# Certificate Policy
# Certificati di autenticazione
# Carta Nazionale dei Servizi

| | | | |
|---|---|---|---|
| Redatto da: | Fulvio Parisi<br>Area Prodotti e Servizi | | Data |
| Verificato da: | Massimo Sciarra<br>Responsabile Area<br>Erogazione e Sviluppo | | Data |
| Verificato da: | Arturo Salvatici<br>Responsabile Area Prodotti<br>e Servizi | | Data |
| Verificato da: | Giorgio Marzorati<br>Responsabile Area<br>Assistenza e Delivery | | Data |
| Approvato da: | Paolo Soru<br>Amministratore Delegato | | Data |

*Il documento è :*

- ***REDATTO*** *se provvisto della/e firma/e di redazione,*
- ***VERIFICATO*** *se provvisto anche della firma di verifica,*
- ***APPROVATO*** *se provvisto di tutte le firme*

Codice documento: **CAACT** - 05 - 01 - 01

*Codice Progetto Cod Sottoprog. N. Doc Versione*

Distribuzione: PUBBLICA

# STORIA DELLE MODIFICHE APPORTATE

**Non applicabile, poiché questa è la prima versione del documento.**

## LEGENDA DI COPERTINA

### Stato del documento

Le firme sulla copertina del presente documento fanno riferimento allo standard interno di ACTALIS per la gestione della documentazione del Sistema Qualità: hanno lo scopo di permetterne il controllo di configurazione e di indicarne lo stato di lavorazione.
*Si segnala che la firma di approvazione autorizza la circolazione del documento limitatamente alla lista di distribuzione e non implica in alcun modo che il documento sia stato revisionato e/o accettato da eventuali Enti esterni.*
In particolare, il documento è da intendersi **REDATTO** se provvisto della/e firma/e di chi lo ha redatto; **VERIFICATO** se ha superato con esito positivo la verifica interna e quindi provvisto della/e firma/e di verifica che ne autorizza il rilascio alla GESTIONE DELLA CONFIGURAZIONE. Nel caso in cui la revisione abbia esito negativo il documento viene modificato e verificato, con un nuovo numero di versione e una nuova data di emissione. Il documento è da intendersi **APPROVATO** se provvisto della firma di approvazione che si aggiunge alle altre.
Un documento sprovvisto di firme è in uno stato indefinito, e non può essere messo in circolazione.

### Distribuzione

La distribuzione di un documento può essere:
- **PUBBLICA**, se il documento può circolare senza restrizioni;
- **INTERNA**, se il documento può circolare solo all'interno di ACTALIS;
- **RISERVATA,** se il documento è distribuibile ad un numero limitato di destinatari;
- **CONTROLLATA**, se il documento è distribuibile ad un numero limitato di destinatari e ogni copia è controllata.

# SOMMARIO

# 1. GENERALITÀ

## 1.1 Scopo

Il presente documento descrive la policy ovvero le regole generali relative all'emissione ed all'utilizzo dei certificati di autenticazione per la Carta Nazionale dei Servizi erogati dal Certificatore accreditato Actalis S.p.A. (di seguito Actalis).

Le procedure operative per l'erogazione del servizio di certificazione sono presenti in un apposito manuale operativo pubblico redatto dall'Ente Emettitore.

## 1.2 Validità

Il presente documento si considera valido nella versione riportata nella sezione di configurazione in copertina.

## 1.3 Riferimenti

1-CA-2001-008-02 – Servizio di certificazione – Gestione backup CA – Documento interno Actalis;

SQ01-00-13-03 – Procedura per la gestione delle verifiche ispettive – Documento interno Actalis;

2-1INFCRT00-2002-002-01-0 – Piano per la sicurezza – Servizio di certificazione – Documento interno Actalis;

SQ01-00-01 Manuale della Qualità – Documento interno Actalis;

CAACT-00-00-03 – Manuale operativo certificati qualificati pubblicato sul sito CNIPA (www.cnipa.it);

[RFC1777] – "Lightweight Directory Access Protocol"

[RFC2246] – "The TLS Protocol version 1"

[RFC2818] – "HTTP over TLS"

[RFC3280] - "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"

[DPR445] Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.

[DIR] Direttiva del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche (Gazzetta Ufficiale delle Comunità europee L. 13 del 13 dicembre 1999).

[DLGS 10] Decreto Legislativo 23 gennaio 2002, n. 10: "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche", pubblicato sulla Gazzetta Ufficiale. n. 39 del 15 febbraio 2002.

[DLGS 196] Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n.123 della Gazzetta Ufficiale n. 174, 29 luglio 2003.

[Decreto] Decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze 9 dicembre 2004, recante "Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi" pubblicato nella Gazzetta ufficiale n.296, 18 dicembre 2004.

[LG] Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi, Area Regolazione e Formazione: ufficio Standard e metodologie del CNIPA, 11 marzo 2005

## 1.4 Acronimi

| | |
|---|---|
| ASN.1 | Abstract Syntax Notation n. 1 |
| CA | Certification Authority |
| CIE | Carta d'Identità Elettronica |
| CNIPA | Centro Nazionale per l'Informatica nella Pubblica Amministrazione |
| CNS | Carta Nazionale dei Servizi |
| CP | Certificate Policy |
| CPS | Certificate Practice Statement |
| CRL | Certificate Revocation List |
| CRS | Carta Regionale dei Servizi |
| DN | Distinguished Name |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secure |
| INA | Indice Nazionale delle Anagrafi |
| ITU-T | International Telecommunication Union |
| LDAP | Lightweight Directory Access Protocol |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PDF | Portable Document Format |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| RFC | Request For Comments |
| RNG | Random Number Generator |
| RSA | Rivest Shamir Adleman |
| SISS | Sistema Informativo Socio Sanitario |
| SSL | Secure Socket Layer |
| TLS | Tansport Layer Security |
| TVCC | TeleVision Closed Circuit |
| UNI | Ente nazionale italiano di UNIficazione |
| UPS | Uninterruptible Power Supply |
| URI | Uniform Resource Identifier |
| VMD | Video Motion Dectection |
| WWW | World Wide Web |

## 1.5 Definizioni

Di seguito sono elencate le definizioni utilizzate nel presente documento:

**Certificate Policy**
La CP è un insieme di regole che indica l'applicabilità di un certificato ad una comunità e/o ad una classe di applicazioni che condividono gli stessi requisiti di sicurezza.

**Certificato digitale**
Insieme di dati elettronici firmati dalla Certification Authority con la chiave privata di certificazione, che garantisce la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica. Il formato del certificato ed i dati ivi contenuti sono definiti dallo standard ITU-T X.509;

**Carta Nazionale dei Servizi**
Documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni. Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete.

**Certification Authority**
Entità pubblica o privata che presta servizi di certificazione (generazione, emissione, conservazione, revoca, sospensione dei certificati) ed altri servizi connessi alla certificazione (es. apposizione riferimento temporale o marcatura temporale ai certificati).

**Certificatore accreditato**
La CA che eroga certificati qualificati ovvero conformi ai requisiti di cui all'allegato I della [DIR] e che risponde ai requisiti fissati dall'allegato II delle medesima direttiva.

**Certification Practice Statement**
Il CPS definisce le procedure che una CA utilizza nell'emissione e gestione (revoca, sospensione, rinnovo) dei certificati digitali. Contiene pertanto delle informazioni più dettagliate rispetto ad una CP sulle metodologie utilizzate da una CA. Un utente valuta l'affidabilità di una CA anche sulla base di quanto dichiarato nel CPS. Il CPS deve essere reso pubblico.

**Ente Emettitore**
Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS.

**Manuale Operativo**
In ambito CNS il manuale operativo descrive le procedure seguite dall'Ente Emettitore per la gestione di tutte le fasi del processo di emissione e gestione delle carte.

**Personalizzazione carte**
La personalizzazione delle carte è quella fase del processo di emissione delle carte in cui sono inserite le informazioni utente necessarie per l'identificazione in rete e per gli altri servizi previsti. Nel corso della personalizzazione sono generati il PIN_utente ed il PUK stampati all'interno di buste retinate.

**PIN_utente**
E' il PIN con cui il titolare attiva le operazioni di autenticazione in rete.

# 2. INTRODUZIONE

Un certificato associa una chiave pubblica di crittografia ad un insieme d'informazioni che identificano un soggetto (individuo o dispositivo). Tale soggetto, il "titolare" del certificato, possiede ed utilizza la corrispondente chiave privata. Altri soggetti, gli utenti, identificano il Titolare verificando, tramite la chiave pubblica contenuta nel certificato, la corrispondenza con la chiave privata. Gli utenti fanno pertanto affidamento sul processo di certificazione della chiave pubblica del Certificatore che svolge il ruolo di "terza parte fidata".

Actalis genera, in qualità di Certificatore, diverse tipologie di certificati digitali. In particolare Actalis, ai sensi dell'articolo 5 del [DLGS 10], è un certificatore accreditato che genera i certificati digitali di autenticazione per la CNS. I certificati di autenticazione CNS sono generati sulla base delle informazioni anagrafiche ottenute in fase di registrazione dall'Ente Emettitore. I certificati digitali di autenticazione CNS sono utilizzati per tutte le funzioni di riconoscimento in rete ed, in combinazione con il PIN utente, consentono l'utilizzo dei servizi in rete delle Pubbliche Amministrazioni da parte del titolare. I certificati di autenticazione CNS sono utilizzati con il protocollo SSL/TLS che stabilisce un canale di comunicazione sicuro tra browser e web server.

Il canale di comunicazione sicuro garantisce:

- riservatezza dei messaggi;
- integrità dei messaggi;
- mutua autenticazione delle parti coinvolte (browser e web server)

## 2.1 Certificate Policy e manuale operativo

Actalis pubblica la CP sul sito web del servizio di certificazione https://portal.actalis.it. I riferimenti a tale documento sono inseriti nel certificato.
Il manuale operativo è predisposto dall'Ente Emettitore – rif. punto 4.4.2 dell'Allegato al [Decreto].

CP e manuale operativo consentono di valutare le caratteristiche ed il livello di affidabilità del servizio di certificazione.

## 2.2 Comunità ed Applicabilità

### 2.2.1 Autorità di certificazione

Actalis è l'autorità di certificazione o Certificatore responsabile della generazione del certificato di autenticazione secondo le specifiche presenti nell'Allegato 2 del [Decreto].

Il Certificato delle chiavi di certificazione che firma i certificati di autenticazione è pubblicato in un elenco presente sul sito web del CNIPA firmato digitalmente. La disponibilità del certificato delle chiavi di certificazione consente la verifica della firma apposta sui certificati di autenticazione.

Di seguito i dati completi che identificano il Certificatore:

| | |
|---|---|
| Denominazione sociale: | **Actalis S.p.A.** |
| Indirizzo della sede legale: | **Via Torquato Taramelli, 26 – 20124 Milano** |
| Legale rappresentante: | **Paolo Michele Soru** (Amministratore Delegato) |
| N° di iscrizione al Registro delle Imprese di Milano: | **R.E.A. n. 1669411** |
| N° di Partita IVA: | **03358520967** |
| N° di telefono (centralino): | **+39 02 68825.1** |
| DUNS number: | **440-489-735** |
| ISO Object Identifier (OID): | **1.3.159** |
| Sito web generale (informativo): | http://www.actalis.it/ |
| Sito web del servizio di certificazione: | https://portal.actalis.it |
| E-mail (informativo): | info@actalis.it |
| Directory server (registro dei certificati): | ldap://ldap.actalis.it |
| | ldap://ldap.csp.multicertify.com |

### 2.2.2 Ente Emettitore

L'Ente Emettitore è la Pubblica Amministrazione che emette la CNS. L'Ente Emettitore è responsabile della registrazione ed identificazione dei richiedenti, dell'aggiornamento dell'INA, della personalizzazione e consegna delle CNS, della successiva gestione delle carte, del rispetto delle normative di tutela dei dati personali.
Per le attività di personalizzazione delle carte e di gestione della CNS, l'Ente Emettitore può avvalersi di servizi di terzi nel rispetto dei requisiti di cui al punto 4.4.2 delle [Regole].

### 2.2.3 Utenti

Gli utenti o relying parties sono tutti quei soggetti che, partecipando ad una transazione telematica, fanno affidamento sul certificato emesso da Actalis ed accettano la presente CP. Gli utenti possono anche non essere titolari di certificati.

### 2.2.4 Titolari

I titolari sono le persone fisiche in possesso di un certificato di autenticazione emesso da Actalis conforme alle regole descritte nella presente CP.

## 2.3 Applicabilità

L'ambito di utilizzo del certificato di autenticazione CNS è il browser web per l'autenticazione tramite protocollo SSL/TLS ed una firma elettronica avanzata nel formato S/MIME. La firma elettronica assicura l'origine delle informazioni e la loro integrità.

L'affidabilità della chiave privata è garantita dalla validità del certificato della corrispondente chiave pubblica ovvero che tale certificato non sia né scaduto, né revocato o sospeso.

In particolare, nell'ambito del progetto CRS Lombardia_SISS della Regione Lombardia, con la chiave privata è prevista anche la firma di un documento che attesta la presenza del cittadino durante l'erogazione di un servizio sanitario.

## 2.4 Dettagli relativi ai contatti

### 2.4.1 Organizzazione di gestione

L'organizzazione che gestisce la presente CP è Actalis.

### 2.4.2 Persona da contattare

Richieste di informazioni sulla presente CP possono essere inoltrate al seguente indirizzo:

Actalis S.p.A.
Via del Giorgione, 59
00147 – ROMA
tel. 06590141
fax: 0659014613

### 2.4.3 Responsabile dell'approvazione

Responsabile dell'approvazione del presente manuale è l'Amministratore Delegato di Actalis, previa verifica dei Responsabili delle Aree organizzative coinvolte indicate nel frontespizio.

# 3. CONDIZIONI GENERALI

## 3.1 Obblighi

### 3.1.1 Obblighi del Certificatore

Il certificatore è tenuto a:

- non rendersi depositario di chiavi private;
- generare il certificato garantendo l'associazione tra la chiave pubblica ed il Titolare secondo i dati comunicati dall'Ente Emettitore;
- garantire un servizio di revoca e sospensione dei certificati con le stesse modalità utilizzate per i certificati qualificati di firma digitale (rif. CAACT-00-00-03);
- attenersi alle regole e procedure previste per i Certificatori nel [Decreto]

### 3.1.2 Obblighi dell'Ente Emettitore

L'Ente Emettitore ha l'obbligo di:

- verificare l'identità del Richiedente;
- registrare i dati del Richiedente;
- comunicare al Certificatore dati e documenti acquisiti in fase di identificazione affinché il Certificatore emetta il certificato;
- informare il Richiedente sulla necessità di tenere segreta la chiave privata e di custodire in modo protetto la CNS;

- attenersi al [DLGS 196] ed alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'articolo 33 del suddetto [DLGS 196];
- predisporre il manuale operativo;
- redigere un manuale utente sulle modalità di utilizzo della CNS e sulle procedure da seguire in caso di smarrimento, furto o timore di compromissione della carta;
- definire accordi di servizio con il Certificatore secondo adeguate garanzie di affidabilità e sicurezza;
- garantire che le operazioni relative al servizio di certificazione avvengano nel rispetto della presente CP e del manuale operativo e secondo le modalità indicate in eventuali specifici accordi di servizio con il Certificatore;
- inoltrare al Certificatore le richieste di revoca e sospensione dei certificati inoltrate dal Titolare;

### 3.1.3 Obblighi dei Titolari

Il Titolare ha l'obbligo di:

- fornire informazioni esatte e veritiere in fase di registrazione;
- custodire la chiave privata con la massima diligenza
- proteggere e conservare il PIN per l'abilitazione della CNS affinché nessun altro soggetto possa avervi accesso ed in luogo diverso da quello in cui è custodita la CNS;
- proteggere e conservare il PUK per lo sblocco della CNS affinché nessun altro soggetto possa avervi accesso ed in luogo diverso da quello in cui è custodita la CNS;
- non essere Titolare di una CIE;
- richiedere immediatamente la revoca del certificato nel caso in cui si sospetti o si sia verificata la compromissione della chiave privata;
- prendere visione della presente CP prima di richiedere all'Ente Emettitore di essere registrato;
- successivamente alla registrazione e fino alla scadenza o revoca del certificato, avvisare prontamente l'Ente Emettitore di ogni variazione alle informazioni fornite in fase di registrazione;
- adottare tutte le misure tecniche ed organizzative idonee ad evitare danno ad altri;
- inoltrare tempestivamente all'Ente Emettitore la richiesta di revoca o sospensione del certificato secondo le procedure indicate dall'Ente Emettitore nel manuale operativo ed al verificarsi di una delle condizioni previste nella presente CP;

### 3.1.4 Obblighi degli utenti

L'Utente ha l'obbligo di:

- conoscere la presente CP;
- verificare la validità del certificato ovvero che non sia presente nella lista dei certificati revocati e sospesi e che non sia scaduto;
- adottare tutte le misure tecniche ed organizzative idonee ad evitare danno ad altri;

L'utente è responsabile per tutti gli utilizzi non conformi ai suindicati punti.

## 3.2 Responsabilità e garanzie

### 3.2.1 Garanzie dell'Autorità di Certificazione

Actalis garantisce che:

- i certificati emessi sono aderenti ai requisiti indicati nella presente CP;
- il certificato è stato generato secondo i dati comunicati dall'Ente Emettitore;

#### 3.2.1.1 Esclusioni di ulteriori garanzie dell'Autorità di Certificazione

Fatti salvi i casi di dolo o colpa grave, Actalis esclude qualsiasi ulteriore garanzia rispetto a quanto dichiarato nel paragrafo 3.2.1

#### 3.2.1.2 Limitazioni di responsabilità dell'Autorità di Certificazione

Fatti salvi i limiti inderogabili di legge, la responsabilità di Actalis sussisterà solo nei casi di dolo o colpa grave.

Actalis non sarà responsabile di eventuali disservizi derivanti dal mancato rispetto, da parte del Titolare o di soggetti terzi, delle norme e specifiche tecnico-operative contenute nella presente CP o da esso richiamate.
Actalis non è responsabile per l'utilizzo da parte del Titolare di un certificato revocato o sospeso.

Actalis non é responsabile per i danni conseguenti ad un utilizzo non conforme del certificato.

#### 3.2.1.3 Forza maggiore

Actalis non sarà responsabile di qualsiasi inadempimento o di qualsiasi evento dannoso, qualora tale mancata esecuzione sia dovuta a cause non imputabili ad Actalis, quali - a scopo esemplificativo e senza intento limitativo - caso fortuito, disfunzioni di ordine tecnico assolutamente imprevedibili e poste al di fuori di ogni controllo, interventi dell'autorità, cause di forza maggiore, calamità naturali, scioperi anche aziendali - ivi compresi quelli presso soggetti di cui le parti si avvalgano nell'esecuzione delle attività connesse al contratto - ed altre cause imputabili a terzi.

## 3.3 Responsabilità del cliente

### 3.3.1 Garanzie del Titolare

Il Titolare garantisce che:

- nessun soggetto non autorizzato possa avere accesso alla chiave privata;
- non utilizzerà la chiave privata per firmare digitalmente un certificato o una CRL;
- tutte le informazioni fornite all'Ente Emettitore sono veritiere;
- proteggere e conservare il codice di attivazione (PIN) ed il codice di sblocco (PUK) della CNS, in luogo sicuro e diverso da quello in cui tale dispositivo è custodito;

## 3.4 Responsabilità dell'utente

Gli utenti sono responsabili in esclusiva della decisione se fare affidamento o meno sulle informazioni presenti nel certificato.

Gli utenti sono tenuti a:

- verificare che il certificato non sia scaduto, revocato o sospeso;
- adottare tutte le misure tecniche ed organizzative idonee ad evitare danno ad altri;
- conoscere l'ambito di utilizzo del certificato ed i limiti di responsabilità del Certificatore indicati nella presente CP;

## 3.5 Interpretazione ed attuazione

### 3.5.1 Legge applicabile

La presente CP è soggetta alla legge italiana e come tale sarà interpretata ed eseguita. Per quanto non espressamente previsto nella presente CP, valgono le norme vigenti.

## 3.6 Clausola compromissoria

### 3.6.1 Controversie tra Actalis e Clienti

Qualsiasi controversia derivante dalla presente CP tra Actalis ed i Titolari è deferita al giudizio di un collegio arbitrale.

La sede dell'arbitrato sarà Milano.

## 3.7 Tariffe

Le tariffe del servizio sono pubblicate sul sito web del servizio di certificazione https://portal.actalis.it.

## 3.8 Pubblicazione

### 3.8.1 Pubblicazione di informazioni sulla CA

Actalis pubblica informazioni relative alla CA sul sito web del servizio di certificazione https://portal.actalis.it.

Il registro dei certificati contenente le liste di revoca è realizzato con software di tipo "directory server". La sua copia pubblica é interrogabile con protocollo LDAP definito nella specifica pubblica [RFC 1777] attraverso Internet.

### 3.8.2 Controlli di accesso

Lo svolgimento delle operazioni che modificano il contenuto del registro dei certificati è possibile solo per il personale espressamente autorizzato. In ogni caso, tutte le operazioni che modificano il contenuto del registro dei certificati sono tracciate nel giornale di controllo. Ad ogni evento registrato nel giornale di controllo è apposto un riferimento temporale contenente la data e l'ora.

Il registro dei certificati è sottoposto ad un monitoraggio che permette di rilevare e segnalare qualsiasi evento che comprometta i requisiti di sicurezza.

## 3.9 Tutela dei dati personali

Responsabile del rispetto delle normative vigenti in merito alla tutela dei dati personali è l'Ente Emettitore.

I dati personali di cui viene in possesso il Certificatore sono trattati conformemente al [DLGS 196]. IL Certificatore predispone tutele rispondenti almeno alle misure minime stabilite nello stesso decreto legislativo.

Per il servizio erogato sulla base della presente CP, il certificatore non tratta dati sensibili ai sensi dell'articolo 4 comma 1 lettera d) o giudiziari ai sensi dello stesso articolo comma 1 lettera e) del [DLGS 196.

## 3.10 Verifiche di conformità

### 3.10.1 Oggetto

Actalis garantisce di effettuare costanti controlli sul rispetto delle norme definite nel presente documento e dei provvedimenti legislativi vigenti ed applicabili.

## 3.11 Diritti di proprietà intellettuale

### 3.11.1 Diritti di proprietà della CP

Il contenuto della presente CP è di proprietà di Actalis che si riserva tutti i diritti.

### 3.11.2 Diritti di proprietà delle chiavi e dei certificati

Le coppie di chiavi crittografiche asimmetriche sono di proprietà del Titolare.

I certificati e le CRL sono di proprietà di Actalis.

Relativamente alla proprietà di altri dati ed informazioni si applicano le leggi vigenti dello Stato italiano.

# 4. OPERATIVITA'

## 4.1 Identificazione e Registrazione

L'identificazione del Richiedente e la registrazione dei dati è a cura dell'Ente Emettitore. Le relative procedure operative sono descritte nel manuale operativo dell'Ente Emettitore. E' predisposto un canale securizzato tra Ente Emettitore e Certificatore per la trasmissione dei dati.

## 4.2 Rinnovo del certificato

Il certificato, in prossimità di scadenza, può essere rinnovato con l'emissione di un nuovo certificato.

Il rinnovo consiste nella generazione di una nuova coppia di chiavi sostitutiva di quella in scadenza e nella conseguente certificazione della nuova chiave pubblica.

### 4.2.1 Richiedenti

La richiesta di rinnovo è presentata dal Titolare.

### 4.2.2 Procedura per il rinnovo

La procedura per il rinnovo del certificato è descritta nel manuale operativo dell'Ente Emettitore.

## 4.3 Revoca del certificato

La revoca determina la cessazione anticipata della validità di un certificato da un dato momento. La revoca di un certificato è irreversibile e non retroattiva.

Il certificato revocato è inserito nella lista dei certificati revocati (CRL).

### 4.3.1 Condizioni per la revoca

La revoca può avvenire in seguito alle seguenti circostanze:

A. smarrimento, furto o guasto della CNS su cui è presente il certificato;
B. compromissione della chiave privata;
C. compromissione del PIN di attivazione della CNS su cui è presente il certificato;
D. variazione dei dati del Titolare presenti nel certificato;
E. mancato rispetto della presente CP;
F. mancato rispetto del manuale operativo dell'Ente Emettitore;

Nel caso di cui al punto E, il Certificatore si riserva la facoltà di revocare il certificato. Salvo i casi di motivata urgenza, l'intenzione di revocare il certificato è comunicata al Titolare anticipatamente con relativa motivazione e data di decorrenza. Successivamente il Certificatore invia una notifica al Titolare.

### 4.3.2 Richiedenti

La richiesta di revoca è inoltrata dal Titolare, dall'Ente Emettitore o su iniziativa del Certificatore.

### 4.3.3 Procedura per la revoca

Le procedure per richiedere la revoca sono indicate nel manuale operativo dell'Ente Emettitore.

## 4.4 Sospensione e riattivazione

La sospensione determina l'interruzione temporanea della validità di un certificato. La sospensione è un'operazione reversibile e non retroattiva.

Il certificato sospeso è inserito nella lista dei certificati revocati e sospesi (CRL).

Al termine della durata della sospensione, il certificato è riattivato.

## 4.5 Condizioni per la sospensione

Le condizioni che possono determinare una richiesta di sospensione sono:

A. sospetta compromissione della chiave privata;
B. interruzione temporanea del servizio;
C. mancata verifica in tempo utile dell'autenticità di una richiesta di revoca

Actalis si riserva la facoltà di sospendere il certificato per sospetti abusi nel suo utilizzo. Salvo i casi di motivata urgenza, qualora il certificatore intenda sospendere un certificato ne darà preventiva comunicazione al titolare,

specificando i motivi della sospensione, la data di decorrenza della stessa e la durata. Successivamente il Certificatore invia una notifica al Titolare.

### 4.5.1 Richiedenti

La richiesta di sospensione è inoltrata dal Titolare, dall'Ente Emettitore o su iniziativa del Certificatore.

### 4.5.2 Procedura per la sospensione

Le procedure per richiedere la sospensione sono indicate nel manuale operativo dell'Ente Emettitore.

## 4.6 Frequenza pubblicazione CRL/CSL

La CRL è l'elenco dei certificati revocati e sospesi pubblicato dal Certificatore nel registro dei certificati. L'elenco, il cui formato è definito nella raccomandazione ITU-X.509, è firmato digitalmente dal Certificatore. Il Certificatore svolge l'attività nel più breve tempo possibile. La frequenza di pubblicazione è indicata nel capitolo descrittivo delle caratteristiche delle chiavi di certificazione e dei certificati di autenticazione da queste firmati (rif. 7).

### 4.6.1 Condizioni per la consultazione delle CRL

Una copia della CRL presente nel registro dei certificati è liberamente consultabile con protocollo LDAP per la sola lettura attraverso la rete Internet. Le operazioni di modifica del registro dei certificati è consentito solo al personale del Certificatore autorizzato. Qualsiasi operazione di modifica è tracciata nel giornale di controllo. L'indirizzo del registro dei certificati in cui è presente la CRL è indicato nel capitolo descrittivo delle caratteristiche delle chiavi di certificazione e dei certificati di autenticazione da queste firmati (rif. 7).

## 4.7 Procedure verifiche di sicurezza

### 4.7.1 Tipologia eventi registrati

Gli eventi registrati, su carta ed in elettronico, sono relativi alla gestione del ciclo vitale dei certificati inclusi richieste di certificazione, di rinnovo, revoca/sospensione, generazione e rilascio certificati e CRL. Sono registrati anche altri eventi quali tentativi di accesso al sistema della PKI, le operazioni svolte dal personale Actalis, l'entrata e l'uscita di visitatori nei locali in cui si svolge l'attività di certificazione.

Gli eventi summenzionati sono elencati a titolo esemplificativo e non esaustivo.

La classificazione completa delle informazioni con la relativa definizione degli obiettivi di sicurezza, l'individuazione delle minacce e delle conseguenti contromisure sono descritte dettagliatamente nel "Piano per la sicurezza" (rif.1.3).

### 4.7.2 Copie di sicurezza

La copia di sicurezza (backup) dei dati, delle applicazioni, del giornale di controllo e di ogni altro file necessario al completo ripristino degli elaboratori critici del sistema è effettuata quotidianamente. La descrizione dettagliata della procedura di backup è presente nel documento "Gestione backup CA" (rif.1.3).

### 4.7.3 Protezione ed archiviazione supporti di backup

I salvataggi sono effettuati su supporti magneto/ottici custoditi in un armadio blindato ubicato in un sito distinto da quello in cui avvengono i salvataggi. Gli accessi ai siti sono controllati mediante badge personale + PIN. I salvataggi sono effettuati su nastri gestiti da librerie a rotazione e successivamente copiati sul nastro magnetico che quotidianamente l'operatore estrae, archivia e sostituisce con il nastro nuovo.

### 4.7.4 Giornale di controllo

L'insieme delle registrazioni effettuate automaticamente dai dispositivi installati presso il Certificatore costituisce il giornale di controllo.

Di ogni evento è registrata la tipologia, la data e l'ora di registrazione e, se disponibili, altre informazioni utili ad individuare gli utenti coinvolti nell'evento.

### 4.7.5 Protezione e backup del giornale di controllo

I file che compongono il giornale di controllo sono trasferiti tutti i giorni su supporto permanente.

I file generati automaticamente dal sistema e dalle applicazioni che formano il giornale di controllo sono accessibili in scrittura solo dai processi a ciò preposti.

L'integrità del giornale di controllo è verificata mensilmente.

### 4.7.6 Gestione ripristino da compromissione o da disastro

Per "compromissione" s'intende la violazione di una o più condizioni vincolanti per l'erogazione del servizio; per "disastro" s'intende un evento dannoso le cui conseguenze determinano l'indisponibilità del servizio in condizioni ordinarie. A seguito di situazioni di "compromissione" o di "disastro" sono previste apposite procedure finalizzate al ripristino (recovery) dei servizi di certificazione.
Tali procedure sono dettagliatamente descritte nel "Piano per la sicurezza" (rif.1.3).

Il ripristino da compromissione o disastro avviene in ogni caso nelle seguenti situazioni:

1. guasti di una o più delle apparecchiature usate per erogare i servizi di certificazione;
2. compromissione (es. rivelazione a terzi non autorizzati oppure perdita) di una o più chiavi private di certificazione;
3. inagibilità dei locali e/o perdita dei sistemi.

Il ripristino del servizio per le prime due situazioni può essere effettuato nell'ambito dell'edificio in cui è erogato il servizio in condizioni ordinarie, mentre per la terza situazione si ricorre a un sito alternativo di Disaster Recovery.

# 5. SICUREZZA FISICA

### 5.1.1 Edificio

L'edificio di via T. Taramelli, 26 in cui sono presenti tutti i sistemi di erogazione del servizio sono presenti dispositivi di sicurezza fisica controllati da appositi sistemi centrali situati in una sala di controllo presidiata 24 ore su 24.

#### 5.1.1.1 Sistemi antintrusione passivi ed attivi

Sul perimetro esterno e all'interno degli edifici sono presenti sistemi passivi antintrusione quali grate, vetrate antiproiettile, porte blindate e cancelli motorizzati e sistemi antintrusione attivi quali TVCC e VMD.

#### 5.1.1.2 Sistemi di rilevazione di situazioni anomale

Nella sala di controllo, presidiata 24 ore su 24, è presente un sistema di centralizzazione allarmi.

#### 5.1.1.3 Sistemi antincendio

Il sistema antincendio è stato realizzato secondo la norma UNI 9795. I sensori per la rilevazione incendio sono presenti in tutti i piani degli edifici.

#### 5.1.1.4 Sistemi di continuità di alimentazione elettrica

L'intero edificio è servito da gruppi di continuità statici e dinamici, e precisamente:

- UPS che garantiscono a tutti i sistemi connessi l'alimentazione necessaria sino all'intervento del gruppo elettrogeno e comunque, in caso d'indisponibilità di quest'ultimo, per almeno un'ora;
- gruppo elettrogeno (generatore di potenza con motore a gasolio) che assicura la continuità di alimentazione, se necessario anche per più giorni.

Un'ulteriore garanzia di continuità è realizzata prelevando l'alimentazione di media tensione da due diverse cabine.

### 5.1.2 Sale tecniche

Per le infrastrutture tecniche sono utilizzate due sale con caratteristiche speciali.

# 6. SICUREZZA LOGICA

## 6.1 Generazione e protezione delle chiavi di certificazione

La generazione e la protezione della chiave avviene tramite un sistema altamente affidabile. Actalis assume ogni precauzione finalizzata alla prevenzione della perdita, della compromissione o dell'utilizzo non autorizzato della suddetta chiave.

Il sistema di generazione della coppia di chiavi assicura:

- la rispondenza della coppia di chiavi ai requisiti degli algoritmi utilizzati
- l'equiprobabilità di generazione di tutte le coppie possibili, tramite un RNG di alta qualità;

L'attivazione della procedura di generazione può avvenire solo a seguito dell'identificazione di un soggetto abilitato.

### 6.1.1 Finalità e validità delle chiavi

Le chiavi di certificazione sono destinate alla firma dei certificati dei Titolari e delle liste di revoca.

La validità della coppia di chiavi di certificazione è indicato nel campo "validity" del certificato al netto di eventuali revoche e sospensioni.

### 6.1.2 Lunghezza delle chiavi

Per firmare i certificati dei clienti e le liste di CRL, Actalis usa chiavi RSA con un modulo di lunghezza a 2048 bit.

### 6.1.3 Distribuzione della chiave pubblica

La chiave pubblica di certificazione è disponibile tramite l'accesso al directory server via LDAP.

# 7. PROFILI DEI CERTIFICATI E DELLE CRL

## 7.1 Introduzione

Actalis ha generato tre chiavi di certificazione per la firma dei certificati di autenticazione CNS. In riferimento al punto 4.4.3 delle [Regole] i certificati delle chiavi di certificazione sono stati depositati presso il CNIPA per la pubblicazione in un'apposita sezione del sito web (www.cnipa.it). I Common Name dei certificati depositati sono i seguenti:

- Regione Lombardia – Certification Authority cittadini
- Actalis S.p.A. – Autenticazione CNS
- Actalis S.p.A. per certificati CNS

In generale i profili dei certificati generati sono conformi al profilo pubblicato sul sito web del CNIPA (www.cnipa.it) e presente nell'Allegato del [Decreto]. In particolare di seguito sono descritti i singoli profili dei suddetti certificati.

### 7.1.1 Regione Lombardia – Certification Authority cittadini: profilo dei certificati e della CRL

Di seguito sono descritti struttura e profilo dei certificati emessi dalla CA "Regione Lombardia – Certification Authority cittadini".

#### 7.1.1.1 Struttura del certificato

Il certificato emesso dalla CA "Regione Lombardia – Certification Authority cittadini" é conforme allo standard X.509v3. La sua struttura, espressa in ASN.1, é la seguente:

```
Certificate ::= SEQUENCE {
      tbsCertificate       TBSCertificate,
      signatureAlgorithm   AlgorithmIdentifier,
      signatureValue       BIT STRING  }

  TBSCertificate ::= SEQUENCE  {
      version         [0]  EXPLICIT Version DEFAULT v1,
      serialNumber         CertificateSerialNumber,
      signature            AlgorithmIdentifier,
      issuer               Name,
      validity             Validity,
      subject              Name,
      subjectPublicKeyInfo SubjectPublicKeyInfo,
      issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                           -- If present, version MUST be v2 or v3
      subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                           -- If present, version MUST be v2 or v3
      extensions      [3]  EXPLICIT Extensions OPTIONAL
                           -- If present, version MUST be v3
      }
```

### 7.1.2 Numero di versione

Il campo Version è valorizzato con il valore v3 definito nello standard X.509v3.

### 7.1.3 Numero di serie

Il campo SerialNumber è un identificativo univoco assegnato da Actalis che distingue ogni certificato emesso.

### 7.1.4 Validità del certificato

La data/ora prima della quale il certificato non è valido, è il valore del campo NotBefore, la data/ora oltre la quale il certificato scade è il valore del campo NotAfter.

Il periodo di validità è pertanto l'intervallo temporale tra i valori NotBefore e NotAfter. Il valore NotBefore è la data/ora di generazione del certificato, il valore di NotAfter è calcolata in base alla durata prevista dalla policy che è di sei anni.

### 7.1.5 Identificativo degli algoritmi di firma utilizzati

Per la firma dei certificati è usato l'algoritmo sha-1withRSAEncryption (OID= 1.2.840.113549.1.1.5).

### 7.1.6 Utilizzo della chiave

L'estensione key usage é marcata "critica" ed indica l'utilizzo previsto della chiave del Titolare in base ai valori presenti. Il valore indicato é digital Signature.

L'estensione Extended Key Usage indica ulteriori utilizzi della chiave del cliente. Il valore presente è TLS WWW Client Authentication (OID 1.3.6.1.5.5.7.3.2). L'estensione Extended Key Usage non è marcata critica.

### 7.1.7 Informazioni del Titolare (subject)

Le informazioni relative al titolare sono presenti nel campo Subject. L'attributo Common Name contiene:

- il codice fiscale del Titolare;
- l'identificativo univoco della CNS;
- il valore dell'hash dei dati personali del Titolare memorizzati nella CNS

L'attributo Country Name contiene il codice ISO3166 dello Stato in cui è residente il Titolare (per l'Italia IT).

L'attributo organizationalUnitName contiene Regione Lombardia.

### 7.1.8 Basic Constraint

L'estensione Basic Constraint indica se il titolare del certificato è una CA; il sottocampo Path Lenght Constraint il livello massimo del percorso di validazione cioè se possono esistere CA subordinate.

Il certificato emesso dalla CA "Regione Lombardia – Certification Authority cittadini" è destinato al Titolare (end entity) e non prevede CA subordinate.

### 7.1.9 Distribuzione CRL

Gli accessi alle CRL possono essere rappresentati da un URI LDAP e da un URI http e sono indicati nell'estensione CRL Distribution Point.

### 7.1.10 Accesso alle informazioni del Certificatore

L'estensione Authority Information Access indica le modalità di accesso alle informazioni ed ai servizi di validazione on line dei certificati. La modalità di accesso è rappresentato dall'URI OCSP http://ocsp.actalis.it/rl
.

### 7.1.11 Identificativo della policy

Il codice identificativo della policy è l'OID 1.3.159.6.1.3.2.10 presente nel campo Policy Identifier dell'estensione Certificate Policies.

### 7.1.12 Identificativo del Certificatore (Issuer)

L'identificativo dell'entità che emette i certificati è l'Issuer Distinguished Name rappresentato di seguito:

| Componente DN | Abbreviazione | Valore impiegato |
|---|---|---|
| Common Name | CN | Regione Lombardia – Certification Authority cittadini |
| Organization | O | Actalis S.p.A. |
| Organization Unit | OU | Servizi di certificazione |
| Country | C | IT |

### 7.1.13 Durata del periodo di validità e fingerprint

Il periodo di validità del certificato delle chiavi di certificazione è di dodici anni, dal 16 dicembre 2004 al 16 dicembre 2016. Per controllarne l'integrità il valore del fingerprint (algoritmo SHA1) è il seguente:

28CE 70C8 63A1 9FF3 B3C7 0CBC E59E 356F 205A CDA4

### 7.1.14 Profilo delle CRL

#### 7.1.14.1 Struttura della CRL

La CRL emessa da "Regione Lombardia – Certification Authority cittadini" è conforme agli standard X.509v3 ed RFC3280. La sua struttura, espressa in ASN.1, è rappresentata di seguito:

```
CertificateList  ::=  SEQUENCE  {
        tbsCertList          TBSCertList,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }
   TBSCertList  ::=  SEQUENCE  {
        version                 Version OPTIONAL,
                                  -- if present, MUST be v2
        signature               AlgorithmIdentifier,
        issuer                  Name,
        thisUpdate                Time,
        nextUpdate               Time OPTIONAL,
        revokedCertificates     SEQUENCE OF SEQUENCE  {
            userCertificate         CertificateSerialNumber,
            revocationDate           Time,
            crlEntryExtensions       Extensions OPTIONAL
                                     -- if present, MUST be v2
                                 }  OPTIONAL,
        crlExtensions            [0]  EXPLICIT Extensions OPTIONAL
                                     -- if present, MUST be v2
                                 }
```

#### 7.1.14.2 Campi base

##### 7.1.14.2.1 Numero di versione

Il valore del campo Version è impostato a 2.

##### 7.1.14.2.2 Algoritmo di firma

Per la firma dei certificati è usato l'algoritmo sha-1withRSAEncryption (OID= 1.2.840.113549.1.1.5).

##### 7.1.14.2.3 Entità emittente

L'identificativo dell'entità che emette le CRL è l'Issuer Distinguished Name di cui al parag. 7.1.12.

##### 7.1.14.2.4 Data/ora di emissione

La data e l'ora di emissione della CRL è presente nel campo thisUpdate.

##### 7.1.14.2.5 Data/ora prossima emissione

La data e l'ora di emissione della CRL successiva è presente nel campo nextUpdate.

##### 7.1.14.2.6 Frequenza pubblicazione CRL

La CRL è pubblicata ogni 12 ore. Non è prevista una nuova pubblicazione ad ogni revoca o sospensione, né la sua marcatura temporale immediata.

### 7.1.15 Actalis S.p.A. – Autenticazione CNS : profilo dei certificati e della CRL

Di seguito sono descritti struttura e profilo dei certificati emessi dalla CA "Actalis S.p.A. – Autenticazione CNS".

#### 7.1.15.1 Struttura del certificato

Il certificato emesso dalla CA "Actalis S.p.A. – Autenticazione CNS" é conforme allo standard X.509v3. La sua struttura, espressa in ASN.1, é la seguente:

```
Certificate ::= SEQUENCE {
      tbsCertificate      TBSCertificate,
      signatureAlgorithm   AlgorithmIdentifier,
      signatureValue      BIT STRING }

  TBSCertificate ::= SEQUENCE {
      version        [0]  EXPLICIT Version DEFAULT v1,
      serialNumber         CertificateSerialNumber,
      signature            AlgorithmIdentifier,
      issuer               Name,
      validity             Validity,
      subject              Name,
      subjectPublicKeyInfo SubjectPublicKeyInfo,
      issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                           -- If present, version MUST be v2 or v3
      subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                           -- If present, version MUST be v2 or v3
      extensions      [3]  EXPLICIT Extensions OPTIONAL
                           -- If present, version MUST be v3
      }
```

### 7.1.16 Numero di versione

Il campo Version è valorizzato con il valore v3 definito nello standard X.509v3.

### 7.1.17 Numero di serie

Il campo SerialNumber è un identificativo univoco assegnato da Actalis che distingue ogni certificato emesso.

### 7.1.18 Validità del certificato

La data/ora prima della quale il certificato non è valido, è il valore del campo NotBefore, la data/ora oltre la quale il certificato scade è il valore del campo NotAfter.

Il periodo di validità è pertanto l'intervallo temporale tra i valori NotBefore e NotAfter. Il valore NotBefore è la data/ora di generazione del certificato, il valore di NotAfter è calcolata in base alla durata prevista dalla policy che è di tre anni.

### 7.1.19 Identificativo degli algoritmi di firma utilizzati

Per la firma dei certificati è usato l'algoritmo sha-1withRSAEncryption (OID= 1.2.840.113549.1.1.5).

### 7.1.20 Utilizzo della chiave

L'estensione key usage é marcata "critica" ed indica l'utilizzo previsto della chiave del Titolare in base ai valori presenti. Il valore indicato é digital Signature.

L'estensione Extended Key Usage indica ulteriori utilizzi della chiave del cliente. Il valore presente è TLS WWW Client Authentication (OID 1.3.6.1.5.5.7.3.2). L'estensione Extended Key Usage non è marcata critica.

### 7.1.21 Informazioni del Titolare (subject)

Le informazioni relative al titolare sono presenti nel campo Subject. L'attributo Common Name contiene:

- il codice fiscale del Titolare;
- l'identificativo univoco della CNS;
- il valore dell'hash dei dati personali del Titolare memorizzati nella CNS

L'attributo Country Name contiene il codice ISO3166 dello Stato in cui è residente il Titolare (per l'Italia IT).
L'attributo Organization contiene il nome convenzionale del progetto.
L'attributo organizationalUnitName contiene la denominazione dell'Ente Emettitore.

### 7.1.22 Basic Constraint

L'estensione Basic Constraint indica se il titolare del certificato è una CA; il sottocampo Path Lenght Constraint il livello massimo del percorso di validazione cioè se possono esistere CA subordinate.

Il certificato emesso dalla CA "Actalis S.p.A. – Autenticazione CNS" è destinato al Titolare (end entity) e non prevede CA subordinate.

### 7.1.23 Distribuzione CRL

L'accesso alle CRL é rappresentato da un URI LDAP ed é indicato nell'estensione CRL Distribution Point.

### 7.1.24 Accesso alle informazioni del Certificatore

L'estensione Authority Information Access indica le modalità di accesso alle informazioni ed ai servizi di validazione on line dei certificati. La modalità di accesso è rappresentato dall'URI OCSP http://ocsp.actalis.it/CNS .

### 7.1.25 Identificativo della policy

Il codice identificativo della policy è l'OID 1.3.159.1.10.1 presente nel campo Policy Identifier dell'estensione Certificate Policies.
La conformità al profilo di cui all'Allegato del [Decreto] è rappresentata dall'OID 1.3.76.16.2.1.

### 7.1.26 Identificativo del Certificatore (Issuer)

L'identificativo dell'entità che emette i certificati è l'Issuer Distinguished Name rappresentato di seguito:

| **Componente DN** | **Abbreviazione** | **Valore impiegato** |
|---|---|---|
| Common Name | CN | Actalis S.p.A. – Autenticazione CNS |
| Organization | O | Actalis S.p.A. |
| Organization Unit | OU | Servizi di certificazione |
| Country | C | IT |

#### 7.1.26.1 Durata del periodo di validità e fingerprint

Il periodo di validità del certificato è di dodici anni, dal 31 marzo 2005 al 31 marzo 2017. Per controllarne l'integrità il valore del fingerprint (algoritmo SHA1) è il seguente:

853B 0A56 B724 CC17 F9BE 9E24 EEDB 528B B499 F94F

### 7.1.27 Profilo delle CRL

#### 7.1.27.1 Struttura della CRL

La CRL emessa da "Actalis S.p.A. – Autenticazione CNS" è conforme agli standard X.509v3 ed RFC3280. La sua struttura, espressa in ASN.1, è rappresentata di seguito:

```
CertificateList  ::=  SEQUENCE  {
        tbsCertList          TBSCertList,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }
   TBSCertList  ::=  SEQUENCE  {
        version                 Version OPTIONAL,
                                  -- if present, MUST be v2
        signature               AlgorithmIdentifier,
        issuer                  Name,
        thisUpdate                Time,
        nextUpdate                Time OPTIONAL,
        revokedCertificates     SEQUENCE OF SEQUENCE  {
            userCertificate         CertificateSerialNumber,
            revocationDate            Time,
            crlEntryExtensions        Extensions OPTIONAL
                                      -- if present, MUST be v2
                                }  OPTIONAL,
        crlExtensions             [0]  EXPLICIT Extensions OPTIONAL
                                      -- if present, MUST be v2
                              }
```

#### 7.1.27.2 Campi base

##### 7.1.27.2.1 Numero di versione

Il valore del campo Version è impostato a 2.

##### 7.1.27.2.2 Algoritmo di firma

Per la firma dei certificati è usato l'algoritmo sha-1withRSAEncryption (OID= 1.2.840.113549.1.1.5).

##### 7.1.27.2.3 Entità emittente

L'identificativo dell'entità che emette le CRL è l'Issuer Distinguished Name di cui al parag. 7.1.26.

##### 7.1.27.2.4 Data/ora di emissione

La data e l'ora di emissione della CRL è presente nel campo thisUpdate.

##### 7.1.27.2.5 Data/ora prossima emissione

La data e l'ora di emissione della CRL successiva è presente nel campo nextUpdate.

##### 7.1.27.2.6 Frequenza pubblicazione CRL

La CRL è pubblicata quotidianamente. Non è prevista una nuova pubblicazione ad ogni revoca o sospensione, né la sua marcatura temporale immediata.

### 7.1.28 Actalis CA per certificati CNS: profilo dei certificati e della CRL

Di seguito sono descritti struttura e profilo dei certificati emessi dalla CA "Actalis CA per certificati CNS".

#### 7.1.28.1 Struttura del certificato

Il certificato emesso dalla CA "Actalis CA per certificati CNS" é conforme allo standard X.509v3. La sua struttura, espressa in ASN.1, é la seguente:

```
Certificate ::= SEQUENCE {
      tbsCertificate      TBSCertificate,
      signatureAlgorithm   AlgorithmIdentifier,
      signatureValue      BIT STRING }

  TBSCertificate ::= SEQUENCE {
      version        [0]  EXPLICIT Version DEFAULT v1,
      serialNumber         CertificateSerialNumber,
      signature            AlgorithmIdentifier,
      issuer               Name,
      validity             Validity,
      subject              Name,
      subjectPublicKeyInfo SubjectPublicKeyInfo,
      issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                           -- If present, version MUST be v2 or v3
```

```
subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                -- If present, version MUST be v2 or v3
extensions      [3]  EXPLICIT Extensions OPTIONAL
                -- If present, version MUST be v3
}
```

### 7.1.29 Numero di versione

Il campo Version è valorizzato con il valore v3 definito nello standard X.509v3.

### 7.1.30 Numero di serie

Il campo SerialNumber è un identificativo univoco assegnato da Actalis che distingue ogni certificato emesso.

### 7.1.31 Validità del certificato

La data/ora prima della quale il certificato non è valido, è il valore del campo NotBefore, la data/ora oltre la quale il certificato scade è il valore del campo NotAfter.

Il periodo di validità è pertanto l'intervallo temporale tra i valori NotBefore e NotAfter. Il valore NotBefore è la data/ora di generazione del certificato, il valore di NotAfter è calcolata in base alla durata prevista dalla policy che è di sei anni.

### 7.1.32 Identificativo degli algoritmi di firma utilizzati

Per la firma dei certificati è usato l'algoritmo sha-1withRSAEncryption (OID= 1.2.840.113549.1.1.5).

### 7.1.33 Utilizzo della chiave

L'estensione key usage é marcata "critica" ed indica l'utilizzo previsto della chiave del Titolare in base ai valori presenti. Il valore indicato é digital Signature.

L'estensione Extended Key Usage indica ulteriori utilizzi della chiave del cliente. Il valore presente è TLS WWW Client Authentication (OID 1.3.6.1.5.5.7.3.2). L'estensione Extended Key Usage non è marcata critica.

### 7.1.34 Informazioni del Titolare (subject)

Le informazioni relative al titolare sono presenti nel campo Subject. L'attributo Common Name contiene:

- il codice fiscale del Titolare;
- l'identificativo univoco della CNS;
- il valore dell'hash dei dati personali del titolare memorizzati nella CNS

L'attributo Country Name contiene il codice ISO3166 dello Stato in cui è residente il Titolare (per l'Italia IT).
L'attributo Organization contiene il nome convenzionale del progetto.
L'attributo organizationalUnitName contiene la denominazione dell'Ente Emettitore.

### 7.1.35 Basic Constraint

L'estensione Basic Constraint indica se il titolare del certificato è una CA; il sottocampo Path Lenght Constraint il livello massimo del percorso di validazione cioè se possono esistere CA subordinate.

Il certificato emesso dalla CA "Actalis CA per certificati CNS" è destinato al Titolare (end entity) e non prevede CA subordinate.

### 7.1.36 Distribuzione CRL

Gli accessi alle CRL possono essere rappresentati da un URI LDAP e da un URI http e sono indicati nell'estensione CRL Distribution Point.

### 7.1.37 Accesso alle informazioni del Certificatore

L'estensione Authority Information Access indica le modalità di accesso alle informazioni ed ai servizi di validazione on line dei certificati. La modalità di accesso è rappresentato dall'URI OCSP https://onlinevalidation.actalis.it/CNS .

### 7.1.38 Identificativo della policy

Il codice identificativo della policy è l'OID 1.3.159.1.10.1 presente nel campo Policy Identifier dell'estensione Certificate Policies.

### 7.1.39 Identificativo del Certificatore (Issuer)

L'identificativo dell'entità che emette i certificati è l'Issuer Distinguished Name rappresentato di seguito:

| Componente DN | Abbreviazione | Valore impiegato |
|---|---|---|
| Common Name | CN | Actalis CA per certificati CNS |
| Organization | O | Actalis S.p.A. |
| Organization Unit | OU | Certification Service Provider |
| Country | C | IT |

#### 7.1.39.1 Durata del periodo di validità e fingerprint

Il periodo di validità del certificato è di dieci anni, dal 13 maggio 2004 al 13 maggio 2014. Per controllarne l'integrità il valore del fingerprint (algoritmo SHA1) è il seguente:

5821 D0ED 3E80 240C D6DD 5FF3 BEB1 74F2 C484 06C7

### 7.1.40 Profilo delle CRL

#### 7.1.40.1 Struttura della CRL

La CRL emessa da "Actalis CA per certificati CNS" è conforme agli standard X.509v3 ed RFC3280. La sua struttura, espressa in ASN.1, è rappresentata di seguito:

```
CertificateList  ::=  SEQUENCE  {
        tbsCertList          TBSCertList,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }
   TBSCertList  ::=  SEQUENCE  {
        version                 Version OPTIONAL,
                                  -- if present, MUST be v2
        signature               AlgorithmIdentifier,
        issuer                  Name,
        thisUpdate               Time,
        nextUpdate               Time OPTIONAL,
        revokedCertificates     SEQUENCE OF SEQUENCE  {
            userCertificate         CertificateSerialNumber,
            revocationDate           Time,
            crlEntryExtensions      Extensions OPTIONAL
```

```
                -- if present, MUST be v2
            } OPTIONAL,
    crlExtensions    [0] EXPLICIT Extensions OPTIONAL
                -- if present, MUST be v2
            }
```

#### 7.1.40.2 Campi base

##### 7.1.40.2.1 Numero di versione

Il valore del campo Version è impostato a 2.

##### 7.1.40.2.2 Algoritmo di firma

Per la firma dei certificati è usato l'algoritmo sha-1withRSAEncryption (OID= 1.2.840.113549.1.1.5).

##### 7.1.40.2.3 Entità emittente

L'identificativo dell'entità che emette le CRL è l'Issuer Distinguished Name di cui al parag. 7.1.39.

##### 7.1.40.2.4 Data/ora di emissione

La data e l'ora di emissione della CRL è presente nel campo thisUpdate.

##### 7.1.40.2.5 Data/ora prossima emissione

La data e l'ora di emissione della CRL successiva è presente nel campo nextUpdate.

##### 7.1.40.2.6 Frequenza pubblicazione CRL

La CRL è pubblicata quotidianamente. Ad ogni revoca o sospensione avviene la pubblicazione di una nuova versione.

# 8. ASSISTENZA E DISPONIBILITA' DEL SERVIZIO

## 8.1 Assistenza

Actalis eroga l'assistenza per la gestione del ciclo di vita del certificato all'Ente Emettitore che attiva un recapito telefonico costantemente attivo - rif. 2.2.7 delle [LG].

## 8.2 Requisiti di qualità

I processi operativi seguiti per l'erogazione del servizio descritto nella presente CP si basano su un sistema di qualità conforme allo standard ISO9001-2000.

## 8.3 Disponibilità del servizio

Gli orari di erogazione del servizio sono i seguenti:

| Tipo di servizio | Orario di disponibilità | Giorni di disponibilità | Eccezioni |
|---|---|---|---|
| Accesso al directory server | 24h | 7 giorni su 7 | Fermi per manutenzione o per cause di forza maggiore |
| Revoca e sospensione dei certificati | 24h | 7 giorni su 7 | Fermi per manutenzione o cause di forza maggiore |
| Registrazione, generazione e rinnovo certificati | Dalle 8.30 alle 17.30 (l'attività di registrazione dei dati è svolta dall'Ente Emettitore. Gli orari degli sportelli possono essere diversi da quelli indicati e sono resi noti dall'Ente Emettitore nel manuale operativo). | Giornate lavorative CCNL credito | Fermi per cause di forza maggiore |

# 9. GESTIONE CLAUSOLE

## 9.1 Procedura modifica clausole

Eventuali modifiche ed integrazioni alla presente CP saranno apportate esclusivamente da Actalis. Le modifiche ed integrazioni apportate saranno descritte nell'apposito capitolo "Storia delle modifiche".

Modifiche non sostanziali (ad esempio correzioni tipografiche) non comportano l'incremento del numero di versione del documento, modifiche sostanziali ovvero che possono avere impatti significativi sui Titolari comportano l'incremento del numero di versione del documento. In ogni caso la CP sarà pubblicata nelle modalità di cui al parag. 9.2.

## 9.2 Distribuzione della CP

La versione corrente della CP è pubblicata in formato Adobe Acrobat PDF sul sito web del servizio di certificazione https://portal.actalis.it.