione dei titolari da identificare nonché quant'altro richiesto dal paragrafo 6.4; per avere valore deve essere accompagnata dall'atto di organizzazione interna che individua i titolari.
La lista viene inoltrata al Certificatore indipendentemente dalla procedura utilizzata per l'emissione delle chiavi.

Registrazione

La registrazione del soggetto titolare richiedente, dipendente della Regione Campania, viene effettuata da un responsabile (RA-R) che prepara le richieste di certificazione da inviare al certificatore.
Il RA-R deve avere tutti i dati anagrafici dei soggetti titolari per eseguire una richiesta centralizzata; i dati gli verranno forniti dal Responsabile dei titolari.
Eventuali verifiche devono essere richieste all'AGC 07 quale Area responsabile del Personale Regionale.

Identificazione e registrazione di soggetti esterni

La identificazione e registrazione di soggetti esterni alla Regione Campania, quando espressamente autorizzata dall'AGC Ricerca Scientifica ed Informatica, avviene attraverso l'esibizione di un documento di riconoscimento idoneo per legge.

Contenuto della richiesta del certificato

La richiesta di certificazione include i seguenti dati:

- nome e cognome del soggetto;
- luogo e data di nascita;
- Area Generale di Coordinamento, Settore e Servizio di appartenenza;
- Matricola, per i titolari dipendenti della Regione Campania;
- Estremi del documento di riconoscimento, per i titolari esterni alla Regione Campania;
- Riferimento all'atto di organizzazione interna emesso dal Coordinatore d'Area o dal Dirigente di Settore;
- telefono e fax, se disponibili;
- indirizzo di posta elettronica (se il titolare non possiede un indirizzo di e-mail, in questo campo occorre inserire l' indirizzo di posta elettronica del responsabile del titolare);

Obblighi di Identificazione

Il Certificatore, per il tramite del responsabile della RA, effettua l'identificazione e la registrazione, secondo le modalità previste nel presente Manuale Operativo.

Comunicazioni tra il Certificatore e i Titolari

Se il titolare dispone di una casella di posta elettronica, essa potrà essere utilizzata dal Certificatore per inviare comunicazioni.
Se il titolare non dispone di una casella di posta elettronica, il Certificatore utilizzerà la casella del responsabile del titolare (RA-I) per inviare comunicazioni.
L'eventuale variazione dell'indirizzo di posta elettronica dovrà essere comunicata al CERTIFICATORE con messaggio sottoscritto dal Titolare o dal Responsabile RA.

Procedure per la generazione e la certificazione delle chiavi pubbliche di firma

Di seguito sono riportate le procedure per la generazione e il rilascio delle chiavi pubbliche di firma. Le procedure sono definite con riferimento a tre diverse modalità di gestione:

a) Procedura centralizzata per il rilascio del token Sw, par. 6.7.1: il dispositivo di firma è un token crittografico realizzato in sw che implementa le funzioni di firma; deve essere attivato dal soggetto titolare mediante un PIN. Tale token può essere consegnato al soggetto titolare (Procedura di Firma

Centralizzata) su supporto magnetico, ottico (Floppy o CD) o su supporto a stato solido (Penna USB o Hard Disk del PC del soggetto titolare).

b) Procedura centralizzata per il rilascio del token sw per procedura di firma su server remoto, par. 6.7.2. Tale token deve essere conservato sul server del certificatore (Procedura di Firma Remota).
c) Procedura centralizzata per il rilascio del Token Hw, par. 6.7.3: il dispositivo di firma è un token crittografico realizzato in hw; deve essere attivato dal soggetto titolare mediante un PIN (Procedura di Firma Centralizzata).

Procedura centralizzata per il rilascio del token sw, di tipo a)

Responsabile - RA	**Soggetto titolare**	**CA - Certificatore della Regione Campania**
Il Responsabile RA-I predispone la lista contenente tutti i certificati da rilasciare e la invia al Responsabile RA-R		
Il responsabile, nella funzione di RA-R, invia al CERTIFICATORE richiesta di rilascio di uno o più certificati (e in genere, token di firma). La richiesta contiene la lista di tutti i soggetti da certificare ed i dati anagrafici degli stessi utili alla emissione dei certificati.		
		Per ogni certificato (o token sw di firma) richiesto: • associa ad ogni soggetto un codice identificativo ed un codice riservato (PIN) da inserire in una busta oscurata, secondo una procedura in grado di garantire la riservatezza; • avvia la procedura di generazione della coppia di chiavi; • pubblica il certificato digitale nell'archivio pubblico dei certificati, associandovi una marca temporale; • prepara un plico contenente il certificato pubblico ed il dispositivo contenente il token (floppy, CD-ROM, penna- USB, etc..); • Invia il plico al responsabile dei titolari; • Invia in busta chiusa il PIN al responsabile RA-R.
Il Responsabile RA-R invia in busta chiusa il PIN al Responsabile RA-I		

Il responsabile RA-I consegna la busta ed il dispositivo di firma a tutti i soggetti (oppure il responsabile consegna al soggetto solo la busta contenente il PIN e provvede ad installare il certificato e la chiave privata del soggetto sul PC dello stesso).		

Procedura centralizzata per il rilascio del token sw per procedura di firma su server remoto, di tipo b)

Responsabile - RA	**Soggetto titolare**	**CA - Certificatore della Regione Campania**
Il Responsabile RA-I predispone la lista contenente tutti i certificati da rilasciare e la invia al Responsabile RA-R		
Il responsabile, nella funzione di RA-R, invia al CERTIFICATORE richiesta di rilascio di uno o più certificati (e in genere, token di firma). La richiesta contiene la lista di tutti i soggetti da certificare ed i dati anagrafici degli stessi utili alla emissione dei certificati.		

Procedura centralizzata per il rilascio del token hw, di tipo c)

Responsabile - RAR	**Soggetto titolare**	**CA - Certificatore della Regione Campania**
Il Responsabile RA-I predispone la lista contenente tutti i certificati da rilasciare e la invia al Responsabile RA-R		
Il responsabile RA-R, invia al CERTIFICATORE richiesta di rilascio di uno o più certificati (e in genere, token di firma). La richiesta contiene la lista di tutti i soggetti da certificare ed i dati anagrafici degli stessi utili alla emissione dei certificati.		

		Per ogni nominativo presente nella lista, deve: - pre-personalizzare i dispositivi di firma con i dati dei soggetti da certificare; - generare le coppie di chiavi; - emettere i certificati; - effettuare la registrazione nel dispositivo di firma del certificato emesso; - attivare i sistemi di distribuzione per la consegna del dispositivo di firma e dei codici PIN e PUK relativi, utilizzando due corrieri differenti
Convoca il soggetto che ha richiesto il certificato		
Prova il funzionamento del dispositivo di firma in presenza del soggetto, provando le chiavi di sottoscrizione	Attiva la procedura di identificazione	
Se la prova del dispositivo fallisce, lo ritira ed avvia le procedure di revoca Se la prova ha esito positivo invia al Certificatore la richiesta di emissione del certificato (per la pubblicazione)		
		dopo aver ricevuto la richiesta firmata: • Pubblica i certificati ed emette una marca temporale relativa alla loro pubblicazione • Aggiorna il giornale di controllo • Invia al RAR i certificati e la marca temporale relativa alla pubblicazione;

Archivia la marca temporale e ne consegna una copia al soggetto Consegna al soggetto: - il dispositivo personalizzato - una busta contenente il PIN ed il relativo PUK per attivare la funzione di firma - una ricevuta cartacea da firmare - un kit hw\sw (applicativo Client) con le istruzioni per l'installazione ed il Manuale Operativo.		
	Firma una ricevuta di avvenuta emissione Firma una ricevuta di emissione e sottoscrive un documento attestante l'uso esclusivo della firma nell'espletamento delle sole funzioni di Funzionario della Regione Campania.	

Le procedure di firma possibili sono:
Procedura di Firma Centralizzata: il soggetto titolare deve conservare personalmente il token di firma o,in alternativa, tenerlo sul proprio PC; le funzioni di firma vengono attivate dal soggetto titolare mediante un PIN.
Procedura di Firma Remota: il soggetto titolare non deve conservare personalmente il token di firma; al momento dell'attivazione della procedura di firma, un applicazione sul PC client su cui il soggetto è connesso:
- genera l'impronta del documento,
- invia l'impronta al server dei token sw,
- attiva la procedura di firma con il suo PIN,
- attende l'impronta firmata,
- scarica il suo certificato a chiave pubblica dal registro dei certificati della Regione Campania,
- crea il plico firmato (documento, firma e certificato).

Emissione di certificati successiva ad una revoca
Un certificato revocato non è mai riattivabile. La richiesta di un nuovo certificato comporta la ripetizione dell'intera procedura di rilascio.

GENERAZIONE DELLE CHIAVI

Sistemi di generazione
La generazione della coppia di chiavi è effettuata mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata. Il sistema di generazione delle chiavi assicura:
- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equiprobabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione.

La generazione delle chiavi può avvenire sul PC locale del soggetto (nel caso di procedura remota) o sul Pc della CA (procedura centralizzata), all'interno del token di firma.

Lunghezza delle chiavi
La lunghezza delle chiavi di certificazione è di 2048 bit.
La lunghezza delle chiavi di sottoscrizione è di 1024 bit.

Algoritmi
Per la generazione e verifica delle firme digitali è usato il seguente algoritmo:

- RSA (Rivest-Shamir-Adleman algorithm).
  La funzione di hash utilizzata per la generazione dell'impronta è:
- SHA-1 (Dedicated Hash Function 3)

Chiavi di certificazione
Il Certificatore si avvale delle seguenti chiavi di certificazione:

- chiavi di certificazione per firmare i certificati relativi alle chiavi di sottoscrizione e liste di revoca (CRL);

Generazione delle chiavi di certificazione
La generazione delle chiavi di certificazione è effettuata esclusivamente dal Responsabile del servizio che le utilizzerà. Essa avviene all'interno del dispositivo di firma personalizzato dalla postazione predisposta a tale funzione dal Certificatore.

Chiavi di sottoscrizione
Le chiavi di sottoscrizione, ovvero di firma, consentono al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Alla firma elettronica avanzata è allegato il certificato corrispondente alla chiave pubblica da utilizzare per la verifica.

Token per la firma
Il token per la firma può essere di due tipologie:
token sw;
token hw;
Il **token sw**, utilizzato per la conservazione della chiave privata e per la generazione della firma, può essere conservato su vari supporti :

- un floppy;
- un CD ROM;
- una penna-USB;
- sul PC del soggetto titolare.

Le chiavi private devono essere conservate e custodite all'interno del token di firma e criptate con l'apposita chiave simmetrica legata al PIN di utente, sia se consegnate al soggetto titolare, sia se installate sul PC del soggetto titolare.
Il **token hw** prevede come semplice supporto una criptocard a norma.
Ciascuna coppia di chiavi è attribuita ad un solo Titolare. La duplicazione della chiave privata o dei dispositivi che la contengono è vietata.

Requisiti del token di firma
L'accesso alla chiave privata da parte del soggetto è protetto con un PIN che deve essere digitato dal titolare ogni volta che egli intende usare la chiave.

Consegna del token di firma

Il token di firma è spedito in busta sigillata al responsabile del soggetto richiedente; con separato plico sigillato sono trasmessi il PIN iniziale ed il relativo PUK ed ogni altro codice necessario per la generazione della coppia di chiavi.

Ricevuto il plico, il responsabile convoca il soggetto e gli consegna personalmente :

- una busta contenente il PIN ed il relativo PUK per attivare la funzione di firma oppure ogni altro codice necessario alla generazione delle chiavi;
- un *kit hardware/software* per l'apposizione e la verifica delle firme, comprendente il token di firma e le istruzioni per l'installazione e l'uso;
- una copia del manuale operativo.

EMISSIONE DEI CERTIFICATI

Informazioni contenute nel certificato

Il certificato contiene:

- numero di serie del certificato;
- denominazione del Certificatore e stato di stabilimento;
- codice identificativo del Titolare presso il Certificatore (nel campo Subject come specificato nella Circolare AIPA\24);
- nome, cognome, codice fiscale data di nascita del Titolare;
- l'indicazione delle funzioni del titolare (ruolo del soggetto);
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- indicazione dell'uso esclusivo della chiave privata per l'esercizio della funzione di ufficio;
- riferimento al presente manuale operativo;
- tipologia delle chiavi.

Profilo del certificato

Il certificato è un documento informatico, firmato digitalmente dal Certificatore, che deve essere generato e pubblicato, a cura dello stesso. I certificati sono conformi alla norma ISO/IEC 9594-8:2001 con le estensioni definite nella Variante 1, ovvero alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

Le informazioni contenute nel certificato seguono le linee guida previste dalla circolare AIPA/24 e successive modificazioni e integrazioni.

In aggiunta a quanto previsto dalla circolare AIPA/24, all'interno del campo "Subject" è presente un sottocampo O (Organization) riportante l'AGC di appartenenza.

Emissione e pubblicazione del certificato

Il certificato è generato con un sistema utilizzato esclusivamente per tale funzione, situato in locali protetti come descritto nel Piano per la sicurezza.

L'accesso al sistema di generazione dei certificati avviene attraverso un'operazione di riconoscimento mediante l'uso del dispositivo di firma.

Il Certificatore, verificato il completamento delle operazioni di consegna ed il ricevimento della richiesta di emissione procede alla pubblicazione del certificato contenente la chiave pubblica, con l'apposizione di una marca temporale.

I certificati relativi alle chiavi pubbliche dei titolari sono conservati, a cura del Certificatore, nel Registro dei certificati.

Tale registro è consultabile anche telematicamente dagli aventi diritto.

REVOCA DEI CERTIFICATI

Premessa

Il Certificatore utilizza per la revoca la Lista dei certificati revocati (CRL).

La lista è consultabile telematicamente nel dominio del certificatore, secondo le modalità descritte nel Manuale operativo.

Revoca dei certificati

La revoca di un certificato determina la cessazione anticipata della sua validità.
La revoca è registrata nel Giornale di controllo ed è efficace a partire dal momento della pubblicazione della lista che le contiene. Il momento di pubblicazione della lista è provato mediante l'apposizione di una marca temporale.
Il Certificatore procede immediatamente alla pubblicazione dell'aggiornamento della lista, alla ricezione della richiesta di revoca.
Il certificato è revocato su:

- richiesta del soggetto titolare;
- richiesta del Responsabile RA-I;
- iniziativa del Certificatore;

Revoca di certificati

Su richiesta del soggetto titolare:

Il soggetto titolare deve richiedere tempestivamente al certificatore o al RA-I la revoca del proprio certificato nei seguenti casi:

- perdita del possesso del dispositivo di firma (smarrimento, distruzione, sottrazione, furto);
- sospetti abusi o falsificazioni;
- compromissione della segretezza della chiave privata.

Il soggetto titolare può richiedere in ogni tempo la revoca del proprio certificato per iscritto, specificandone i motivi e la decorrenza.

Su richiesta del Responsabile RA-I

Il Responsabile RA provvede tempestivamente alla revoca dei certificati per:

- decadenza dal ruolo di dipendente regionale;
- cessazione dall'esercizio delle sue funzioni per dispensa, rimozione, destituzione;
- altre ipotesi di cessazione definitiva dalle funzioni;
- esecuzione di provvedimenti dell'autorità giudiziaria comportanti la cessazione dalle funzioni.

Su iniziativa del certificatore

Il Certificatore deve procedere tempestivamente alla revoca oltre che nei casi di richiesta da parte dei soggetti a ciò abilitati, nei casi di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi e falsificazioni e negli altri casi previsti dal presente manuale.
Salvo i casi di urgenza, la revoca del certificato è preventivamente comunicata dal Certificatore al soggetto titolare, con specificazione dei motivi, nonché della data e dell'ora a partire dalla quale il certificato non sarà più valido.

Modalità di revoca

Le richieste di revoca devono essere inoltrate con le modalità previste nei paragrafi successivi.
Salvo i casi di maggiore urgenza da evidenziarsi all'atto della richiesta, ovvero di emergenza, le richieste di revoca vanno presentate con almeno due giorni feriali di anticipo rispetto alla data di entrata in vigore.

Procedure di revoca dei certificati su richiesta del Titolare

Il soggetto Titolare può inoltrare la richiesta di revoca dei certificati attraverso una richiesta scritta con firma autografa presso il Responsabile del Certificatore o RA-I. Questi provvede all'inoltro della richiesta al Certificatore con le modalità descritte nel presente paragrafo;
Il Titolare deve compilare la richiesta indicando:

- nome e cognome;
- sede e AGC di appartenenza;
- dati identificativi del certificato (numero seriale);
- motivazione e decorrenza della revoca;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

Il Certificatore, ricevuta la richiesta, provvede alla revoca del certificato, al suo inserimento nell'apposita Lista dei certificati revocati (CRL) ed alla pubblicazione della Lista nel Registro dei certificati.
Il Certificatore comunica al soggetto Titolare ed al Responsabile RA-I l'avvenuta revoca. La comunicazione viene effettuata con documento informatico firmato digitalmente, o con lettera raccomandata.

Procedure di revoca dei certificati su richiesta del Responsabile RA-I

Il Responsabile RA può inoltrare la richiesta di revoca dei certificati al Certificatore attraverso una richiesta scritta con firma autografa;
La richiesta scritta e sottoscritta dal Responsabile RA-I è inoltrata al Certificatore nei tempi e con le modalità previste dal presente paragrafo.
La richiesta deve indicare:

- nome e cognome del Titolare;
- AGC, Settore e Servizio di appartenenza;
- dati identificativi del certificato (numero seriale);
- decorrenza della revoca ;
- eventuali altri elementi rilevanti a determinare i casi di maggiore urgenza ovvero di emergenza.

Il Responsabile RA-I comunica la richiesta al Certificatore, che ne rilascia ricevuta.

Il Certificatore, ricevuta la richiesta, provvede alla revoca del certificato, al suo inserimento nella apposita Lista dei certificati revocati (CRL) ed alla pubblicazione della lista nel Registro dei certificati.

Il Certificatore notifica al Titolare ed al Responsabile RA-I l'avvenuta revoca. La comunicazione viene effettuata con documento informatico firmato digitalmente o con lettera raccomandata.

Procedure di revoca dei certificati su iniziativa del Certificatore

Il certificatore può revocare un certificato, comunicandone la motivazione e la data ed ora a partire dalla quale il certificato non sarà più valido.
Nei casi di motivata urgenza, il certificatore procede alla revoca senza fornire alcun preavviso al Titolare.

Disponibilità dei servizi di revoca

Il Certificatore garantisce la disponibilità del servizio dal Lunedì al Venerdì negli orari di ufficio, sia per le richieste di revoca inoltrate tramite modulo firmato digitalmente e trasmesso telematicamente sia per la richiesta di revoca sottoscritta in modo autografo.

Aggiornamento delle Liste dei Certificati revocati (CRL)

Le liste di revoca dei certificati sono aggiornate in seguito ad ogni richiesta di revoca e ad esse è apposta una marca temporale.
La pubblicazione nel Registro dei certificati avviene ogni 4 (quattro) ore.
In caso di richiesta di revoca del certificato per certa o sospetta compromissione, manomissione o perdita del possesso della chiave privata, il Certificatore procede all'inserimento del certificato nella Lista di revoca e alla pubblicazione immediata della stessa nel Registro dei certificati.

MODALITÀ DI SOSTITUZIONE DEI CERTIFICATI

Sostituzione delle chiavi del Titolare

I certificati di firma hanno una validità di tre anni. Tale validità vincola e limita l'utilizzo dei certificati, e delle relative chiavi, da parte del Titolare che, almeno sessanta giorni prima della scadenza, dovrà chiederne la sostituzione al Certificatore che rilascia un nuovo certificato secondo la procedura remota riportata al par 7.7.1.

Sostituzione delle chiavi di certificazione

Il Certificatore, 90 giorni prima della scadenza del certificato relativo ad una chiave di certificazione avvia la procedura di sostituzione, generando una nuova coppia di chiavi.

REGISTRO DEI CERTIFICATI

Informazioni contenute nel Registro dei certificati

Il Certificatore pubblica le seguenti informazioni nel Registro dei certificati:

- elenco di tutti i certificati emessi;
- lista dei certificati revocati (CRL);

Le liste dei certificati revocati sono conformi allo standard ITU X.509.

Procedura di gestione del Registro dei certificati

Il Registro dei certificati è consultabile da qualsiasi soggetto autorizzato nel dominio di esercizio 24 ore al giorno, 7/7 giorni, esclusi i tempi dedicati alla manutenzione programmata.
Il Registro dei certificati è gestito dalla directory di sistema ITU-T X.500.
Il Certificatore mantiene una copia di riferimento del Registro dei certificati, inaccessibile dall'esterno, allocata su un sistema sicuro installato in locali protetti.
Sistematicamente, verifica la conformità tra la copia operativa e la copia di riferimento del Registro, annotando ogni discordanza nel Registro operativo.
Modificazioni al contenuto del Registro dei certificati sono effettuate esclusivamente da personale autorizzato. Tali operazioni sono sistematicamente registrate sul Giornale di controllo inoltre sono annotate la data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il Registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile.
Una copia di sicurezza della copia operativa e di quella di riferimento del Registro dei certificati sono conservate in armadi di sicurezza distinti, situati in locali diversi.

Procedura di aggiornamento del Registro dei certificati

Il Certificatore provvede all'aggiornamento del Registro dei certificati quando:

- emette nuovi certificati;
- pubblica Liste di revoca in seguito alla revoca di un certificato;

Ogni aggiornamento viene asseverato mediante apposizione di marca temporale.
Il Certificatore cura l'allineamento tra copia di riferimento copia operativa e copia di sicurezza del Registro dei certificati secondo la seguente procedura:

- Il Responsabile del Registro dei certificati controlla l'applicazione che pubblica ed aggiorna la Lista dei certificati emessi sulla copia di riferimento. L'inserimento/cancellazione di un certificato nella copia di riferimento viene registrato nel Giornale di controllo e asseverato mediante apposizione di marca temporale
- Il Responsabile del Registro dei certificati controlla l'applicazione che pubblica ed aggiorna le Liste di revoca sulla copia di riferimento. L'inserimento/cancellazione di un certificato nella CRL viene registrato nel Giornale di controllo e asseverato mediante apposizione di marca temporale.
- Il Responsabile del Registro dei certificati cura l'allineamento tra la copia di riferimento e la copia operativa.

Modalità di accesso al Registro dei certificati

Il registro dei certificati è un Internet Directory Server e server LDAP compatibile con le specifiche X.500 1993 e che supporta il protocollo LDAP v. 3. Il registro dei certificati è accessibile per i soggetti autorizzati all'indirizzo Intranet della Regione Campania.

PROTEZIONE DELLA RISERVATEZZA

Modalità di protezione della riservatezza

Tutti i dati che risiedono su database sono protetti da prodotti che implementano politiche di autorizzazione per l'accesso ai dati legati a meccanismi di autenticazione degli utenti.

Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali, di cui all'art. 34 del D. Lgs. 196/2003 e dall'Allegato B del medesimo Decreto, nell'esecuzione delle seguenti attività:

- individuazione degli incaricati;
- assegnazione di codici identificativi;
- protezione degli elaboratori;
- modalità di designazione degli incaricati del trattamento.

GESTIONE DELLE COPIE DI SICUREZZA

Il Certificatore effettua periodicamente, e secondo politiche ben definite, copie di sicurezza del sistema di certificazione.

Tali copie sono mantenute in armadi di sicurezza siti in locali diversi e ugualmente protetti. In tal modo viene garantita l'integrità dei dati e la continuità del servizio di certificazione.

Le procedure per la gestione delle copie di sicurezza sono descritte nel Piano per la sicurezza..

GESTIONE DEGLI EVENTI CATASTROFICI

Il Certificatore in caso di disastro, predispone opportune procedure che consentono il tempestivo ripristino dei servizi del sistema di certificazione

Le procedure per la gestione degli eventi catastrofici si uniformano a quanto previsto dal Documento Programmatico per la Sicurezza della Regione Campania.

GIORNALE DI CONTROLLO

Tutte le registrazioni effettuate automaticamente dai dispositivi installati presso il Certificatore, sono archiviate ed annotate nel Giornale di controllo.

Dati da archiviare

I dati da annotare e da archiviare nel Giornale di Controllo, cui è associata la data e l'ora dell'effettuazione, sono i seguenti:

1. ogni sessione di lavoro relativa alla generazione della coppia di chiavi al di fuori del dispositivo di firma;
2. la personalizzazione del dispositivo di firma;
3. la generazione dei certificati, siano essi relativi a chiavi di sottoscrizione che a chiavi di certificazione o di marcatura temporale;
4. la revoca dei certificati emessi;
6. l'entrata e l'uscita dai locali protetti del sistema di generazione dei certificati;
7. l'inizio e la fine di ciascuna sessione di lavoro inerente alla generazione dei certificati;
8. tutte le operazioni che modificano il contenuto del Registro dei certificati, ossia l'aggiornamento delle liste di revoca e la pubblicazione dei certificati generati;
9. la data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il Registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile.

Conservazione dei dati

Le registrazioni sono effettuate indipendentemente su supporti distinti e di tipo. Esse riportano la data e l'ora in cui sono state effettuate e sono conservate per un periodo di 30 anni.

Protezione dell'archivio

Il Giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.

Gestione del Giornale di controllo

Alla funzione della Sicurezza Dati è demandato il compito di gestire il Giornale di controllo, attraverso l'effettuazione di operazioni di back-up, controlli e report periodici.

Verifiche

L'integrità del Giornale di controllo è verificata con frequenza mensile