Certificati Qualificati di Firma Remota per Clienti Bancari, Assicurativi e di Credito al Consumo

Integrazione del Manuale Operativo di Actalis

Redatto da:	Andrea Sassetti Direttore Servizi di CA	_____	_____ Data
Verificato da:	Giorgio Girelli Direttore Generale	_____	_____ Data
Approvato da:	Simone Braccagni 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 - 00 - 00 - 10 Integrazione MO

Codice Progetto Cod Sottoprog. N. Doc Versione

Distribuzione: PUBBLICA

Firmato digitalmente da
Andrea Sassetti

STORIA DELLE MODIFICHE APPORTATE

Data	Autore	Note
25/06/2014	Andrea Sassetti	Prima versione approvata

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

INDICE DELLE FIGURE

Non è stata trovata alcuna voce dell'indice delle figure.

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

SOMMARIO

1. GENERALITÀ 6
1.1 Scopo del documento 6
1.2 Riferimenti alle norme di legge 6
1.3 Convenzioni di lettura 7
1.4 Riferimenti agli standard 7
1.5 Definizioni e acronimi 8
2. INTRODUZIONE 9
2.1 Dati identificativi del certificatore (art. 40/3/a) 9
2.2 Versione del manuale operativo (art. 40/3/b) 9
2.3 Responsabile del manuale operativo (art. 40/3/c) 9
3. DISPOSIZIONI GENERALI 9
3.1 Obblighi del certificatore, del titolare e dei richiedenti la verifica delle firme (art. 40/3/d) 9
3.1.1 Obblighi e responsabilità del certificatore 9
3.1.2 Obblighi e responsabilità del titolare 9
3.1.3 Obblighi dei richiedenti la verifica delle firme 10
4. ASPETTI OPERATIVI 10
4.1 Note sull'organizzazione del personale (art. 34) 10
4.1.1 Registration Authority 10
4.2 Identificazione e registrazione degli utenti (art. 40/3/g) 11
4.2.1 Registrazione e attivazione on-line di un cliente 11
4.2.2 Registrazione e attivazione on-line di un cliente *prospect* 13
4.2.3 Inserimento di ruoli, limiti di valore e di uso 14
4.2.4 Verifiche svolte dal certificatore in fase di registrazione 14
4.2.5 Dispositivo di firma 14
4.2.5.1 Requisiti di sicurezza e caratteristiche del dispositivo di firma 14
4.2.5.2 Personalizzazione del dispositivo di firma 14
4.2.5.3 Conservazione e distribuzione del dispositivo di firma 14
4.3 Generazione delle chiavi (art. 40/3/h) 15
4.3.1 Modalità di generazione delle chiavi di certificazione 15
4.3.2 Modalità di generazione delle chiavi di marcatura temporale 15
4.3.3 Modalità di generazione delle chiavi di sottoscrizione degli utenti 15
4.4 Emissione dei certificati qualificati (art. 40/3/i) 15
4.4.1 Richiesta del certificato 16
4.4.2 Generazione del certificato 16
4.4.3 Policy supportate 16
4.4.4 Pubblicazione del certificato 16
4.5 Sospensione e revoca dei certificati (art. 36/3/l) 16
4.5.1 Circostanze per la sospensione o revoca del certificato 16
4.5.2 Richiesta di sospensione o revoca da parte del titolare 16
4.5.3 Richiesta di sospensione o revoca da parte del terzo interessato 17

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

4.5.4 Sospensione o revoca del certificato su iniziativa del certificatore 17
4.5.5 Completamento della sospensione o revoca del certificato 17
4.6 Sostituzione delle chiavi (art. 40/3/m) 17
4.7 Gestione del registro dei certificati (art. 40/3/n) 17
4.8 Accesso al registro dei certificati (art. 40/3/o) 17
4.9 Protezione dei dati personali (art. 40/3/q) 17
4.10 Apposizione e definizione del riferimento temporale (art. 40/3/p) 17
4.11 Utilizzo del sistema di verifica delle firme (art. 40/3/r) 17
4.12 Generazione della firma digitale (art.40/3/s) 17

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

1. GENERALITÀ

1.1 Scopo del documento

Questo documento è un'**Integrazione** del **Manuale Operativo** (in seguito citato con la sigla **MO**) del servizio di emissione e gestione di certificati qualificati erogato da Actalis S.p.A.

Mentre il MO vale per tutti i tipi di certificato qualificato emessi da Actalis, senza distinzione per clienti e/o ambiti di applicazione, nell'ambito del quale Actalis emette certificati qualificati per **firma remota**.

Come parte del MO di Actalis, questo documento è stato sottoposto all'approvazione dell'AGID ed è pubblicato sul sito web di Actalis.

Per tutto quanto non espressamente specificato nel presente documento, resta valido quanto descritto nel MO, al quale si rimanda (anche per i riferimenti normativi e tecnici eventualmente non riportati). Per agevolare la verifica incrociata, in questo documento è stata conservata, ove possibile, la stessa struttura e titolazione del MO.

1.2 Riferimenti alle norme di legge

[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.

[RTFD] Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici", pubblicato sulla Gazzetta Ufficiale n.129 del 6 giugno 2009.

[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).

[DLGS196] Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n.123 della G.U. n. 174, 29 luglio 2003.

[CAD] Decreto Legislativo 7 marzo 2005, n. 82: "Codice dell'Amministrazione Digitale" (CAD), pubblicato nella Gazzetta Ufficiale n. 112 del 16 maggio 2005, e s.m.i.

[DLB45/09] Deliberazione CNIPA n.45 del 21 maggio 2009, "Regole per il riconoscimento e la verifica del documento informatico", Pubblicato nella G.U. n. 282 (serie generale) del 3 dicembre 2009, come modificato dalla Determinazione DigitPA n.69/2010.

[DLGS235] Decreto Legislativo 30 dicembre 2010 , n. 235: "Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69", pubblicato in GU n. 6 del 10 gennaio 2010, Suppl. Ordinario n. 8.

[DLGS231] Decreto Legislativo 21 novembre 2007, n. 231: "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione e successive modificazioni e integrazioni".

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

1.3 Convenzioni di lettura

Nel resto del documento, l'azienda Actalis S.p.A., erogatrice del servizio di certificazione qui descritto e disciplinato, è indicata semplicemente con "Actalis".

Col termine "Manuale Operativo" (anche citato con la sigla MO) s'intende sempre riferirsi alla *versione corrente* del Manuale Operativo generale pubblicata sul portale web di Actalis all'indirizzo https://portal.actalis.it.

I riferimenti alla normativa e agli standard sono riportati tra parentesi quadre. In particolare, in alcuni dei titoli e sottotitoli di questo documento è riportato tra parentesi l'articolo, il comma e la lettera di riferimento delle [RTFD].

1.4 Riferimenti agli standard

[LDAP3] Wahl, M., Kille, S. and T. Howes, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[PKCS1] B. Kaliski, "PKCS#1: RSA Encryption - Version 1.5", Internet RFC 2313, March 1998.

[PKCS10] B. Kaliski, "PKCS#10: Certification Request Syntax - Version 1.5", Internet RFC 2314, March 1998.

[SHA1] ISO/IEC 10118-3:1998, "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions", May 1998.

[X500] ITU-T Recommendation X.500 (1997 E), "Information Technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services", August 1997.

[X509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[RFC 3161] Adams, C., Cain, P., Pinkas, D. and Zuccherato, R., "Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC 5816] Santesson, S., Pope, N., "ESSCertIDv2 Update for RFC 3161", RFC 5186, March 2010.

[RFC 5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[ETSI 280] ETSI TS 102 280 v 1.1.1 – "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", March 2004.

[ETSI 862] ETSI TS 101 862 v.1.3.2 – "Qualified Certificate profile", June 2004.

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

1.5 Definizioni e acronimi

Il seguente elenco riporta il significato di acronimi ed abbreviazioni usati in questo documento:

AgID	Agenzia per l'Italia Digitale (ex DigitPA)
CCIAA	Camera di Commercio, Industria, Artigianato ed Agricoltura
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CNS	Carta Nazionale dei Servizi
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DigitPA	Ex CNIPA
DN	Distinguished Name
DNS	Domain Name System
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
http	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IB	Internet Banking (della Banca/Assicurazione/Finanziaria)
IEN	Istituto Elettrotecnico Nazionale
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
OID	Object IDentifier
OTP	One-Time Password (codice dinamico)
PA	Pubblica Amministrazione
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Function
SSL	Secure Sockets Layer
TST	Time Stamping Token
URL	Uniform Resource Locator

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

2. INTRODUZIONE

2.1 Dati identificativi del certificatore (art. 40/3/a)

Il servizio di certificazione è erogato da Actalis S.p.A., identificata come riportato nel MO.

2.2 Versione del manuale operativo (art. 40/3/b)

Il presente documento è un'integrazione al Manuale Operativo relativo al servizio di certificazione di chiavi pubbliche erogato dalla Actalis ai sensi del [DLGS82] e successive correzioni ed integrazioni e delle [RTFD]. Il codice interno di questo documento è riportato sul frontespizio. La versione di riferimento del MO è quella pubblicata sul sito web di Actalis (si veda il par. 2.2 del MO).

2.3 Responsabile del manuale operativo (art. 40/3/c)

Il responsabile del presente documento è il medesimo del MO (cfr. il paragrafo 2.3 del MO).

3. DISPOSIZIONI GENERALI

3.1 Obblighi del certificatore, del titolare e dei richiedenti la verifica delle firme (art. 40/3/d)

3.1.1 Obblighi e responsabilità del certificatore

Gli obblighi e le responsabilità del certificatore rimangono invariate rispetto a quanto indicato nel corrispondente paragrafo del MO.

3.1.2 Obblighi e responsabilità del titolare

In generale, restano validi gli obblighi e responsabilità del titolare indicati nel MO.

Nel caso specifico, il titolare ha l'obbligo di:

1) richiedere il certificato con le modalità previste dal presente documento;
2) fornire all'ente certificatore, tramite i sistemi della Registration Authority (RA) , informazioni complete, esatte e veritiere al momento della richiesta del certificato;
3) conservare con la massima diligenza i codici (in particolare il PIN) utilizzati per l'attivazione della procedura di firma, al fine di preservarne l'integrità e la riservatezza (si rammenta che, in base alle norme vigenti, la firma si presume riconducibile al titolare del certificato salvo che quest'ultimo non fornisca prova contraria);
4) assicurare la custodia e l'uso esclusivamente personale del dispositivo utilizzato per la generazione del codice dinamico (OTP) necessario per la firma remota (si rammenta che, in base alle norme vigenti, la firma si presume riconducibile al titolare del certificato salvo che quest'ultimo non fornisca prova contraria);
5) utilizzare il certificato nel rispetto delle procedure descritte nel presente Manuale Operativo Integrativo e del contratto tra l'Ente Certificatore ed il Titolare stesso;

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

6) di non sottoscrivere digitalmente documenti elettronici avvalendosi di chiavi private per le quali sia stato revocato il certificato;
7) conservare con la massima diligenza il codice di sospensione di emergenza;
8) nel caso in cui intenda richiedere la revoca o sospensione del proprio certificato, seguire le modalità previste dal presente documento.

3.1.3 Obblighi dei richiedenti la verifica delle firme

Gli obblighi e le responsabilità di coloro che ricevono e verificano le firme rimangono invariati rispetto a quanto indicato nel corrispondente paragrafo del MO.

4. ASPETTI OPERATIVI

4.1 Note sull'organizzazione del personale (art. 34)

Il personale preposto all'erogazione e controllo del servizio è il medesimo che si occupa della gestione dei servizi di certificazione di Actalis le cui figure organizzative, definite e organizzate nel rispetto dell'art. 38 delle [RTFD], sono descritte nell'appositi paragrafo del MO.

4.1.1 Registration Authority

Per informazioni generali sulle Registration Authority (RA) si rimanda a quanto riportato nel relativo paragrafo del MO.

Nell'ambito del servizio di CA erogato, **le funzioni di registrazione sono svolte in conformità ad un apposito "Accordo di Delega" stipulato col certificatore.** Pertanto, la RA è responsabile nei confronti del certificatore della corretta identificazione dei titolari, ferme restando le responsabilità in capo al certificatore previste dalle vigenti norme di legge. Più precisamente,la RA deve (tra le altre cose):

- accertarsi che l'utente sia compiutamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei codici di attivazione della firma;
- accertarsi che l'utente sia compiutamente informato sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
- garantire l'accurata identificazione del richiedente il certificato, nonché la registrazione dello stesso, secondo le procedure previste nel MO e nel presente documento di integrazione;

Per ulteriori dettagli sui compiti ed obblighi della RA si rimanda al contratto di delega.

Il certificatore rende disponibili alla RA gli strumenti e le procedure che consentono di svolgere telematicamente le operazioni di registrazione degli utenti, richiesta e ottenimento del certificato, attivazione del servizio di firma remota, nonché sospensione, riattivazione e revoca dei certificati. A tali strumenti e procedure possono accedere solo gli operatori e processi software espressamente autorizzati dal certificatore.

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

4.2 Identificazione e registrazione degli utenti (art. 40/3/g)

Ai sensi delle norme vigenti, l'identificazione dell'utente richiedente - ai fini del rilascio del *primo certificato* - può avvenire nei seguenti modi:

- **De visu**: l'utente si presenta in persona presso la Banca che opera come RA (vedere il par. 4.1.1) ed esibisce un documento valido d'identificazione dell'utente ai sensi del [DPR445]; l'operatore di RA verifica il documento e ne trattiene una copia; per ulteriori dettagli si rimanda al MO.
- **A distanza** con una delle seguenti modalità:
  - in ottemperanza alle **norme antiriciclaggio** ai sensi del [DLGS231];
  - mediante **firma digitale** ai sensi del CAD; in questo caso l'utente si identifica telematicamente apponendo una firma mediante un certificato qualificato (valido) già in suo possesso, non necessariamente emesso da Actalis;
  - mediante identificazione fatta con l'ausilio di un sistema di videoconferenza (**identificazione via webcam**) e prevede che il Titolare venga riconosciuto tramite una sessione di videoconferenza fatta con un Operatore di Registrazione (OdR) qualificato, in conformità con quanto previsto e descritto nel MO Actalis (rif. § 4.2.1.4 *Altre modalità di identificazione a distanza*)
  - mediante **CNS** o **CIE**, ai sensi del CAD: l'utente si identifica telematicamente utilizzando una Carta Nazionale dei Servizi (CNS) oppure una Carta d'Identità Elettronica (CIE), e dunque attraverso un certificato di autenticazione (valido) già in suo possesso;
  - mediante un **sistema di autenticazione forte** (a due fattori), giudicato adeguatamente sicuro da Actalis e dall'AGID, che sia stato fornito all'utente previa identificazione con una delle altre modalità.

Più in generale di rimanda alle procedure di identificazione previste dal MO pubblicato dall'Ente Certificatore Actalis.

Di seguito si precisano le procedure di registrazione definite che riportano anche la metodologia di identificazione seguita.

4.2.1 Registrazione e attivazione on-line di un cliente

Si descrive di seguito, sinteticamente, la procedura di attivazione del servizio di firma remota per coloro che sono già clienti della Banca/Assicurazione/Finanziaria, cioè coloro che già hanno accesso a servizi on-line della Banca/Assicurazione/Finanziaria e sono dunque già dotati di un sistema di autenticazione forte basato su OTP. Tali utenti sono già stati identificati dalla Banca/Assicurazione/Finanziaria per l'attivazione dei servizi Bancari/Assicurativi per cui è necessario solamente provvedere all'acquisizione del consenso alla generazione del certificato di firma digitale.

Il metodo d'identificazione utilizzato, in questo caso, è quello a distanza basato su un sistema di autenticazione forte fornito all'utente e successivamente alla identificazione certa secondo una delle procedure previste dal presente documento e comunque riportate e descritte nel MO dell'Ente Certificatore Actalis.

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

In questo caso, la procedura si svolge interamente on-line, attraverso il portale web della Banca/Assicurazione/Finanziaria, ed è così articolata:

1) L'utente accede all'area clienti del portale della banca, autenticandosi con user-id e pass-word, e seleziona la funzione di richiesta del certificato di firma remota (nel corso del processo, l'utente specifica il valore desiderato per il proprio **PIN di firma**).
2) Il portale, previa accettazione da parte dell'utente delle condizioni contrattuali della CA, chiede all'utente di confermare la richiesta mediante inserimento di un **codice dinamico** (**OTP**). Tale codice OTP è generato dal dispositivo di autenticazione forte che la Banca/Assicurazione/Finanziaria ha già consegnato all'utente per l'accesso ai servizi e conferma di operazioni e disposizioni
3) Il portale richiede alla CA, mediante una transazione sicura, di creare il certificato di firma remota all'interno del HSM a favore dello specifico utente. Tale certificato qualificato avrà specifiche **limitazioni d'uso e d'utilizzo** relativamente allo scenario in questione (cfr. § 4.2.3)
4) La CA genera il certificato di firma remota all'interno dello HSM, invia all'utente il corrispon-dente codice di emergenza (ai sensi dell'Art 17 delle RTFD) e conferma al portale della Banca/Assicurazione/Finanziaria il completamento del processo.
5) Il portale della Banca/Assicurazione/Finanziaria sottopone all'utente il modulo di registrazione, da sottoscrivere digitalmente mediante il certificato di firma remota poc'anzi generato.
6) L'utente appone al contratto la propria firma remota; a tal fine deve inserire, oltre al PIN di firma, anche un codice dinamico (OTP), generato con il dispositivo di cui al punto 2)
7) Il portale della Banca/Assicurazione/Finanziaria completa la procedura di attivazione della firma remota per l'utente.

Si noti che la procedura richiede un'**autenticazione a due fattori** del'utente.

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

4.2.2 Registrazione e attivazione on-line di un cliente *prospect*

Si descrive di seguito, sinteticamente, la procedura di registrazione e attivazione del servizio di firma remota per i client *prospect* della Banca/Assicurazione/Finanziaria, ossia coloro che non sono ancora clienti ma sono interessati ad acquistare un servizio o prodotto offerto e per il quale è necessaria la firma remota. Tali utenti non sono mai stati identificati dalla Banca/Assicurazione/Finanziaria, in precedenza, ed è quindi necessario seguire una procedura di identificazione tra quelle previste nel presente documento (*ad esempio basata sulla normativa anti-riciclaggio [DLGS231] oppure tramite identificazione con webcam*) per poi provvedere all'acquisizione del consenso alla generazione del certificato di firma digitale.

In questo caso, la procedura si svolge interamente on-line, attraverso il portale web della Banca/Assicurazione/Finanziaria, ed è così articolata (si omettono i passaggi non essenziali ai fini del presente documento):

1) L'utente *prospect* accede all'area *pubblica* del portale della Banca/Assicurazione/Finanziaria e seleziona il prodotto desiderato tra quelli offerti; qui compila un modulo on-line fornendo i dati personali necessari (secondo il caso), incluso il proprio indirizzo di posta elettronica e il proprio n. di telefono cellulare.
2) Il portale della Banca/Assicurazione/Finanziaria crea un account provvisorio per l'utente e lo registra su un sistema di autenticazione forte basato sull'invio all'utente di codici dinamici (OTP), ad esempio, via SMS.
3) L'utente procede, sul portale della Banca/Assicurazione/Finanziaria, con la richiesta del certificato di firma remota (nel corso del processo, l'utente specifica il valore desiderato per il proprio **PIN di firma**).
4) Il portale, previa accettazione da parte dell'utente delle condizioni contrattuali della CA, chiede all'utente di confermare la richiesta mediante inserimento di un **codice dinamico** (**OTP**) che viene inviato all'utente stesso, ad esempio, via **SMS**.
5) Il portale richiede alla CA, mediante una transazione sicura, di creare il certificato di firma remota all'interno del HSM a favore dello specifico utente. Tale certificato qualificato avrà specifiche **limitazioni d'uso e d'utilizzo** relativamente allo scenario in questione (cfr. § 4.2.3)
6) La CA genera il certificato di firma remota all'interno dello HSM, invia all'utente il corrispondente codice di emergenza (ai sensi dell'Art 17 delle RTFD) e conferma al portale della Banca/Assicurazione/Finanziaria il completamento di questa fase del processo.
7) Il portale della Banca/Assicurazione/Finanziaria sottopone all'utente il modulo di registrazione e richiesta certificato, da sottoscrivere digitalmente mediante il certificato di firma remota poc'anzi generato.
8) L'utente appone al contratto la propria firma remota; a tal fine deve inserire, oltre al PIN di firma, anche un codice dinamico (OTP) che riceve, ad esempio, via SMS
9) Il portale della Banca/Assicurazione/Finanziaria chiede alla CA di **sospendere** il certificato di firma remota poc'anzi generato (con data di sospensione uguale alla data di creazione del certificato stesso).
10) La Banca/Assicurazione/Finanziaria avvia la procedura di identificazione dell'utente secondo le modalità previste nel presente documento oltre che nel MO dell'Ente Certificatore.

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

11) Al termine della procedura di identificazione di cui al passo precedente,
    a) se la procedura si è conclusa positivamente, la banca richiede alla CA di **riattivare** il certificato precedentemente sospeso e conclude il processo in modo conseguente, abilitando l'utente alla gestione della propria firma remota attraverso il portale della banca stessa;
    b) altrimenti, la banca richiede alla CA di **revocare** il certificato precedentemente sospeso e conclude il processo in modo conseguente.

Si noti che la procedura richiede un'**autenticazione a due fattori** dell'utente.

4.2.3 Inserimento di ruoli, limiti di valore e di uso

In considerazione del fatto che il certificato di firma remota sarà usato solamente nell'ambito dei rapporti tra il titolare e la Banca/Assicurazione/Finanziaria, e tenendo anche conto della modalità di identificazione e attivazione on-line, il certificato conterrà una specifica **limitazione d'uso**. Come previsto dalle regole tecniche emanate dall'AgID, tale limitazione sarà codificata all'interno del certificato in forma leggibile (human readable).

Una volta attivato il servizio di firma digitale remota, secondo le procedure descritte nei paragrafi precedenti, il titolare potrà disporre del proprio certificato esclusivamente tramite i servizi applicativi esposti dal portale della Banca/Assicurazione/Finanziaria. Pertanto, l'uso del certificato sarà limitato sia attraverso le limitazioni d'uso riportate nel certificato stesso, sia da misure tecniche che lo rendono fruibile esclusivamente attraverso i servizi on-line offerti dalla Banca/Assicurazione/Finanziaria.

4.2.4 Verifiche svolte dal certificatore in fase di registrazione

I dati di registrazione raccolti dalla Banca/Assicurazione/Finanziaria e forniti ad Actalis, insieme alla concomitante documentazione (es. modulo di richiesta certificato firmato dal richiedente, eventuali abilitazioni professionali, ecc.), sono considerati a priori *esatti e veritieri* in base all'Accordo di Delega (cfr. il paragrafo 4.1.1), pertanto il certificatore non svolge ulteriori verifiche su tali dati, se non "a campione" in fase di audit interno.

4.2.5 Dispositivo di firma

4.2.5.1 Requisiti di sicurezza e caratteristiche del dispositivo di firma

Resta valido quanto riportato nel MO, al quale si rimanda.

4.2.5.2 Personalizzazione del dispositivo di firma

Il Certificatore tiene comunque traccia di quali HSM (modello e numero di serie) sono utilizzati per gestire le chiavi di firma degli utenti.

4.2.5.3 Conservazione e distribuzione del dispositivo di firma

Il certificatore mantiene un inventario dei dispositivi di firma HSM da parte del Responsabile della registrazione o da un suo delegato ai senso dell'art. 33 delle [RTFD].

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

4.3 Generazione delle chiavi (art. 40/3/h)

4.3.1 Modalità di generazione delle chiavi di certificazione

Resta valido nella sua interezza quanto riportato nel MO, al quale si rimanda.

4.3.2 Modalità di generazione delle chiavi di marcatura temporale

Vale, in generale, quanto riportato nel MO.

4.3.3 Modalità di generazione delle chiavi di sottoscrizione degli utenti

Le chiavi di sottoscrizione degli utenti (ossia le chiavi RSA private di firma remota) sono generate dal Certificatore all'interno degli HSM descritti nella sezione 4.2.5.

Actalis utilizza, per la generazione delle credenziali di firma, il software approvato e certificato a tale scopo dal produttore il dispositivo sicuro.

Le chiavi sono generate a fronte di richieste opportunamente autenticate provenienti dal sottosistema di provisioning del sistema di firma remota.

4.4 Emissione dei certificati qualificati (art. 40/3/i)

L'emissione dei certificati qualificati avviene in seguito ad uno dei processi di registrazione descritti nel capitolo 4.2 del presente documento integrativo al MO.

Il richiedente interagisce col certificatore esclusivamente con modalità telematiche.

Prima dell'emissione del certificato, Actalis effettua una verifica sulla presenza di tutte le informazioni necessarie alla sua generazione, alcune delle quali sono raccolte e memorizzate in un apposito database ("database di registrazione", che devono essere almeno:

- nome e cognome,
- data di nascita,
- comune, provincia e stato estero di nascita,
- codice fiscale,
- indirizzo di residenza, eventualmente all'estero,
- indirizzo di posta elettronica,
- numero di cellulare,
- tipo e numero del documento d'identità o del documento di riconoscimento equipollente allegato.

Actalis inserirà nel certificato le limitazioni d'uso definite nel paragrafo "Inserimento di ruoli, limiti di valore e di uso".

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

4.4.1 Richiesta del certificato

La richiesta di certificato, in standard PKCS#10, viene generata su comando del sottosistema di provisioning del servizio di firma remota (cfr. il paragrafo precedente).

Per altri dettagli su questa fase del processo, si rimanda al MO.

4.4.2 Generazione del certificato

La generazione del certificato avviene, nel rispetto dell'art. 14 delle [RTFD], secondo la seguente procedura:

- Il sistema di firma remota invia alla CA la richiesta di certificato in formato PKCS#10;
- La CA verifica il corretto funzionamento della coppia di mediante validazione della firma contenuta nella struttura dati PKCS#10;
- se la verifica è superata, la CA genera il certificato col formato e con le informazioni previste;
- la generazione del certificato è attestata da un riferimento temporale;
- la generazione del certificato è registrata nel giornale di controllo;
- il certificato viene automaticamente installato nel sistema di firma remota.

Per altri dettagli su questa fase del processo, si rimanda al MO.

4.4.3 Policy supportate

In aggiunta a quanto descritto nel MO, i certificati potranno contenere anche ulteriori Policy OID se richiesto dalla Banca/Assicurazione/Finanziaria, purché nel rispetto delle norme vigenti.

4.4.4 Pubblicazione del certificato

Resta valido quanto riportato nel MO, al quale si rimanda.

4.5 Sospensione e revoca dei certificati (art. 36/3/l)

4.5.1 Circostanze per la sospensione o revoca del certificato

La revoca può avvenire in seguito a tutte le circostanze esposte nel MO, fatta eccezione per il caso di smarrimento/rottura del dispositivo sicuro (trattandosi nel caso specifico di HSM dei quali Actalis assicura la continuità di servizio).

Il Certificatore revoca o sospende il certificato di sua iniziativa, per richiesta del Titolare o della Banca/Assicurazione/Finanziaria, per esecuzione di un provvedimento dell'autorità.

4.5.2 Richiesta di sospensione o revoca da parte del titolare

Al termine della procedura di registrazione ed attivazione, in una delle modalità descritte nella sezione 4.2, vengono fornite all'utente le informazioni necessarie per richiedere la sospensione, riattivazione o revoca del proprio certificato (nonché altre operazioni di "gestione" della propria firma remota) attraverso il portale della Banca/Assicurazione/Finanziaria.

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

L'utente ha comunque la possibilità, in alternativa, di richiedere la sospensione, riattivazione o revoca del proprio certificato rivolgendosi direttamente al certificatore, con le modalità descritte nel MO.

4.5.3 Richiesta di sospensione o revoca da parte del terzo interessato

Resta valido quanto riportato nel MO, al quale si rimanda.

4.5.4 Sospensione o revoca del certificato su iniziativa del certificatore

Resta valido quanto riportato nel MO, al quale si rimanda.

4.5.5 Completamento della sospensione o revoca del certificato

Resta valido quanto riportato nel MO, al quale si rimanda.

4.6 Sostituzione delle chiavi (art. 40/3/m)

Resta valido quanto riportato nel MO, al quale si rimanda.

4.7 Gestione del registro dei certificati (art. 40/3/n)

Resta valido quanto riportato nel MO, al quale si rimanda.

4.8 Accesso al registro dei certificati (art. 40/3/o)

Resta valido quanto riportato nel MO, al quale si rimanda.

4.9 Protezione dei dati personali (art. 40/3/q)

Resta valido quanto riportato nel MO, al quale si rimanda.

4.10 Apposizione e definizione del riferimento temporale (art. 40/3/p)

Resta valido quanto riportato nel MO, al quale si rimanda.

4.11 Utilizzo del sistema di verifica delle firme (art. 40/3/r)

Actalis mette a disposizione molti strumenti per la verifica delle firma dei quali la Banca/Assicurazione/Finanziaria si può avvalere. Si rimanda al MO per quanto riguarda la descrizione degli strumenti e le loro modalità di utilizzo.

4.12 Generazione della firma digitale (art.40/3/s)

Nell'ambito del servizio di firma remota erogato da Actalis alla Banca/Assicurazione/Finanziaria, oggetto del presente documento, la generazione (ossia creazione) della firma digitale è prevista nella sola modalità remota, basata sull'impiego di HSM. A tal riguardo, vale in generale quanto riportato nel MO relativamente alla sola modalità remota.

In particolare, la richiesta di firma proveniente dagli applicativi della Banca/Assicurazione/Finanziaria in nome dell'utente (titolare del certificato) è sempre autenticata con **due fattori**:

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.

- un **PIN statico**, conosciuto solo del titolare;
- un **codice dinamico** (OTP: One-Time Password)

Modalità alternative o aggiuntive di autenticazione forte potranno essere implementate, a fronte di situazioni specifiche che lo giustifichino, col previo assenso e verifica del certificatore.

Inoltre, come specificato nel paragrafo "Inserimento di ruoli, limiti di valore e di uso", il certificato di firma remota sarà utilizzabile esclusivamente tramite i servizi esposti dal portale della Banca/Assicurazione/Finanziaria.

FINE DEL DOCUMENTO

Il contenuto del presente documento è di proprietà di Actalis S.p.A.
Tutti i diritti riservati.