BANCA D'ITALIA
EUROSISTEMA

SERVIZIO DI CERTIFICAZIONE A CHIAVE PUBBLICA PER I CERTIFICATI DI AUTENTICAZIONE E CRITTOGRAFIA

PUBLIC KEY INFRASTRUCTURE (PKI)

CERTIFICATION PRACTICE STATEMENT

CERTIFICATE POLICY

Versione 1.4.2 - 26/07/2023

1. CARATTERISTICHE GENERALI DEL SERVIZIO

1.1 Descrizione del servizio

La Banca d'Italia svolge il servizio di certificazione delle chiavi pubbliche per l'emissione di certificati di firma elettronica qualificata e per la gestione del loro ciclo di vita ai sensi delle disposizioni europee ("Regolamento (UE) n. 910/2014) e nazionali (previste dal Codice dell'Amministrazione Digitale).

La Banca emette inoltre certificati di autenticazione e crittografia (nel seguito ausiliari) non qualificati ai sensi del Regolamento (UE) 910/2014. I certificati di autenticazione consentono di accertare l'identità del soggetto che accede a basi dati o a sistemi elaborativi; quelli di crittografia permettono di preservare la riservatezza dei dati e delle informazioni scambiate o archiviate. Il certificato di crittografia è utilizzato per la firma elettronica delle mail.

I certificati sono emessi per i seguenti soggetti:

- dipendenti della Banca d'Italia per le finalità di lavoro per le quali sono rilasciati;
- rappresentanti di interlocutori istituzionali, in casi del tutto particolari, per esigenze connesse esclusivamente ai rapporti con la Banca d'Italia.

Il servizio si basa su una infrastruttura tecnico-organizzativa – Public Key Infrastructure (PKI) – costituita principalmente da due componenti: la Registration Authority (RA), che provvede all'identificazione dei richiedenti e alla registrazione delle istanze relative al ciclo di vita dei certificati; la Certification Authority (CA) che gestisce l'emissione, il ciclo di vita dei certificati e le liste di revoca e sospensione. Più in dettaglio, per una migliore comprensione di quanto segue, si precisa che l'infrastruttura di PKI della Banca d'Italia è costituita anche dalle seguenti componenti tecnologiche:

- copia di riferimento del Registro dei certificati (directory master), componente utilizzata dalla Certification Authority per la pubblicazione dei certificati e della lista di revoca e sospensione;
- copia operativa del Registro dei certificati (directory shadow), componente utilizzata dai titolari e dalle applicazioni per il download dei certificati e della lista di revoca e sospensione;
- sistema di registrazione (Registration Web Application), suite applicativa utilizzata per la gestione del flusso delle richieste (emissione, sospensione, rinnovo, riattivazione e revoca dei certificati dei titolari), accessibile solo dal personale abilitato;
- servizio Online Certificate Status Protocol (OCSP), per la verifica dello stato dei certificati.

I certificati sono generati presso l'Amministrazione Centrale della Banca d'Italia e la componente tecnologica è situata in locali adeguatamente protetti.

Il presente documento contiene le seguenti policy inerenti il servizio di certificazione a chiave pubblica per i certificati ausiliari:

- Certification Practice Statement (CPS), che definisce le procedure operative per l'emissione, la gestione e l'utilizzo dei certificati ausiliari. Nel documento

sono anche indicati gli obblighi e le responsabilità dei diversi attori e le misure di sicurezza fisiche e logiche previste dal servizio di certificazione;
- Certificate Policy (CP), che specificano i requisiti e le regole per l'utilizzo dei certificati ausiliari nei diversi contesti.

Il documento riporta i termini e le condizioni relativi all'utilizzo dei certificati ed è rivolto ai soggetti che entrano in relazione con la Banca d'Italia in qualità di titolari dei certificati, terzi interessati (cfr. glossario) o soggetti che richiedono la verifica di un certificato rilasciato dalla Banca d'Italia. Tali termini e condizioni diventano effettivi dal momento in cui un soggetto diviene titolare di un certificato di autenticazione o crittografia emesso dalla Banca d'Italia.

Il documento è redatto secondo lo standard Internet Engineering Task Force (IETF) RFC 3647.

1.2 Identificativo del documento

Questo documento è consultabile, in italiano e inglese, al seguente indirizzo Internet http://www.bancaditalia.it/firmadigitale e contiene la versione 1.4.1 del 07/06/2023:
- del CPS identificato dall'Object Identifier Number (O.I.D.) 1.3.76.38.1.3.2;
- delle CP identificate dai rispettivi OID:
  - 1.3.76.38.1.3.2.1[1] per i certificati di autenticazione;
  - 1.3.76.38.1.3.2.2 per i certificati di crittografia, usati anche per la firma elettronica delle mail.

Le specifiche regole che riguardano il certificato di autenticazione o crittografia sono identificabili nel seguito come:
- [1.3.76.38.1.3.2.1 AUTENTICAZIONE];
- [1.3.76.38.1.3.2.2 CRITTOGRAFIA].

Laddove non specificato, la presente policy di riferimento è valida per tutti i profili dei certificati emessi.

La versione e la data di ultima revisione del documento sono indicate nel frontespizio. La versione è identificabile in calce a ogni pagina.

1.3 Ruoli della PKI

Nel capitolo 9 sono dettagliati gli obblighi e le responsabilità dei diversi attori coinvolti nel servizio di certificazione o che usano i certificati.

1.3.1 Autorità di certificazione (Certification Authority - CA)

Il ruolo di CA è svolto in modalità accentrata dalla Banca d'Italia attraverso una componente tecnologica denominata "Servizi di certificazione ausiliari"[2].

[1] Gli OID sono stati registrati presso l'autorità nazionale competente (UNINFO).
[2] La CA della Banca d'Italia è strutturata su un solo livello.

Il responsabile del servizio di certificazione è la Banca d'Italia; l'assolvimento dei relativi compiti è attribuito al Servizio Sviluppo informatico.

Dati identificativi del Certificatore

Denominazione	Banca d'Italia
Indirizzo della sede legale	Via Nazionale, 91 – 00184 ROMA
Legale Rappresentante	Governatore pro tempore
PEC	svi@pec.bancaditalia.it
e-mail	pki@bancaditalia.it
Indirizzo Internet	www.bancaditalia.it
Telefono	06/47921
Help Desk[3] per le richieste di sospensione d'urgenza	06/47929361

Il certificato della CA ha durata ventennale ed è consultabile, con la relativa impronta, sul sito della Banca d'Italia http://www.bancaditalia.it/firmadigitale. I dettagli del profilo del certificato sono indicati nel capitolo 7.

1.3.2 Autorità di registrazione (Registration Authorithy - RA)

Il ruolo di Registration Authority (RA) è svolto in modalità decentrata dalla Banca d'Italia - tramite le proprie Filiali e le Strutture dell'Amministrazione Centrale - che svolgono le seguenti attività:

- accoglimento e validazione delle richieste di emissione e gestione dei certificati;
- registrazione del soggetto richiedente;
- autorizzazione all'emissione del certificato richiesto;
- gestione delle richieste inerenti il ciclo di vita dei certificati.

Nel seguito del documento, ogni riferimento alla Registration Authority deve essere inteso secondo il seguente schema.

Strutture della Banca d'Italia che agiscono come RA	Soggetto che effettua la richiesta inerente il certificato
Unità con compiti segretariali delle Filiali	Con riferimento al luogo in cui il richiedente svolge la propria attività lavorativa: - dipendenti; - in casi del tutto particolari, per rappresentanti di interlocutori istituzionali per esigenze connesse esclusivamente ai rapporti con la Banca d'Italia
Unità con compiti segretariali dell'Amministrazione Centrale	Con riferimento al luogo in cui il richiedente svolge la propria attività lavorativa: - dipendenti; - in casi del tutto particolari, per rappresentanti di interlocutori

[3] Cfr. paragrafo 4.9.

	istituzionali per esigenze connesse esclusivamente ai rapporti con la Banca d'Italia

1.3.3 Titolari e terzi interessati

Con il termine "titolare" si intende, nel seguito, il soggetto a cui è stato rilasciato dalla Banca d'Italia un certificato.

Per terzo interessato si intende un interlocutore istituzionale (ente o persona giuridica) che può chiedere l'emissione di un certificato in favore di un altro soggetto (titolare), da esso designato e a lui legato da un rapporto di rappresentanza o di lavoro. Tale legame deve essere motivato e attestato in sede di richiesta del certificato.

I titolari dei certificati sono i dipendenti della Banca d'Italia per le finalità di lavoro per le quali sono rilasciati e, in casi del tutto particolari, rappresentanti di interlocutori istituzionali che utilizzano i certificati esclusivamente nei rapporti con la Banca d'Italia.

Non è prevista la possibilità di rilascio di un certificato ad una persona giuridica.

1.3.4 Richiedenti la verifica di un certificato

I richiedenti la verifica di un certificato sono tutti i soggetti (persone fisiche o giuridiche) che, partecipando ad una transazione telematica, fanno affidamento sulle informazioni contenute nel certificato digitale emesso dalla Banca d'Italia.

1.3.5 Altri partecipanti

Non ci sono altri partecipanti oltre a quelli presentati nei paragrafi precedenti.

1.4 Uso dei certificati

I certificati sono utilizzati per le finalità di lavoro per le quali sono rilasciati e per le esigenze connesse esclusivamente ai rapporti con la Banca d'Italia.

Le coppie di chiavi generate dal servizio di certificazione della Banca d'Italia appartengono alle seguenti tipologie:

1. chiavi di certificazione (nel seguito chiavi di CA o di root CA), cioè le chiavi utilizzate dalla Banca d'Italia per firmare elettronicamente i certificati dei titolari e la lista di revoca e sospensione dei certificati;
2. chiavi del titolare, vale a dire le chiavi attribuite dalla Banca d'Italia a persone fisiche, per la crittografia di documenti e email e la firma elettronica di queste ultime e l'autenticazione.

Ogni coppia di chiavi è utilizzabile unicamente per la tipologia di operazione per la quale è stata generata. L'indicazione della tipologia di operazione che è possibile effettuare con la coppia di chiavi è riportata nel relativo certificato.

È esplicitamente fatto divieto di usare i certificati dei titolari:

- come certificati di una CA;
- per usi differenti da quelli indicati nella richiesta;
- oltre il periodo di validità;
- dopo la revoca da parte della CA;
- per finalità diverse da quelle previste nei limiti d'uso.

1.5 Gestione del CPS e delle CP

La Banca d'Italia cura la redazione e la pubblicazione del presente documento; il documento è revisionato periodicamente e aggiornato in caso di cambiamenti significativi dell'infrastruttura o della normativa di riferimento.

È responsabile del presente documento:

Nome	Stefano
Cognome	Massi
PEC	svi@pec.bancaditalia.it
e-mail	stefano.massi@bancaditalia.it

Il responsabile del documento è stato formalmente nominato dalla Banca d'Italia.

L'elenco delle persone responsabili per i diversi ruoli stabiliti nella PKI è riportato in un documento formale[4], di cui è stata inviata copia all'Agenzia per l'Italia Digitale (AgID).

I ruoli sono stati definiti in modo tale da garantire il principio di *separation of duties* (es. Responsabile della sicurezza logica e dell'amministrazione della componente tecnologica, Responsabile della conduzione tecnica dei sistemi, Responsabile dei servizi logistici, Responsabile delle verifiche e delle ispezioni, ecc.).

Eventuali modifiche al documento possono essere proposte da ciascuno dei suddetti Responsabili e approvate dal Responsabile del documento stesso.

Il documento viene quindi aggiornato con un nuovo numero di versione e inviato al Servizio Comunicazione per la pubblicazione sul sito istituzionale. Le modifiche possono interessare l'intero documento o parti di esso e sono indicate da nuovi numeri assegnati alle versioni modificate[5].

La Banca d'Italia pubblica l'ultima versione del documento sul proprio sito Internet all'indirizzo http://www.bancaditalia.it/firmadigitale.

1.6 Definizioni, acronimi e riferimenti normativi

Glossario

Ai fini del presente documento si applicano le definizioni contenute nel Regolamento UE 910/2014 (eIDAS) e nel Decreto Legislativo 7 marzo 2005, n.82 (CAD), e successive modifiche e integrazioni.

[4] "Relazione sull'organizzazione dell'infrastruttura PKI", prot. n. 0978987/23 del 01/06/2023.

[5] In particolare, le nuove versioni sono indicate con un numero intero seguito da un decimale che è zero. Modifiche di minore entità sono segnalate attraverso un numero decimale maggiore di zero.

Certificatore	Un prestatore di servizi fiduciari che emette certificati.
Certificato ausiliario	Un'attestazione elettronica che associa i dati elettronici, necessari per l'autenticazione informatica o la crittografia, ad una persona fisica confermandone almeno il nome o lo pseudonimo.
Chiave privata	Elemento della coppia di chiavi asimmetriche destinato a essere utilizzato soltanto dal titolare.
Chiave pubblica	Elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico.
Chiavi asimmetriche	Coppia di chiavi asimmetriche, una privata e una pubblica, correlate tra loro, da utilizzarsi nell'ambito di sistemi di firma, cifratura e autenticazione.
Chiavi di certificazione	Coppia di chiavi utilizzabili dal prestatore di servizi per la generazione e verifica delle firme apposte o associate ai certificati qualificati, per la sottoscrizione delle informazioni sullo stato di validità dei certificati - la lista dei certificati revocati e sospesi (CRL).
Crittografia asimmetrica	Tipologia di operazione matematica mediante la quale, utilizzando apposite chiavi tra loro differenti e specifici algoritmi, dal risultato della cifratura di un file ottenuta con una chiave è possibile risalire al file originario unicamente applicando a tale risultato lo stesso algoritmo con l'utilizzo dell'altra chiave.
CRL (Certificate Revocation List)	Cfr. Lista dei certificati revocati.
Firma digitale	Un particolare tipo di firma qualificata basata su un su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.
Firma elettronica qualificata	Una firma elettronica qualificata ai sensi del Regolamento eIDAS.
Firmatario	Una persona fisica che crea una firma elettronica.
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
HSM (Hardware Security Module)	Insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.

Impronta di una sequenza di simboli binari (bit)	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
Infrastruttura a chiavi pubbliche (PKI)	Insieme di macchine, software, persone e regole che consentono l'emissione e la gestione dei certificati elettronici e dei relativi dispositivi di firma.
Lista dei certificati revocati (CRL)	Elenco elettronico dei certificati che sono stati revocati dal certificatore che li ha emessi. Tale elenco - che costituisce parte integrante del Registro dei certificati - è firmato, tenuto e aggiornato dal prestatore di servizi.
Marca temporale	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.
OCSP (online certificate status protocol)	Protocollo di rete utilizzato per verificare la validità dei certificati elettronici.
Pass-phrase	Sequenza di caratteri alfanumerici e di punteggiatura, conosciuta solo dal titolare del certificato, il quale deve comunicarla al servizio di Help desk per chiedere la sospensione d'urgenza del certificato in caso di smarrimento, furto o compromissione della sicurezza della smartcard.
PIN (Personal Identification Number)	Codice di identificazione personale.
PKI (Public Key Infrastructure)	Cfr. Infrastruttura a chiavi pubbliche.
Prestatore di servizi fiduciari	Una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato.
Prestatore di servizi fiduciari qualificato	Un prestatore di servizi fiduciari qualificato ai sensi dell'eIDAS.
PUK (Pin Unlock Key)	Codice di sblocco del PIN.
Registrazione	Attività di acquisizione, autenticazione e archiviazione dei dati dei richiedenti i certificati. La registrazione costituisce condizione necessaria per l'accoglimento della domanda di certificazione.
Registro dei certificati	La combinazione di uno o più archivi informatici, tenuto dal certificatore, contenente tutti i certificati emessi.
Revoca del certificato	Operazione con la quale il certificatore annulla la validità del certificato da un dato momento in poi.
Richiedente	Persona fisica che, anche su designazione del terzo interessato, chiede al certificatore l'attribuzione di una coppia di chiavi (pubblica e privata) e il relativo certificato; una volta emesso il certificato, il richiedente ne diviene titolare.
Riferimento temporale	Evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
Servizio fiduciario	Un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

	a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.
Servizio fiduciario qualificato	Un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel Regolamento eIDAS.
Sistema di registrazione (Registration Web Application)	Suite applicativa utilizzata per la gestione del flusso delle richieste (emissione, sospensione, rinnovo, riattivazione e revoca dei certificati dei titolari), accessibile solo dal personale abilitato.
Smartcard	Dispositivo di sicurezza sul quale risiedono la coppia di chiavi (pubblica e privata) e il certificato del titolare.
Sospensione del certificato	Operazione con cui il prestatore di servizi sospende la validità del certificato per un periodo di tempo.
Sottoscrittore	Persona fisica o giuridica che deve rispettare gli obblighi per la sottoscrizione previsti dal certificatore.
Terzo interessato	Ente o persona giuridica che chiede l'emissione di un certificato in favore di un altro soggetto (titolare), da esso designato, a lui legato da un rapporto di rappresentanza o di lavoro.
Titolare	La persona fisica (cfr. firmatario) che ha richiesto e ottenuto dal certificatore, anche su designazione del terzo interessato, l'attribuzione di una coppia di chiavi (pubblica e privata) e quindi il relativo certificato.
Token USB	Dispositivo di sicurezza sul quale risiedono la coppia di chiavi (pubblica e privata) e il certificato del titolare.
Validazione temporale	Risultato della procedura informatica con cui si attribuisce ad uno o più documenti informatici un riferimento temporale opponibile ai terzi.

Acronimi

AgID	Agenzia per l'Italia Digitale – organismo di vigilanza nazionale dei prestatori di servizi fiduciari qualificati
CA	Certification Authority
CRL	Certificate Revocation List
DM	Directory Master
DS	Directory Shadow
HSM	Hardware Security Module

http	Hyper Text Transfer Protocol
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
OCSP	On-line Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
SAN	Storage Area Network

Riferimenti normativi

Legge 59/1997 art. 15, comma 2	Legge 15 marzo 1997, n. 59 "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa" pubblicata nel S.O. 56/L alla Gazzetta Ufficiale n. 63 del 17 marzo 1997
D.Lgs. 196/2003	Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali e successive modifiche e integrazioni
D. Lgs. 82/2005 "Codice dell'amministrazione digitale"	Decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni Pubblicato nel S.O. N. 93/L alla Gazzetta Ufficiale n. 112 del 16 maggio 2005[6] e successive modifiche e integrazioni
Determinazione AgID 121/2019 e successive modifiche e integrazioni	Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate
DPCM 19.07.2012	DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 19 luglio 2012 Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma
DPCM 22.02.2013	DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera *b)*, 35, comma 2, 36, comma 2, e 71. Pubblicato nella Gazzetta Ufficiale del 21 maggio 2013 n. 117
Regolamento eIDAS	Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS) e che abroga la direttiva 1999/93/CE Pubblicato Gazzetta ufficiale dell'Unione Europea del 28 agosto 2014 L. 257

[6] Il "Codice", in vigore dal 1^ gennaio 2006, ha abrogato le previsioni in materia di firme elettroniche, documenti informatici, carta d'identità elettronica e sviluppo dei sistemi informativi delle PP.AA. contenute nel D.P.R. 28.12.2000, n. 445.

Regolamento GDPR	Regolamento (UE) n. 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE Pubblicato Gazzetta ufficiale dell'Unione Europea del 4 maggio 2016 L. 119

2 RESPONSABILITÀ DELLE PUBBLICAZIONI E DEGLI ARCHIVI ONLINE

La Banca d'Italia gestisce ed è responsabile del contenuto e delle modalità di pubblicazione relative allo stato dei certificati, alle policy di riferimento e alle procedure che regolano il servizio di certificazione.

All'indirizzo http://www.bancaditalia.it/firmadigitale sono disponibili:

- il certificato della CA;
- l'impronta del certificato della CA;
- il CPS/CP di cui al presente documento;
- il manuale di utilizzo del software di crittografia.

La Banca d'Italia gestisce e rende pubblica la lista dei certificati revocati e sospesi che è aggiornata a seguito ad ogni richiesta di revoca o sospensione. La revoca avviene entro un'ora dall'identificazione del richiedente e dalla verifica dell'autenticità della richiesta. La pubblicazione della lista avviene al massimo ogni 24 ore ed è consultabile gratuitamente attraverso i seguenti indirizzi Internet:

- OCSP - http://ocsp.certificazione.bancaditalia.it/ocsp
- LDAP - ldap://ldap.certificazione.bancaditalia.it/cn=Banca%20d'Italia%20CA%20ausiliaria,ou=Servizi%20di%20certificazione%20ausiliari,o=Banca%20d'Italia/00950501007,l=Roma,c=IT?certificateRevocationListc=IT
- HTTP - http://www.certificazione.bancaditalia.it/crl/crlaus.crl

L'accesso agli archivi per la pubblicazione degli aggiornamenti ai citati documenti è possibile solo da personale autorizzato a operare sull'infrastruttura PKI della Banca d'Italia, da postazioni abilitate.

3 IDENTIFICAZIONE E AUTENTICAZIONE DEL TITOLARE

La Banca d'Italia, in qualità di Registration Authority, identifica la persona che effettua la richiesta di un certificato e si accerta dell'autenticità della richiesta come descritto nei paragrafi seguenti.

L'identificazione e l'autenticazione del titolare del certificato avviene all'atto della richiesta di prima emissione.

3.1 Identificazione univoca del certificato e del titolare

I certificati digitali emessi dalla Banca d'Italia sono identificati in maniera univoca da un codice seriale; i titolari dei certificati sono identificati da un codice identificativo univoco (I.U.T.).

I certificati contengono il Distinguished Name (DN) della CA e del titolare del certificato, rispettivamente nei campi issuer name e subject name.
La Banca d'Italia garantisce che i Distinguished Name dei titolari siano unici in quanto in essi è inserito anche il codice fiscale.
Non è previsto l'uso di pseudonimi e non è ammesso l'utilizzo di un DN privo di significato poiché esso identifica i soggetti a cui si applicano le regole previste in questo documento.

Le informazioni presenti nei certificati sono codificate in conformità alle raccomandazioni ITU-T X.509.

3.2 Accertamento iniziale dell'identità del titolare

I dipendenti sono già identificati e autenticati dalla Banca d'Italia che detiene tutti i documenti ad essi relativi (fascicolo personale) a seguito della loro assunzione. Fermo il rispetto delle norme di legge, la procedura di identificazione e autenticazione per i dipendenti avviene sulla base della conoscenza personale e può quindi subire talune variazioni rispetto a quella per i soggetti esterni.
Per essi inoltre non è ovviamente prevista la designazione da terze parti come per i soggetti esterni.
Ciò detto, valgono per i dipendenti – a parità di altre condizioni – le regole di seguito descritte per i soggetti esterni.

I soggetti esterni alla Banca d'Italia che richiedono l'emissione di certificati devono essere designati dagli enti (terzi interessati) per i quali operano in virtù di un rapporto di lavoro o di rappresentanza. Il terzo interessato invia alla RA competente una nota di designazione con in allegato la richiesta del titolare (cfr. paragrafo 4.1).
La fase di identificazione e autenticazione si completa all'atto della consegna dei certificati. In tale circostanza, la RA invita il titolare dei certificati a recarsi presso la RA stessa al fine di autenticarne l'identità sulla base di uno dei seguenti documenti, in corso di validità:

1) il passaporto;
2) la patente di guida;
3) la patente nautica;
4) il libretto di pensione;
5) il patentino di abilitazione alla conduzione di impianti termici;
6) il porto d'armi;
7) le tessere di riconoscimento, purché munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato.

Questi documenti sono previsti dall'AgID in conformità con le disposizioni della legge italiana (Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 art. 35).

Le informazioni fornite sono trattate mediante procedure informatiche con logiche strettamente correlate alle finalità sopra descritte e con l'impiego di misure di sicurezza idonee a garantire la riservatezza dei dati personali nonché ad evitare l'indebito accesso ai dati ai sensi della normativa europea e nazionale in materia di protezione dei dati personali.

3.3 Identificazione e autenticazione del titolare in caso di richieste di rinnovo di un certificato

I certificati emessi dalla Banca sono validi per 5 anni.

Il rinnovo di un certificato avviene quando esso è prossimo alla scadenza ed equivale al rilascio di un certificato che attesta una nuova chiave pubblica.

I dipendenti della Banca d'Italia non devono espressamente chiedere il rinnovo di un certificato in quanto il titolare, dopo aver ricevuto una comunicazione automatica in prossimità della scadenza dei certificati, compie l'operazione in autonomia in modalità decentrata, previa identificazione e autenticazione da parte di un'applicazione specificamente predisposta per compiere tale operazione. Questa ultima, richiede l'autenticazione del titolare e verifica che la smartcard sia associata all'utente autenticato.

I soggetti esterni (terzi interessati), in prossimità della scadenza dei certificati, ricevono una comunicazione dalla Banca d'Italia con la quale si richiede se, con riferimento a ciascun titolare, sia necessaria l'emissione di un certificato uguale a quello in scadenza. In caso di risposta affermativa, il terzo interessato invia alla RA competente una nota di designazione con in allegato la richiesta del titolare (cfr. paragrafo 4.7).
La fase di identificazione e autenticazione si completa, come descritto al paragrafo 3.2, alla consegna della smartcard, previa esibizione di un valido documento d'identità. La RA provvede contestualmente a ritirare la smartcard contenente i certificati in scadenza e la rende inutilizzabile mediante taglio del microcircuito.

La RA verifica l'autenticità della richiesta sulla base dei dati presentati in fase di registrazione, dello stato dei certificati e delle evidenze in suo possesso; in particolare, verifica i seguenti elementi contenuti nella richiesta:

- generalità del titolare del certificato del quale si richiede il rinnovo;
- pregressa designazione del titolare da parte del terzo interessato.

3.4 Identificazione e autenticazione del titolare in caso di richieste di revoca

Le richieste di revoca per i dipendenti (identificati e autenticati dalla RA di riferimento come nel paragrafo 3.2) possono essere presentate dal titolare o dalla Struttura presso la quale presta servizio.

Le richieste di revoca per i soggetti esterni (identificati e autenticati dalla RA di riferimento come nel paragrafo 3.2) possono essere presentate dal titolare o dal terzo interessato.

La RA verifica l'autenticità della richiesta sulla base dei dati presentati in fase di registrazione, dello stato dei certificati e delle evidenze in suo possesso; in particolare, verifica i seguenti elementi contenuti nella richiesta:

- generalità del titolare del certificato del quale si richiede il rinnovo;
- pregressa designazione del titolare da parte del terzo interessato.

4 CICLO DI VITA DEI CERTIFICATI

Il servizio di certificazione svolto dalla Banca d'Italia riguarda l'emissione dei certificati e il loro rinnovo alla scadenza, la sospensione e la revoca degli stessi, la tenuta e la pubblicazione della lista dei certificati revocati e sospesi per la verifica di validità dei certificati medesimi.

Le richieste di emissione sono gestite dalla Banca d'Italia mediante risorse umane, assetti tecnologici e procedure operative definiti nel presente documento.

La RA si avvale per la registrazione delle richieste di una applicazione web accessibile esclusivamente dalla rete interna della Banca d'Italia e solo da operatori specificamente autorizzati.

Tutti i moduli per le richieste inerenti il ciclo di vita dei certificati sono disponibili sul sito www.bancaditalia.it/firmadigitale.

4.1 Richiesta di certificati

Le persone fisiche che possono presentare alla RA richieste per il rilascio dei certificati sono quelli indicati al paragrafo 1.3.3.

Il richiedente redige e sottoscrive, con apposito modulo, l'istanza che deve:

a) indicare i dati anagrafici, il codice fiscale, il numero di telefono (di rete fissa o cellulare), l'indirizzo di posta elettronica del richiedente;
b) contenere l'attestazione da parte del richiedente circa l'attendibilità delle informazioni fornite e l'impegno a comunicare ogni variazione delle stesse;
c) essere corredata di una copia di un valido documento di riconoscimento del richiedente nonché di copia del tesserino contenente il codice fiscale (solo per i soggetti esterni).

Il richiedente, nel sottoscrivere il modulo, dichiara inoltre di:

- essere informato delle condizioni d'uso dei certificati individuate nel presente documento e nelle disposizioni integrative emanate dalla Banca d'Italia nonché di impegnarsi a non utilizzarli per funzioni e finalità diverse da quelle previste nelle disposizioni della Banca d'Italia;
- essere a conoscenza che, dal momento di ricezione della smartcard, potrà comunicare con l'Help desk della Banca d'Italia soltanto negli orari e nelle giornate specificati nel presente documento;
- aver ricevuto l'informativa sulla protezione dei dati personali forniti.

Per i soggetti esterni, la richiesta di certificato è allegata alla nota di designazione dal soggetto terzo interessato per il quale i richiedenti operano in virtù di un rapporto di lavoro o di rappresentanza. La nota di designazione - sottoscritta dal legale rappresentante dell'ente ovvero da altro soggetto a ciò delegato - deve:

- indicare le generalità del soggetto designato, la tipologia dei certificati da rilasciare, le finalità per le quali vengono richiesti i certificati;

- contenere una dichiarazione nella quale il terzo attesti di conoscere il contenuto del CPS/CP e di impegnarsi al rispetto degli obblighi in esso previsti a suo carico;
- recare in allegato la richiesta di certificato, redatta e sottoscritta dal soggetto designato.

La suddetta documentazione è inviata[7] alla RA competente.

4.2 Esame della richiesta

La RA esamina la documentazione ricevuta e provvede all'inserimento dei dati di identificazione del titolare nel sistema di registrazione.

L'eventuale mancato accoglimento dell'istanza è comunicato dalla RA al richiedente e, se del caso, al terzo interessato.

La convalida delle richieste è in carico alla RA che la riceve ed è gestita tramite il sistema di registrazione. Dopo la convalida, la RA inoltra le richieste all'infrastruttura di CA per procedere con l'emissione del certificato.

4.3 Emissione del certificato

Il certificato è generato presso i competenti Servizi dell'Amministrazione Centrale della Banca d'Italia con un sistema utilizzato esclusivamente per tale funzione, situato in locali adeguatamente protetti. L'emissione dei certificati avviene in modalità:

- decentrata, utilizzata principalmente per l'emissione di certificati destinati ai dipendenti della Banca d'Italia[8];
- accentrata[9], utilizzata di norma per l'emissione di certificati, generati con lo stato "sospeso", destinati a soggetti esterni. Al termine delle operazioni di

---

[7] Tramite servizio di recapito certificato (PEC) o da casella di posta elettronica convenzionale. Le credenziali di accesso alla PEC devono risultare conformi alle modalità richiamate dal Codice dell'Amministrazione Digitale e ciò deve essere attestato dal gestore del sistema nel messaggio PEC. Qualora non siano possibili le modalità precedenti, la richiesta è presentata con posta ordinaria o con consegna a mani.

[8] Il titolare in fase di assunzione riceve un badge di identificazione personale provvisto di chip crittografico (smartcard). L'utente si autentica, su protocollo HTTPS sulla rete interna della Banca, a un'applicazione web per la generazione dei certificati. Una volta effettuato l'accesso, l'applicazione web verifica che all'utente autenticato sia associata la smartcard rilevata dall'applicazione. A seguito dell'esito positivo del controllo, l'applicazione richiede al titolare di scegliere PIN e PUK – che vengono opportunamente registrati nella smartcard – nonché una pass-phrase da utilizzare per il riconoscimento del titolare da parte dell'Help desk nel caso di sospensione d'urgenza dei certificati. A conclusione di questa prima fase, il sistema genera la coppia di chiavi crittografiche direttamente all'interno del chip della smartcard; la chiave pubblica è trasmessa dall'applicazione web al server della CA per la generazione dei certificati all'interno del locale protetto. Il possesso della chiave privata da parte del titolare è attestato dal fatto che le richieste sono inviate alla CA dall'applicazione web che ha verificato l'associazione fra la smartcard e l'utente autenticato. La CA restituisce all'applicazione web il relativo certificato; l'applicazione lo inserisce nella smartcard.

[9] Il processo di generazione dei certificati e di produzione dei dispositivi sicuri contenenti le chiavi private (smartcard, token USB) è affidato alla Funzione Tecnica dell'Amministrazione Centrale della Banca. L'operatore autorizzato si autentica, utilizzando chiavi e certificati memorizzati su apposite smartcard, all'applicativo per l'emissione dei certificati aprendo una sessione verso la Certification

emissione la Funzione tecnica della Banca d'Italia spedisce[10] le smartcard e i relativi codici segreti (PIN, PUK, pass-phrase) alla RA che ha registrato l'utente.

A conclusione del processo di emissione, il certificato richiesto, la relativa chiave privata e il certificato relativo alle chiavi di certificazione della Banca d'Italia sono registrati sulla smartcard del titolare.

Al termine delle operazioni di generazione, il certificato è inserito nel Registro dei certificati; memorizzando la data e l'ora di emissione del certificato.

La Banca d'Italia informa i titolari dell'avvenuta creazione dei certificati comunicandone la loro disponibilità attraverso funzioni automatizzate per i dipendenti e attraverso la RA per i soggetti esterni.

4.4 Accettazione del certificato

I dipendenti, all'atto dell'assunzione, ricevono il badge personale su cui installare il certificato e l'accettazione del certificato si completa con l'installazione dello stesso sul badge personale (modalità decentrata).

Per i soggetti esterni, la RA - ricevute le buste contenenti rispettivamente la smartcard e i codici segreti (PIN, PUK e pass-phrase)[11] - invita il titolare del certificato a recarsi presso la RA stessa per completare l'identificazione previa esibizione di un documento valido (cfr. paragrafo 3.2). La RA, dopo averne autenticato l'identità, consegna al richiedente le buste contenenti la smartcard e i codici segreti e indica il sito dove è disponibile il presente documento. A seguito della consegna, il certificato, precedentemente emesso in stato "sospeso", viene attivato dalla RA tramite il sistema di registrazione.

Le operazioni di consegna del dispositivo di sicurezza che contiene la chiave privata sono verbalizzate e il relativo documento è conservato agli atti dalla RA.
Con la firma del verbale il titolare accetta il certificato.

4.5 Utilizzo del certificato e della coppia di chiavi

Ogni coppia di chiavi è assegnata ad un solo titolare.

I titolari dei certificati sono responsabili del corretto utilizzo degli stessi e della custodia dei dispositivi che li contengono; devono farne uso solo per le finalità per le quali sono stati rilasciati, mantenerli nel loro esclusivo possesso e informare la Banca d'Italia di ogni evento che ne possa compromettere la funzionalità. In particolare, i titolari devono proteggere le loro chiavi private da un uso non autorizzato e interrompere l'utilizzo della chiave privata dopo la sua scadenza o la revoca del certificato; conservare con la massima

Authority. L'operatore genera la smartcard contenente la chiave privata e la chiave pubblica del titolare.

[10] Con vettori separati.

[11] Il PIN deve essere digitato per procedere alle operazioni di autenticazione o crittografia e può essere variato dal titolare all'atto del primo utilizzo del dispositivo. Il PUK serve a sbloccare la smartcard dopo un numero prestabilito di tentativi errati di inserimento del PIN.

diligenza e separatamente il dispositivo che contiene la chiave privata e i codici segreti (PIN, PUK e pass-phrase) ricevuti dalla Banca d'Italia, al fine di garantirne l'integrità e la massima riservatezza. I titolari devono:

- utilizzare il certificato secondo le indicazioni degli attributi KeyUsage e ExtendedKeyUsage presenti nel certificato;
- verificare lo stato del certificato e utilizzarlo solo se detto stato risulta "in corso di validità".

I seguenti utilizzi sono esplicitati nel certificato nei campi keyUsage e ExtendedKeyUsage:

- *Auxiliary CA Certificate*
  KeyUsage: Certificate Signing, CRL Signing, Off-line CRL Signing.

- [1.3.76.38.1.3.2.1 AUTENTICAZIONE]
  KeyUsage: Digital Signature, Key Encipherment
  ExtendedKeyUsage: Client Autentication, Smart card Logon

- [1.3.76.38.1.3.2.2 CRITTOGRAFIA]
  KeyUsage: Digital Signature, Key Encipherment
  ExtendedKeyUsage: Email protection

Le terzi parti che utilizzano il certificato sono responsabili dell'utilizzo della chiave pubblica e del certificato per le finalità indicate nel presente documento.

4.6 Rinnovo del certificato (senza rigenerazione della chiave pubblica)[12]

La Banca d'Italia rinnova i certificati emettendo una nuova chiave pubblica del titolare, pertanto le procedure da seguire in caso di rinnovo sono quelle descritte al paragrafo 4.7.

Nel presente documento ogni riferimento al rinnovo di un certificato deve intendersi relativo all'emissione di un nuovo certificato con una nuova coppia di chiavi.

4.7 Rinnovo del certificato (con rigenerazione della chiave pubblica)

Per la Banca d'Italia, la riemissione delle chiavi di un certificato (re-key[13]) equivale al rilascio di un nuovo certificato che attesta una nuova chiave pubblica.

I dipendenti della Banca, in prossimità della scadenza dei certificati, ricevono una comunicazione automatica dal sistema di registrazione.
Il processo di rinnovo di un certificato prevede il riutilizzo della smartcard già in possesso del dipendente. Il richiedente è identificato direttamente dall'applicazione per la procedura di rinnovo di un certificato sulla smartcard. La procedura identifica il titolare verificando che la smartcard sia associata all'utente che si è autenticato. L'operazione comporta la cancellazione dei precedenti certificati dalla smartcard.

[12] Il rinnovo previsto dallo standard RFC 3647 prevede l'emissione di un nuovo certificato per il titolare senza modificare la chiave pubblica o le altre informazioni contenute nel certificato.
[13] Questa procedura è indicata come rinnovo nel modulo di richiesta.

Per i soggetti esterni, in prossimità della scadenza dei certificati, la RA provvede a chiedere ai terzi interessati se, con riferimento a ciascun titolare designato, sia necessario procedere al rinnovo.
In caso affermativo, il terzo interessato invia[14] alla RA competente una nota sottoscritta dal legale rappresentante o da altro soggetto all'uopo delegato, nella quale indica le generalità del titolare e le finalità per le quali viene richiesto il rinnovo di un certificato; alla predetta nota il terzo interessato allega la richiesta di emissione dei certificati effettuata dal titolare, da questi pure sottoscritta.
Il titolare è invitato dalla RA competente a recarsi presso i propri uffici per la consegna della nuova smartcard, contenente i certificati rinnovati e relativi codici segreti; nella circostanza viene ritirata la smartcard contenente i certificati in scadenza, dopo averla resa inutilizzabile mediante taglio del microcircuito. Il titolare è identificato previa esibizione di un documento valido.
Le suddette operazioni vengono verbalizzate e il relativo documento è conservato agli atti dalla RA; l'avvenuta consegna della nuova smartcard e dei relativi codici segreti dà luogo alla successiva attivazione dei certificati da parte della RA.

[1.3.76.38.1.3.2.2 ENCR] La Banca d'Italia conserva la chiave di crittografia del titolare nel formato PKCS#12 per consentire il recupero delle precedenti chiavi di crittografia dell'utente (key history) e affinché possa continuare a decifrare con queste ultime anche quando riceve un nuovo certificato di crittografia.

Solo nei casi di revoca per smarrimento, furto, compromissione della sicurezza e deterioramento della smartcard, la RA provvede d'ufficio all'avvio della procedura di rinnovo di un certificato.

4.8 Modifica del certificato

Il titolare deve comunicare alla Banca d'Italia eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica (e-mail), ecc.

Le modifiche che implicano variazioni delle informazioni contenute in un certificato richiedono il rinnovo del certificato stesso.

[14] Tramite servizio di recapito certificato (PEC) o da casella di posta elettronica convenzionale. Le credenziali di accesso alla PEC devono risultare conformi alle modalità richiamate dal Codice dell'Amministrazione Digitale e ciò deve essere attestato dal gestore del sistema nel messaggio PEC. Qualora non siano possibili le modalità precedenti, la richiesta è presentata con posta ordinaria o con consegna a mani. La richiesta deve essere sottoscritta con firma elettronica qualificata. Nel caso non fosse possibile utilizzare una firma qualificata, è necessario allegare una fotocopia di un valido documento di identificazione del titolare.

4.9 Revoca e sospensione di un certificato[15]

Revoca

Il titolare o il terzo interessato possono chiedere alla RA competente, con apposito modulo, la revoca del certificato al verificarsi delle causali riepilogate nella tabella riportata di seguito.

In caso di furto, smarrimento o compromissione della sicurezza della smartcard, il titolare è tenuto a rivolgersi al servizio di Help desk per la sospensione d'urgenza, secondo le modalità descritte nel presente documento (cfr. infra).
Nell'ipotesi di ritrovamento della smartcard può essere richiesta la riattivazione del certificato sospeso. Al contrario, qualora il furto o lo smarrimento vengano confermati, il titolare deve inoltrare richiesta di revoca.

La revoca del certificato avviene d'ufficio nel caso in cui, entro i 12 mesi successivi alla richiesta di sospensione (cfr. infra), non venga chiesta dallo stesso soggetto che ha chiesto la sospensione, l'attivazione o la revoca del certificato.

RICHIEDENTE / CAUSALE	TITOLARE (soggetto esterno o dipendente)	TERZO INTERESSATO (per i soggetti esterni)	BANCA D'ITALIA (per i dipendenti)
SMARRIMENTO DELLA SMARTCARD (previa sospensione)	X	-	-
FURTO DELLA SMARTCARD (previa sospensione)	X	-	-
COMPROMISSIONE DELLA SICUREZZA[16] (previa sospensione)	X	-	-
DETERIORAMENTO DELLA SMARTCARD	X	X	X
MODIFICA DELLA POSIZIONE TITOLARE[17]	-	X	X

Per i dipendenti della Banca d'Italia, la richiesta è comunicata alla RA dal titolare o dalla Struttura presso la quale presta servizio. La RA provvede ad inserire la richiesta nella Registration Web Application (sistema che offre le funzionalità di registrazione e per la gestione dei certificati).

[15] La revoca di un certificato determina la cessazione anticipata della sua validità. La sospensione di un certificato comporta l'interruzione temporanea della sua validità.
[16] Per compromissione della sicurezza deve intendersi il verificarsi di qualunque evento che faccia venire meno la certa riconducibilità al legittimo titolare dell'uso delle chiavi private.
[17] Causale da utilizzare ad esempio in caso di cessazione del titolare dall'attività lavorativa.

Per i soggetti esterni, la richiesta di revoca dovrà essere presentata[18] dal titolare o dal terzo interessato alla competente RA. Qualora la richiesta sia avanzata dal terzo interessato va sottoscritta dal legale rappresentante dell'ente ovvero da altro soggetto a ciò delegato.

La RA, verificata l'autenticità della stessa, provvede ad avviare il procedimento di revoca, avvalendosi della specifica funzionalità del sistema di registrazione.
Essa informa il titolare e, se del caso, il terzo interessato dell'avvenuta revoca del certificato, specificando la data e l'ora a partire dalle quali il certificato non è più valido.

Salvo i casi di smarrimento e furto, il titolare è tenuto a restituire o a far recapitare alla RA la smartcard in proprio possesso dopo averla resa inutilizzabile mediante taglio del microcircuito.
L'operazione di ritiro della smartcard viene verbalizzata e l'avvenuto ritiro è segnalato nel sistema di registrazione tramite la specifica funzionalità.
A seguito della revoca per smarrimento, furto, compromissione della sicurezza e deterioramento della smartcard, la Banca provvede d'ufficio all'avvio della procedura per il rinnovo del certificato.

I certificati sono sospesi o revocati da parte della Banca d'Italia mediante inserimento del relativo numero identificativo (serial number) nella CRL.
La sospensione e la revoca sono efficaci a partire dal momento dell'inserimento dei certificati nella suddetta lista (per ulteriori dettagli su questa ultima, consultare il capitolo 7).

Un certificato revocato non può essere ripristinato.

La revoca, la sospensione e la successiva riattivazione dei certificati sono memorizzate con l'indicazione della data e dell'ora di esecuzione dell'operazione.
La lista di revoca e sospensione è aggiornata ad ogni richiesta e pubblicata almeno ogni 24 ore. La revoca avviene entro un'ora dall'identificazione del richiedente e dalla verifica dell'autenticità della richiesta.

La Banca d'Italia, qualora venga a conoscenza di sospetti abusi, falsificazioni, negligenze, si riserva la facoltà di sospendere o revocare i certificati del titolare previa, salvo i casi di urgenza, comunicazione motivata ai titolari stessi.

[18] Tramite servizio di recapito certificato (PEC) o da casella di posta elettronica convenzionale. Le credenziali di accesso alla PEC devono risultare conformi alle modalità richiamate dal Codice dell'Amministrazione Digitale e ciò deve essere attestato dal gestore del sistema nel messaggio PEC. Qualora non siano possibili le modalità precedenti, la richiesta è presentata con posta ordinaria o con consegna a mani. La richiesta deve essere sottoscritta con firma elettronica qualificata. Nel caso non fosse possibile utilizzare una firma qualificata, è necessario allegare una fotocopia di un valido documento di identificazione del titolare.

Revoca dei certificati delle chiavi di certificazione

La Banca d'Italia procede alla revoca del certificato relativo alla coppia di chiavi di certificazione in caso di:

- compromissione della chiave privata, intesa come diminuita affidabilità delle caratteristiche di sicurezza di quest'ultima;
- cessazione dell'attività.

La revoca implica la registrazione del certificato nella lista dei certificati revocati e sospesi e viene comunicata a tutti i titolari di certificati emessi dalla Banca d'Italia firmati con la chiave privata appartenente alla coppia revocata.

Nel caso in cui la revoca discenda dalla compromissione della chiave privata della Banca d'Italia, vengono revocati d'ufficio tutti i certificati sottoscritti con detta chiave.

Sospensione

Il titolare o il terzo interessato possono chiedere alla RA competente la sospensione della validità del certificato al verificarsi delle causali riepilogate nella tabella che segue.

RICHIEDENTE / CAUSALE	TITOLARE (soggetto esterno o dipendente)	TERZO INTERESSATO (per i soggetti esterni)	BANCA D'ITALIA (per i dipendenti)
SMARRIMENTO DELLA SMARTCARD	X	--	--
FURTO DELLA SMARTCARD	X	--	--
COMPROMISSIONE DELLA SICUREZZA	X	--	--
PROLUNGATA ASSENZA DEL TITOLARE	--	--	X
ALTRO[19]	X	X	X

Laddove sia indicata la causale altro, è necessario fornire un'opportuna motivazione.

Per i dipendenti della Banca d'Italia, la richiesta di sospensione è comunicata alla RA dal titolare o dalla Struttura presso la quale presta servizio o dal titolare all'Help desk in caso di sospensione di urgenza. La RA provvede ad inserirla nella Registration Web Application (sistema che offre le funzionalità di registrazione e per la gestione dei certificati).

[19] La causale "altro" comprende tutte le fattispecie non riconducibili a quelle espressamente individuate.

Per i soggetti esterni, la richiesta di sospensione dovrà essere presentata[20] dal titolare alla competente RA. Qualora la richiesta sia avanzata dal terzo interessato va sottoscritta dal legale rappresentante dell'ente ovvero da altro soggetto a ciò delegato.

La RA, verificata l'autenticità della stessa, provvede ad avviare il procedimento di sospensione avvalendosi della specifica funzionalità del sistema di registrazione.
La RA informa il titolare e il terzo interessato dell'avvenuta sospensione del certificato, specificando la data e l'ora a partire dalle quali il certificato non è più valido.

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

Modalità di comunicazione della sospensione d'urgenza

La Banca d'Italia garantisce un servizio di sospensione:
- per le richieste d'urgenza relative a furto, smarrimento e compromissione della sicurezza tramite il servizio di Help desk (tel. 06/47929361) disponibile 24 ore su 24, tutti i giorni feriali e festivi;
- negli altri casi negli orari di ufficio (8.30-16.30).

Per l'identificazione del titolare nei colloqui telefonici con l'Help desk in cui si richiede la sospensione d'urgenza dei certificati è necessario fornire una pass-phrase che è stata comunicata all'utente alla consegna del certificato.

Qualora l'operazione di identificazione del richiedente non vada a buon fine, il certificato viene sospeso in via cautelativa. Entro le successive 24 ore il richiedente dovrà comunicare idonei elementi ai fini della sua identificazione.

Riattivazione dei certificati sospesi

Lo stesso soggetto che ha avanzato l'istanza di sospensione invia alla RA una richiesta di attivazione contenente i dati identificativi del titolare e del certificato.
La richiesta di riattivazione è avanzata con le modalità e osservando l'iter procedurale già descritto per le richieste di sospensione diverse da quelle di urgenza.

La CA procede alla riattivazione del certificato attraverso la cancellazione dello stesso dalla lista dei certificati revocati e sospesi.

La RA comunica al titolare e al terzo interessato l'avvenuta riattivazione del certificato, specificando la data e l'ora a partire dalle quali esso è nuovamente attivo.

[20] Tramite servizio di recapito certificato (PEC) o da casella di posta elettronica convenzionale. Le credenziali di accesso alla PEC devono risultare conformi alle modalità richiamate dal Codice dell'Amministrazione Digitale e ciò deve essere attestato dal gestore del sistema nel messaggio PEC. Qualora non siano possibili le modalità precedenti, la richiesta è presentata con posta ordinaria o con consegna a mani. . La richiesta deve essere sottoscritta con firma elettronica qualificata. Nel caso non fosse possibile utilizzare una firma qualificata, è necessario allegare una fotocopia di un valido documento di identificazione del titolare.

4.10 Servizi relativi allo stato del certificato

La Banca d'Italia garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati emessi, sospesi e revocati.
La gestione del Registro dei certificati avviene con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che l'operatore autorizzato possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza.
Per i dettagli sulla fruizione dei servizi si fa rinvio al capitolo 7.

4.11 Termine di validità del certificato

Il certificato cessa di essere valido quando:

- il certificato arriva a scadenza senza che sia stato richiesto il rinnovo;
- il certificato viene revocato.

4.12 Key escrow e key recovery delle chiavi di certificazione[21]

Il ripristino della chiave di certificazione (key recovery) è previsto in caso di guasto dell'HSM. Al fine di consentire il key recovery, la CA mantiene una copia di backup di detta chiave con gli stessi livelli di sicurezza previsti per la chiave primaria.

[1.3.76.38.1.3.2.1 AUTENTICAZIONE] La Banca d'Italia non conserva la chiave di autenticazione del titolare.

[1.3.76.38.1.3.2.2 CRITTOGRAFIA] La Banca d'Italia conserva la chiave di crittografia del titolare nel formato PKCS#12 per consentire il recupero delle precedenti chiavi di crittografia dell'utente (key history) e affinché possa continuare a decifrare con queste ultime anche quando riceve un nuovo certificato di crittografia.

[21] Per la chiave di autenticazione del titolare non è prevista la procedura di key escrow (affidamento di una coppia di chiavi ad un soggetto esterno) o key recovery poiché la Banca d'Italia non agisce come depositario delle chiavi.

5 CONTROLLI RELATIVI AI LOCALI DELLA PKI E AGLI AMBITI GESTIONALI E OPERATIVI

La Banca d'Italia ha definito specifiche policy in materia di sicurezza ICT e riservatezza delle informazioni e si attiene alla normativa europea e nazionale in materia di protezione dei dati personali.
L'infrastruttura della PKI è sottoposta periodicamente ad assessment di sicurezza.

La PKI della Banca d'Italia rientra nelle misure di continuità previste per la "Gestione della continuità dei servizi ICT essenziali". La Banca d'Italia dispone di un Piano di Continuità Operativa per limitare gli effetti negativi di eventi di diversa natura, quali indisponibilità di risorse logistiche (stabili, elettricità), ICT (pc, sistemi informatici, reti) e umane. Il Piano di Continuità Operativa:

- elenca i processi critici e le funzioni responsabili;
- stabilisce i ruoli e le responsabilità organizzative e gestionali ai diversi livelli;
- elenca i siti per la gestione dell'emergenza e i protocolli di utilizzo dei siti di recovery;
- individua il personale essenziale per assicurare la continuità operativa;
- contiene le regole procedurali e le informazioni necessarie per l'attivazione e per la gestione dello stato di emergenza;
- stabilisce le regole da seguire per la conservazione e la diffusione delle informazioni;
- disciplina le modalità da seguire per tornare allo stato di ordinaria operatività.

5.1 Controlli fisici

5.1.1 Ubicazione e caratteristiche dei locali

L'infrastruttura PKI della Banca d'Italia è ubicata presso un sito primario e uno secondario di recovery. I locali sono dotati di protezione volumetrica contro l'intrusione.
L'infrastruttura presenta una configurazione ad alta affidabilità per il recovery in caso di disastro grazie a:

- componenti hardware e software fisicamente installate nei locali della Banca d'Italia (on premise), presso il sito primario e il sito secondario, collegate tra di loro in rete mediante fibre ottiche;
- Storage Area Network (SAN), configurata in modalità di copia remota sincrona con il sito secondario.

Entrambi i siti sono sottoposti a sorveglianza e assistiti da un servizio di controllo degli accessi negli orari di ufficio nonché presidiati da specifici posti di controllo negli orari di chiusura.

5.1.2 Accesso ai locali

L'attività operativa della CA e tutta l'attività relativa al ciclo di vita del processo di certificazione sono svolte all'interno di locali il cui accesso è riservato al solo personale autorizzato, con profili differenziati a seconda delle aree cui si è abilitati. L'accesso ai locali avviene attraverso bussole rotanti. L'accesso ad ogni livello richiede l'uso di badge del personale tramite lettori di prossimità.

Le postazioni di approvazione delle richieste di rilascio dei certificati non richiedono un livello di sicurezza fisica superiore a quello dei normali posti di lavoro.

5.1.3 Energia elettrica e impianto di condizionamento dei locali

Tutte le apparecchiature sono alimentate da sistemi di continuità assoluta, ridondanti. Il sistema di condizionamento consente il controllo dell'umidità e la climatizzazione di base. Un sistema di supervisione monitora H24 per 365 giorni lo stato degli impianti tecnologici (elettrici e di condizionamento) e permette di localizzare rapidamente eventuali anomalie sull'impianto.

5.1.4 Rilevazione di perdite d'acqua

L'impianto rileva la presenza di acqua dovuta a rotture delle tubazioni e/o componenti dell'impianto di condizionamento nonché alla eventuale perdita sui tubi delle acque di scarico, in modo da ridurre al minimo l'impatto dell'esposizione all'acqua dei sistemi della PKI.

5.1.5 Prevenzione e protezione da incendi

Le misure di prevenzione e protezione dall'incendio sono state progettate per soddisfare le normative locali di sicurezza antincendio.
L'impianto antincendio è costituito dall'integrazione di un sistema di rilevamento fumi e da un sistema di estinzione.

5.1.6 Sistemi di archiviazione

I dispositivi contenenti dati personali sono trattati secondo la normativa europea e nazionale in materia di protezione dei dati personali.

Tutti i supporti contenenti software di produzione, i dati di audit, o informazioni di backup sono all'interno delle strutture di Banca d'Italia protetti da adeguati controlli fisici e logici volti a limitare l'accesso solo al personale autorizzato e a proteggerli da danni accidentali.

Le quantità di sicurezza per l'accesso alle funzioni critiche dell'infrastruttura sono protette tramite l'uso di casseforti chiuse, contenitori e armadi, la cui apertura e chiusura di è registrata per eventuali controlli di audit.

5.1.7 Smaltimento dei rifiuti

Prima dello smaltimento dei dispositivi crittografici sono fisicamente distrutti o azzerati secondo le indicazioni fornite dai produttori.

5.1.8 Sito di backup esterno

La Banca d'Italia esegue i backup di routine dei dati critici del sistema, dei log di audit e di altre informazioni utili a garantire il corretto ripristino dei dati.

Il sito secondario è in copia remota sincrona.

5.2 Ruoli funzionali per la conduzione dell'infrastruttura

Le operazioni relative alla Certification Authority sono svolte in via accentrata presso l'Amministrazione centrale. La trasmissione dei dati dalla RA alla CA avviene sulla rete interna della Banca, adeguatamente protetta.

I ruoli funzionali per la conduzione dell'infrastruttura sono distribuiti come riportato nella tabella.

Ruoli Funzionali	Servizio Gestione sistemi informatici (GES)	Servizio Sviluppo informatico (SVI)	Servizio Revisione interna (REV)	Servizio Immobili (IMM)	Servizio Logistica e servizi (LOS)
Responsabile del servizio di certificazione		X			
Responsabile dell'evoluzione dell'infrastruttura (progettazione e realizzazione dell'infrastruttura informatica)		X			
Responsabile dei presidi di sicurezza dell'infrastruttura (verifiche di sicurezza prima del rilascio in esercizio)		X			
Responsabile dell'evoluzione della piattaforma applicativa (progettazione e realizzazione delle applicazioni)		X			
Responsabile della sicurezza fisica dell'infrastruttura				X	
Responsabile della sicurezza logica e dell'amministrazione della componente tecnologica	X				

Responsabile delle verifiche di sicurezza delle infrastrutture e delle applicazioni in fase di esercizio	X				
Responsabile della conduzione tecnica dei sistemi	X				
Responsabile dei servizi tecnici	X				
Responsabile dei servizi logistici					X
Responsabile delle verifiche e delle ispezioni (auditing)			X		

Gli autorizzati al trattamento dei dati ai sensi della normativa europea e nazionale in materia di protezione dei dati personali sono: i Capi dei Servizi dell'Amministrazione Centrale e delle Filiali per la fase di registrazione delle richieste; il Capo del Servizio Sviluppo informatico, struttura responsabile per la Banca d'Italia del servizio di certificazione; il Capo del Servizio Gestione sistemi informatici presso il quale si svolgono le fasi di produzione dei certificati e l'attività di *Help desk*; gli addetti autorizzati al trattamento.

La Banca d'Italia considera affidabile il personale di seguito indicato data l'esistenza di un rapporto di lavoro e/o di una collaborazione in essere avente come oggetto il servizio di certificazione:

- personale responsabile per l'amministrazione della sicurezza (security officer);
- personale autorizzato ad installare, configurare e manutenere i sistemi per la gestione del servizio (system administrator);
- personale responsabile della conduzione quotidiana del sistema e autorizzato a svolgere copie di backup (system operator);
- personale autorizzato a consultare archivi e log di audit (system auditor).

Le funzioni più critiche del servizio di certificazione sono svolte con procedure basate su un controllo di tipo "four eyes" e un processo di autenticazione forte. L'accesso ai moduli crittografici per la gestione dei certificati è riservato ai security officer secondo procedure definite che prevedono la presenza di almeno due persone autorizzate per l'accesso ai dispositivi.

La Banca d'Italia considera affidabili tutti gli impiegati che hanno un ruolo nelle seguenti fasi:

- convalida delle informazioni contenute nelle richieste di certificati;
- accettazione, rigetto o altro esame di richieste relative al ciclo di vita dei certificati;
- rilascio o revoca di certificati, ivi incluso il personale che ha accesso alle parti riservate dell'archivio;
- elaborazione di informazioni e domande presentate dai titolari.

5.3 Requisiti del personale addetto e relativi controlli

Il personale addetto al servizio ha una pluriennale esperienza nel campo della definizione, sviluppo e gestione di servizi di PKI e ha ricevuto una adeguata formazione sulle procedure e gli strumenti da utilizzare nelle varie fasi operative.

In caso di atti non autorizzati o di altre violazioni delle policy e procedure della Banca d'Italia sono stabilite idonee misure disciplinari, commisurate alla frequenza e gravità delle azioni poste in essere.

La manutenzione dell'infrastruttura è assicurata tramite servizi di assistenza specialistica e di manutenzione delle varie componenti erogati da società di terze parti che operano, ove necessario on site, secondo le direttive del personale della Banca responsabile della gestione e dello sviluppo dell'infrastruttura. Per i servizi professionali erogati da soggetti esterni viene effettuata una valutazione dei Curricula Vitae.

Gli obblighi del personale della Banca sono stabiliti nel Regolamento del personale della Banca d'Italia; gli obblighi del personale esterno sono stabiliti nelle condizioni generali di contratto per i servizi professionali.

5.4 Procedure di registrazione degli eventi

Le principali attività di auditing sulle componenti dell'infrastruttura sono svolte effettuando interrogazioni sul sistema della Banca d'Italia che raccoglie le segnalazioni relative a particolari eventi sui sistemi informatici o agli incidenti di sicurezza informatica. Tale sistema è ospitato in locali protetti.

La Certification Authority registra tutte le transazioni che riguardano il ciclo di vita dei certificati in file di log che possono essere interrogati qualora necessario.

Le operazioni di audit sui sistemi della PKI sono svolte da postazioni di lavoro abilitate che si connettono ai sistemi mediante un canale cifrato, previa autenticazione.
La Banca d'Italia analizza i propri log di audit per attività sospette o anomale in risposta a segnalazioni generate sulla base di irregolarità e incidenti sull'infrastruttura di CA e RA.

Gli audit log sono conservati per un periodo di 12 mesi dopo il trattamento e storicizzati per renderli disponibili anche dopo l'eventuale cessazione della CA.

Tutti gli eventi sono registrati ai sensi delle normative nazionali in materia e della normativa europea e nazionale in materia di trattamento dei dati personali; in particolare viene effettuata la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

Le attività inerenti la risoluzione di problemi di carattere sistemistico ed applicativo sono svolte utilizzando le informazioni contenute nei file di log di tutti gli applicativi dell'infrastruttura. I file di log vengono esaminati almeno su base settimanale per eventi significativi legati alla sicurezza ed operativi. Le revisioni sul file di log comprendono una verifica che lo stesso non sia stato manomesso, l'ispezione di tutte le voci del file, ed un'indagine di avvisi o irregolarità nei file di log.

Le informazioni registrate dai log sono protette da rischi di modifica e distruzione accidentale/intenzionale applicando le misure di controllo degli accessi.

5.5 Archiviazione delle registrazioni

La Banca d'Italia protegge le registrazioni archiviate in modo tale che soltanto le persone autorizzate possano consultarle per gli usi consentiti. I dati archiviati elettronicamente sono protetti contro la visione, modifica, cancellazione o altra manomissione non autorizzata mediante l'attuazione di idonei controlli fisici e logici.

La Banca d'Italia mantiene per 20 anni la registrazione di tutte le informazioni relative al certificato dal momento della sua emissione anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari.

La Banca d'Italia realizza un backup sia dell'archivio elettronico delle informazioni sui certificati rilasciati ogni giorno sia dei file di log settimanalmente.

I back-up della chiave privata della CA sono generati e mantenuti in conformità a quanto indicato nel capitolo 6.

5.6 Cambio delle chiavi della CA

Le chiavi di certificazione hanno validità 20 anni. La scadenza del certificato di CA è di almeno due anni successiva alla scadenza dei certificati dei titolari emessi dalla CA.
La Banca d'Italia novanta giorni prima della scadenza del certificato relativo ad una chiave di certificazione avvierà la procedura di sostituzione, generando una nuova coppia di chiavi. La procedura di sostituzione delle chiavi avverrà nel rispetto degli stessi requisiti utilizzati per la generazione avendo cura che il termine del periodo di validità del certificato delle chiavi di certificazione sia successivo di almeno due anni rispetto ai certificati rilasciati ai titolari.
In aggiunta al certificato (self-signed) relativo alla nuova coppia di chiavi di certificazione di cui sopra, la Banca d'Italia genererà:

- un certificato della CA relativo alla nuova chiave pubblica sottoscritto con la chiave privata della vecchia coppia;
- un certificato della CA relativo alla vecchia chiave pubblica sottoscritto con la nuova chiave privata.

5.7 Incidenti di sicurezza e disaster recovery

La Banca d'Italia procederà alla revoca (cfr. paragrafo 4.9) del certificato relativo alla coppia di chiavi di certificazione in caso di compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza di quest'ultima, o cessazione della propria attività.

La Banca d'Italia prevede un sistema tecnico e organizzativo per la gestione di tutti gli eventi che determinano impatti sulla disponibilità dei sistemi (malfunzionamenti),

sull'integrità e sulla riservatezza delle informazioni in essi trattati (incidenti di sicurezza). In riferimento all'infrastruttura PKI, sono considerati incidenti di particolare rilievo:

- la mancata pubblicazione della lista dei certificati revocati e sospesi;
- il mancato aggiornamento entro i periodi previsti della suddetta lista;
- i malfunzionamenti del servizio di CA e dei dispostivi HSM che contengono le chiavi private.

Anche in assenza di incidenti di sicurezza, almeno annualmente sono identificate e analizzate le vulnerabilità dei sistemi operativi e delle applicazioni.

In caso di incidenti di sicurezza che possono avere particolari impatti sul servizio di certificazione e sui dati personali, la Banca d'Italia, ove applicabile, informerà i soggetti istituzionali competenti, di tutte le violazioni della sicurezza o delle perdite di integrità che abbiano un impatto significativo sui servizi prestati o sui dati personali custoditi.
Qualora l'incidente possa avere impatti sul titolare del certificato, la Banca d'Italia provvederà ad informare il titolare attraverso i dati forniti in sede di registrazione.

Nel caso di indisponibilità di tutte le infrastrutture hardware e software e di telecomunicazione del sito elaborativo primario, le specifiche procedure di disaster recovery hanno l'obiettivo di ripristinare, nel sito secondario, la situazione elaborativa immediatamente precedente l'evento disastroso, senza perdita di dati per tutti i servizi applicativi e infrastrutturali che prevedono tale salvaguardia. L'emissione di nuovi certificati per il personale esterno è sospesa fino al ripristino dei sistemi nel sito primario.

5.8 Cessazione della CA

All'atto dell'eventuale cessazione dell'attività di prestatore di servizi fiduciari, la Banca di Italia non individuerà un prestatore di servizi fiduciari sostitutivo e porrà in essere il seguente piano di cessazione.

- Almeno 60 giorni prima della cessazione:

  1. sarà inviata un'informativa a tutti gli utenti del servizio di Certification Authority (CA) svolto dalla Banca d'Italia e agli altri soggetti istituzionali rilevanti;
  2. saranno informati i titolari dei certificati, specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati;
  3. le registrazioni e le informazioni relative ai certificati, intervenute dal momento della loro emissione, saranno conservate dalla Banca d'Italia anche dopo la cessazione delle attività, per almeno 20 anni; ciò al fine di fornire prova in eventuali procedimenti legali e/o amministrativi;
  4. saranno definite e rese pubbliche le modalità con cui rendere disponibili le informazioni di revoca.

- Alla data di cessazione:

  1. le chiavi di certificazione e il relativo hardware saranno dismessi in modo sicuro secondo le indicazioni dei fornitori, nel rispetto del principio del four eyes e verbalizzando l'operazione;

2. sarà assicurato un servizio per il recupero in modalità sicura di tutte le chiavi di crittografia di un utente (key history);
3. saranno revocati i certificati attivi emessi dalla CA cessata;
4. sarà aggiornata per l'ultima volta la lista di revoca e saranno rese indisponibili le chiavi di certificazione della CA cessata per l'emissione di certificati.

6 CONTROLLI DI SICUREZZA TECNICI

L'infrastruttura PKI è logicamente separata dalle altre infrastrutture elaborative della Banca d'Italia ed è dotata di propri apparati, server fisici e macchine virtuali, console di gestione.

L'infrastruttura hardware prevede l'installazione in due siti, uno primario e uno di recovery, delle seguenti apparecchiature elaboratori, sistemi di storage, apparati di interconnessione, per ciascun sito, in appositi armadi (rack).

I server sono configurati in cluster, il che consente di avere automatismi che assicurano il recovery delle principali risorse applicative e di sistema.

Le operazioni di registrazione delle richieste sono effettuate attraverso un applicativo web raggiungibile esclusivamente della rete interna della Banca d'Italia.

6.1 Installazione e generazione della coppia di chiavi

Le coppie di chiavi generate dal servizio di certificazione della Banca d'Italia appartengono alle seguenti tipologie:

- chiavi di certificazione, cioè le chiavi utilizzate dalla Banca d'Italia per firmare elettronicamente i certificati dei titolari e la lista di revoca e sospensione dei certificati. Le chiavi di certificazione hanno validità 20 anni. Con tali chiavi saranno sottoscritti i certificati dei titolari con periodo di validità temporalmente inferiore alla validità delle chiavi di certificazione.
- chiavi di autenticazione e di crittografia (queste ultime usate anche per la firma elettronica delle mail), attribuite dalla Banca d'Italia ai singoli titolari. Ciascuna coppia di chiavi è attribuita ad un solo titolare.

Ogni coppia di chiavi è utilizzabile unicamente per la tipologia di operazione per la quale è stata generata. L'indicazione della tipologia di operazione che è possibile effettuare con la coppia di chiavi è riportata nel relativo certificato.

Generazione della coppia di chiavi

La generazione della coppia di chiavi di certificazione avviene in un ambiente fisicamente sicuro, all'interno del dispositivo di sicurezza certificato, secondo una procedura che richiede l'intervento congiunto di almeno due persone diverse ("dual control"). L'esecuzione della procedura ("key ceremony") è tracciata in un report conservato dal responsabile della sicurezza.

La generazione della coppia di chiavi di autenticazione o crittografia del titolare avviene all'interno del dispositivo consegnato al titolare.
La generazione della coppia di chiavi (pubblica e privata) è effettuata dalla Banca d'Italia mediante dispositivi e procedure che garantiscono, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e un adeguato livello di sicurezza della coppia generata, nonché la segretezza della chiave privata. Tali dispositivi sono in grado di:

- generare al proprio interno coppie di chiavi asimmetriche con equiprobabilità di generazione di tutte le coppie possibili;

- autenticare informaticamente il soggetto che attiva la procedura di generazione;
- proteggere la chiave privata da accessi non autorizzati;
- effettuare le elaborazioni crittografiche di cifra;
- garantire la conformità della coppia di chiavi ai requisiti previsti per gli algoritmi di generazione e di verifica utilizzati;
- evitare che nelle operazioni di autenticazione o crittografia il dispositivo consegnato al titolare comunichi all'esterno le chiavi private del titolare.

[1.3.76.38.1.3.2.2 ENCR] Per i dipendenti della Banca d'Italia che dispongono del dispositivo mobile aziendale è possibile installare il certificato di crittografia software su un dispositivo mobile per consentire l'invio e la ricezione di mail cifrate da questo ultimo.
Durante la generazione dei certificati digitali sul dispositivo che contiene le chiavi private del titolare è prodotto anche il certificato di crittografia software su un file e relative chiavi; il certificato di crittografia e la chiave privata sono esportati su un file in formato PKCS#12. Il file PKCS#12 è adeguatamente protetto da una password di sblocco poiché contiene la chiave privata del titolare. La creazione del file PKCS#12 avviene attraverso un processo completamente automatizzato al termine del quale al titolare sono inviate due mail contenenti rispettivamente il file PKCS#12 protetto dalla password e la password di sblocco, cifrata con la chiave di crittografia in possesso del titolare. Alla ricezione delle mail, l'utente decifra la password di sblocco con la propria chiave di crittografia. La password di sblocco è richiesta per accedere al file PKCS#12 da installare sul dispositivo mobile aziendale.

Lunghezza delle chiavi ed algoritmi

Le coppie di chiavi devono essere di lunghezza sufficiente ad impedire ad altri di determinarne la chiave privata utilizzando crittoanalisi.

La lunghezza delle chiavi di certificazione è di 4096 bit.

La lunghezza delle chiavi dei certificati dei titolari è di 2048 bit.

Per la generazione delle chiavi è utilizzato l'algoritmo RSA (Rivest-Shamir-Adleman), con esponente pubblico pari a 65537 (0x10001).

La funzione di hash utilizzata è SHA256encryption.

Generazione e installazione del certificato

I certificati sono generati con un sistema dedicato, situato in locali adeguatamente protetti. Le modalità di installazione dei certificati sui dispositivi sono descritte nel paragrafo 4.3.
Al termine delle operazioni di generazione, il certificato è inserito nel Registro dei certificati; memorizzando la data e l'ora di emissione del certificato.
I certificati sono consultabili secondo le modalità descritte nel presente documento (cfr. capitolo 7).

Il certificato contenente la chiave pubblica di certificazione della CA è generato nel formato ISO 9594-8 ed è pubblicato sul sito della Banca d'Italia all'indirizzo http://www.bancaditalia.it/firmadigitale.

Le chiavi private del titolare, il relativo certificato e i certificati relativi alle chiavi di certificazione della Banca d'Italia sono memorizzati su un dispositivo elettronico (smartcard/un token USB) dotato di microchip con funzionalità crittografiche.

6.2 Protezione della chiave private e controlli dei dispositivi crittografici

La Banca d'Italia ha posto in essere una combinazione di controlli fisici, logici e procedurali al fine di garantire la sicurezza delle chiavi private.
I titolari sono obbligati a prendere le precauzioni necessarie per prevenire la perdita, divulgazione, modifica o l'uso non autorizzato delle chiavi private.
Il titolare conserva con la massima diligenza e separatamente il dispositivo che contiene la chiave privata e i codici segreti (PIN, PUK e pass-phrase) ricevuti dalla Banca d'Italia, al fine di garantirne l'integrità e la massima riservatezza.

Sistema di Emissione dei Certificati

Il prodotto software utilizzato per la gestione dei certificati è implementato con toolkit crittografici che hanno conseguito la certificazione FIPS 140-2 L3.

Dispositivi crittografici per le chiavi di CA

Il dispositivo HSM che contiene la chiave privata di certificazione della CA ha conseguito la certificazione Common Criteria EAL 4+.
Le operazioni di gestione del dispositivo avvengono mediante applicativi installati sul sistema di emissione dei certificati oppure mediante comandi proprietari dello stesso HSM.
Le operazioni di amministrazione vengono autorizzate dai referenti dei dispositivi crittografici attraverso l'utilizzo di chiavi hardware.
La Banca d'Italia adotta meccanismi tecnici e procedurali che prevedono la partecipazione di più persone autorizzate allo svolgimento di operazioni crittografiche sensibili per la CA.
In caso di dismissione o sostituzione a seguito di guasto dell'HSM, si procede preliminarmente alla cancellazione dei dati presenti sul dispositivo stesso, conformemente alle procedure rilasciate dal produttore.
Al termine del loro ciclo di vita, le chiavi di firma della CA vengono distrutte in modo sicuro ed anche il dispositivo hardware che le contiene viene messo in disuso in modo sicuro. Le operazioni sono condotte secondo il principio del "four-eyes" e sono verbalizzate.

Dispositivi crittografici del titolare

I dispositivi utilizzati dai titolari sono certificati Common Criteria EAL4+ (protection Profile CWA14169).
Sono previsti i seguenti dispositivi sicuri: smartcard (per i dipendenti della Banca d'Italia integrate con i badge personali); in casi del tutto particolari, token USB per talune categorie di soggetti esterni. L'accesso alla chiave privata da parte del titolare è protetto da un PIN.

Nell'ambito del processo di personalizzazione del dispositivo di sicurezza, si svolgono le seguenti operazioni:

- acquisizione dei dati identificativi del titolare e loro associazione al dispositivo;

- registrazione nel dispositivo dei dati identificativi del titolare presso la Banca d'Italia;
- registrazione nel dispositivo del certificato relativo alle chiavi del titolare.

La responsabilità della protezione della chiave privata è in carico al titolare che custodisce il dispositivo di sicurezza.
Le chiavi private dei titolari non possono essere estratte, allo stato attuale della tecnologia, dai dispositivi di sicurezza che le contengono.
La Banca non duplica le chiavi private o i dispositivi di sicurezza che le contengono.

Backup delle chiavi private

La Banca d'Italia crea copie di backup della chiave privata della CA ai fini del recupero di routine e del disaster recovery.
Il processo di generazione delle chiavi di certificazione prevede la clonazione delle chiavi private su dispositivi di salvaguardia (back-up) che presentano i medesimi profili autorizzativi dell'originale e sono custoditi in locali protetti. Quando viene creato un backup della coppia di chiavi CA su un altro modulo crittografico hardware, le coppie di chiavi vengono trasportate da un modulo all'altro in forma criptata. Queste copie possono essere usate qualora, a seguito di malfunzionamenti o dell'impossibilità di usare la chiave originale, non fosse possibile garantire la continuità del servizio di certificazione.

[1.3.76.38.1.3.2.1 AUTENTICAZIONE] Per le chiavi private di autenticazione non è previsto il back-up e il key escrow (cfr. capitolo 4).

[1.3.76.38.1.3.2.2 CRITTOGRAFIA] La Banca d'Italia conserva, in modalità sicura, copie di back-up delle chiavi private di crittografia del titolare per garantire la gestione del key history in modo che il titolare possa decifrare i documenti cifrati con vecchie chiavi private.

Archiviazione della chiave privata

La chiave privata della CA è conservata su moduli hardware crittografici in forma criptata.
Quando la coppia di chiavi della CA è giunta alla scadenza del periodo di validità, sarà archiviata per un periodo di almeno 5 anni. La coppia di chiavi CA archiviata sarà memorizzate in maniera sicura con l'ausilio di moduli crittografici hardware che soddisfano i requisiti del presente CPS/CP.
[1.3.76.38.1.3.2.1 AUTENTICAZIONE] La Banca d'Italia non archivia le chiavi private dei titolari.

[1.3.76.38.1.3.2.2 CRITTOGRAFIA] La Banca d'Italia archivia le chiavi private dei titolari per il key history.

Distruzione della chiave privata

Ove necessario, la Banca d'Italia distruggerà le chiavi private della CA in modo tale da garantire in misura ragionevole che non esistano residui della chiave che potrebbero portare ad una ricostruzione della stessa. Al termine del loro ciclo di vita, le chiavi di firma della CA vengono distrutte in modo sicuro secondo le procedure indicate dal fornitore degli apparati ed anche il dispositivo hardware che le contiene viene messo in disuso in modo sicuro. Le operazioni sono condotte secondo il principio del "four-eyes" e sono verbalizzate.

Con riferimento alle chiavi private dei titolari, queste sono distrutte in occasione della consegna di una nuova smartcard, in quanto la vecchia smartcard è resa inutilizzabile mediante taglio del microcircuito.

6.3 Altri aspetti relativi alla gestione della coppia di chiavi

Quanto descritto nei paragrafi precedenti esaurisce l'argomento relativo alla gestione della coppia di chiavi.

6.4 Dati per l'attivazione della chiave privata

La chiave privata della CA è sempre attiva.

I titolari del certificato attivano la chiave privata con l'inserimento del PIN, richiesto a seguito dell'inserimento del dispositivo nell'apposito lettore. I titolari rimuovono il dispositivo che contiene la chiava privata dall'apposito lettore dopo ogni operazione svolta.

6.5 Controlli per la sicurezza dell'infrastruttura

L'infrastruttura è stata classificata secondo i profili di sicurezza, riservatezza e disponibilità ed è stata condotta la relativa analisi dei rischi individuando gli opportuni presìdi di sicurezza. La Banca d'Italia utilizza sistemi affidabili che garantiscono la sicurezza tecnica e l'affidabilità dei processi; gli asset sono stati configurati per innalzarne il livello di sicurezza (hardening), in particolare per i sistemi operativi dei sistemi di elaborazione, per cui tutti gli ambienti sono sottoposti ad una gestione della configurazione centralizzata, mediante la quale sono stati disabilitati tutti i servizi non necessari al funzionamento dell'infrastruttura PKI.

La Banca d'Italia assicura che i sistemi contenenti i software della CA e i relativi file siano garantiti da un accesso non autorizzato con procedure di autenticazione forte e limita l'accesso ai server di produzione.

I privilegi delle utenze sono opportunamente profilati, secondo i principi di need-to-know e least privilege. Le password delle utenze di alto privilegio sono custodite in cassaforte.

Le politiche di accesso ai sistemi di certificazione sono differenziate per le componenti core (Certification Authority e directory master) e i servizi a corredo (sistema di

registrazione degli eventi, componenti coinvolte nel Processo di Registrazione, copia Operativa del Registro dei certificati).

La copia del registro dei certificati è allocata su un sistema sicuro installato in locali protetti ed accessibile solo dal sistema di generazione dei certificati che vi registra i certificati emessi e la lista dei certificati revocati e sospesi.
La Banca d'Italia utilizza sistemi affidabili per la gestione del Registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza.
Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

La registrazione degli eventi è configurata per monitorare gli eventi di sistema al fine di diagnosticare problemi e monitorare l'esecuzione di specifici comandi.

Tutti i posti di lavoro e tutti i server dell'infrastruttura PKI sono protetti da antivirus.

6.6 Ciclo di vita dei controlli di sicurezza

La Banca d'Italia gestisce gli aspetti di sicurezza attraverso i seguenti processi che mirano a garantire un adeguato livello di protezione delle risorse informatiche rispetto ai profili di riservatezza, integrità, disponibilità, verificabilità e accountability, lungo l'intero ciclo di vita dell'infrastruttura software e hardware.

- Analisi del rischio informatico, volta all'identificazione e valutazione del rischio connesso con l'utilizzo di risorse informatiche e alla selezione delle contromisure di sicurezza idonee a garantire i livelli di sicurezza richiesti. Il processo di analisi del rischio informatico si completa attraverso lo svolgimento delle verifiche di sicurezza pre-produzione, prima del rilascio in esercizio. Le fasi del processo di analisi del rischio vengono ripetute in occasione di modifiche rilevanti al sistema o all'occorrere di incidenti significativi e, in ogni caso, periodicamente, per tenere conto dell'evoluzione del contesto tecnologico, nonché del quadro delle minacce e delle vulnerabilità.
- Gestione degli incidenti di sicurezza[22], intesa come l'insieme delle attività svolte per minimizzare l'impatto dell'incidente e garantire il tempestivo ripristino dei servizi. Il processo si basa su una procedura formale definita e periodicamente verificata che tenga conto, tra l'altro, dell'obiettivo di raccogliere e preservare tutte le informazioni utili per la ricostruzione dell'accaduto. L'attività viene completata da una fase di verifica a posteriori volta a individuare le vulnerabilità che hanno reso possibile l'incidente al fine di prevenire ulteriori accadimenti della specie.
- Gestione della continuità operativa di applicazioni e sistemi informatici, finalizzata a contenere entro un livello predeterminato e considerato accettabile l'impatto sull'organizzazione provocato da incidenti di vasta portata o da disastri e agevolare il ripristino in tempi contenuti delle normali condizioni di operatività.

[22] La violazione, o l'imminente minaccia di violazione, delle norme e delle prassi aziendali di sicurezza informatica o delle norme dell'ordinamento giuridico vigente, di livello nazionale e sovranazionale, costituiscono un incidente di sicurezza.

- Gestione dei cambiamenti relativa a qualsiasi modifica da apportare ai sistemi in esercizio, che è sottoposta a un processo formale allo scopo di garantire il mantenimento dei livelli di sicurezza previsti sia sui sistemi interessati dalla modifica sia su quelli connessi. I cambiamenti devono essere documentati e analizzati per valutare gli impatti su reputazione, compiti e patrimonio della Banca d'Italia. Per i cambiamenti più significativi viene aggiornata l'analisi dei rischi.
- Monitoraggio della sicurezza informatica, composto da diverse attività con modalità e frequenza stabilite nell'ambito dell'analisi del rischio informatico, per:
    - la verifica della conformità dei presidi di sicurezza;
    - il monitoraggio degli eventi di sicurezza significativi allo scopo di rilevare e segnalare eventuali potenziali problematiche di sicurezza;
    - l'individuazione di eventuali vulnerabilità nelle configurazioni dei sistemi.
- Processo di Vulnerability and Patch Management che ha l'obiettivo di individuare ed eliminare le nuove vulnerabilità e quindi le potenziali situazioni di rischio, al fine di preservare la confidenzialità, l'integrità e la disponibilità delle informazioni, dei servizi e delle applicazioni.

6.7 Controlli di sicurezza della rete

L'infrastruttura PKI è organizzata secondo un approccio di difesa a strati, mediante la disposizione degli elaboratori e degli apparati su livelli differenti di rete, separati tramite apparati di sicurezza in grado di consentire i soli flussi di comunicazione autorizzati (firewall). I criteri di aggregazione degli elaboratori e degli apparati nei suddetti livelli rispondono, oltre che ad una logica funzionale, al possesso di omogenei requisiti di sicurezza.

Le procedure di configurazione delle componenti di rete assicurano la gestione dei cambiamenti alle configurazioni, la restrizione dell'accesso alle componenti, la prevenzione di accessi/modifiche impropri o non autorizzati alle configurazioni. Le procedure di configurazione delle componenti di rete assicurano:

- la gestione dei cambiamenti delle configurazioni;
- accessi limitati secondo il principio del minimo privilegio;
- che siano evitati accessi o modifiche non autorizzati.

Il servizio di certificazione è basato su un'infrastruttura di sicurezza che usa meccanismi di firewalling e il protocollo TLS (Transport Layer Security) in modo da realizzare un canale sicuro tra tutti i soggetti abilitati all'accesso alla CA. Tutti i flussi di rete (protocolli, sorgente, destinazione) che transitano tra domini di sicurezza diversi sono identificati, classificati ed autorizzati. Il sistema è altresì supportato da specifici prodotti di sicurezza (anti intrusione di rete, monitoraggio, protezione da virus) e da tutte le relative procedure di gestione.
Periodicamente o dopo ogni cambiamento rilevante viene svolto un penetration test dell'infrastruttura.

L'accesso al directory master è possibile solo dalla CA. L'accesso alla copia operativa del Registro dei certificati avviene con modalità diverse a seconda che la richiesta provenga dalle reti esterne o dalla rete interna della Banca d'Italia:

- l'accesso dalla rete pubblica (Internet) è filtrato da proxy server che, dopo aver analizzato le richieste, le inoltrano alla copia operativa del Registro dei certificati;

- l’accesso dalla rete interna avviene direttamente sulla copia operativa del Registro dei certificati.

6.8 Riferimenti temporali

Certificati, lista di revoca e sospensione ed altre voci memorizzate sui database di revoca e sospensione contengono informazioni relative all’ora e alla data.

I riferimenti temporali derivano da un sistema alimentato da una sorgente esterna (ETS, External Time Source) tramite sincronizzazione satellitare GPS. Tali riferimenti corrispondono alla scala di tempo UTC (IEN).

7 PROFILI DEI CERTIFICATI, DELLA CRL, DEL OCSP

7.1 Profili dei certificati

I certificati digitali emessi dalla Banca d'Italia sono firmati con le chiavi della CA e conformi allo standard ISO/IEC X.509 v3 e alla specifica RFC 5280, che prevede una struttura dati con campi fissi e variabili in relazione all'utilizzo del certificato. In analogia alle coppie di chiavi generate, i certificati si distinguono in:

- certificato di CA, relativo alla chiave di certificazione utilizzata per la firma dei certificati di sottoscrizione e delle CRL;
- certificati ausiliari emessi per le persone fisiche (titolari), relativi a chiavi di autenticazione e crittografia.

I certificati sono generati presso l'Amministrazione Centrale della Banca d'Italia con un sistema dedicato ospitato dalla rete interna della Banca d'Italia adeguatamente protetta. L'accesso al sistema è riservato solo agli operatori autorizzati e per le funzioni a loro assegnate.
Al termine delle operazioni di generazione, il certificato è inserito nel Registro dei certificati; memorizzando la data e l'ora di emissione del certificato.

Il certificato del titolare contiene:

- il numero di serie o altro codice identificativo del certificato;
- il nome, la ragione o denominazione del prestatore di servizi e lo stato nel quale è stabilito;
- il codice identificativo del titolare presso l'Ente prestatore di servizi;
- il nome, il cognome e il codice fiscale e la data di nascita del titolare del certificato;
- l'indicazione del termine iniziale e finale di validità del certificato;
- la firma elettronica dell'Ente prestatore di servizi;
- il valore della chiave pubblica;
- gli algoritmi di generazione e verifica utilizzabili;
- l'algoritmo di firma del certificato;
- la tipologia della coppia di chiavi in base all'uso cui sono destinate;
- l'indirizzo e-mail del titolare (facoltativo);
- il luogo in cui il certificato relativo alla firma elettronica qualificata del prestatore di servizi è disponibile gratuitamente;
- l'indirizzo telematico dal quale è accessibile la CRL.

I certificati ausiliari rilasciati ai titolari hanno validità massima di 5 anni.

L'individuazione del titolare avviene mediante l'uso del Distinguished name (DN) come previsto dallo standard ISO 9594-1.
Le informazioni personali contenute nel certificato sono utilizzabili unicamente per identificare il titolare relativamente alle operazioni per cui è abilitato.
La Banca d'Italia custodisce le informazioni relative al certificato per 20 anni dalla data di emissione del certificato.

Le caratteristiche del certificato sono conformi ai requisiti dello standard ISO/IEC 9594-8.

Se il certificato è relativo a una coppia di chiavi di certificazione, è specificato l'uso delle chiavi stesse per la certificazione.

Profili del certificato della CA

Field	Value	Critical
Version	V3	
Serial Number	<serial number>	
Signing Algorithm	SHA256WithRSAEncryption	
Issuer DN	CN= Banca d'Italia CA ausiliaria OU=Servizi di certificazione ausiliari O=Banca d'Italia/00950501007 L=Roma C=IT	
SubjectPublicKeyInfo	<RSA 4096 bit PublicKey>	
Subject DN	CN= Banca d'Italia CA ausiliaria OU=Servizi di certificazione ausiliari O=Banca d'Italia/00950501007 L=Roma C=IT	
Signed By	Self Signed	
Validity (*y *mo *d) or end date of the certificate	20y	
Extensions		
Basic Constraints	IsCA	X
SubjectKeyIdentifier (SKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	
KeyUsage	Certificate Signing, CRL Signing , Off-line CRL Signing	X
CertificatePolicies	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale	
Default CRL Dist. Point	URL=http://www.certificazione.bancaditalia.it/crl/crlaus.crl URL=ldap://ldap.certificazione.bancaditalia.it/cn=Banca%20d'Italia%20CA%20ausiliaria,ou=Servizi%20di%20certificazione%20ausiliari,o=Banca%20d'Italia/00950501007,l=Roma,c=IT?certificateRevocationList	

Profili dei certificati dei titolari

Employees		
Field	**Encryption**	**Authentication**
Version	V3	V3
Serial Number	<random bytes>	<random bytes>
Signature	SHA256WithRSAEncryption	SHA256WithRSAEncryption
Issuer	CN = Banca d'Italia CA ausiliaria OU = Servizi di certificazione ausiliari O = Banca d'Italia/00950501007 L=Roma C = IT	CN = Banca d'Italia CA ausiliaria OU = Servizi di certificazione ausiliari O = Banca d'Italia/00950501007 L=Roma C = IT
Validity	<5 y>	<5 y>
Subject	SERIALNUMBER = TIN<Country Code>-<Tax identification number> CN = <Last Name Name> G = <Name> SN = < Last Name> dnQualifier = <IUT> O = Banca d'Italia/00950501007 C = <Country>	SERIALNUMBER = TIN<Country Code>-<Tax identification number> CN = <Last Name Name > G = <Name> SN = < Last Name> dnQualifier = <IUT> O = Banca d'Italia/00950501007 C = <Country>
SubjectPublicKeyInfo	<RSA 2048 bit PublicKey>	<RSA 2048 bit PublicKey >
Extensions		
AuthorityKeyIdentifier (AKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>
SubjectKeyIdentifier (SKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>
KeyUsage	Digital Signature, Key Encipherment	Digital Signature, key Encipherment
Extended KEyUsage	Email protection	Client Authentication Smart card Logon
SubjectAlternateName (SAN)	Name RFC822=<subscriber email> User Principal Name = userid@domain	Name RFC822=<subscriber email> User Principal Name = userid@domain
Certificate Policies	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale

	[2]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2.2 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [2,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso=I titolari fanno uso del certificato solo per le finalita' di lavoro per le quali esso e' rilasciato. The holder must use the certificate only for the purposes for which it is issued.	[2]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2.1 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [2,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso=I titolari fanno uso del certificato solo per le finalita' di lavoro per le quali esso e' rilasciato. The holder must use the certificate only for the purposes for which it is issued.
AuthorityInformationAccess (AIA)	[1]Accesso alle informazioni sull'autorità Metodo di accesso=Autorità emittente il certificato (1.3.6.1.5.5.7.48.2) Nome alternativo: URL=http://www.bancaditalia.it/footer/firmadigitale/BdI_CA_ausiliaria.cer [2]Accesso alle informazioni sull'autorità Metodo di accesso=Protocollo di stato del certificato online (1.3.6.1.5.5.7.48.1) Nome alternativo: URL=http://ocsp.certificazione.bancaditalia.it/ocsp	[1]Accesso alle informazioni sull'autorità Metodo di accesso=Autorità emittente il certificato (1.3.6.1.5.5.7.48.2) Nome alternativo: URL=http://www.bancaditalia.it/footer/firmadigitale/BdI_CA_ausiliaria.cer [2]Accesso alle informazioni sull'autorità Metodo di accesso=Protocollo di stato del certificato online (1.3.6.1.5.5.7.48.1) Nome alternativo: URL=http://ocsp.certificazione.bancaditalia.it/ocsp
CRLDistributionPoints (CDP)	URL=http://www.certificazione.bancaditalia.it/crl/crlaus.crl URL=ldap://ldap.certificazione.bancaditalia.it/cn=Banca%20d'Italia%20CA%20ausiliaria,ou=Servizi%20di%20certificazione%20ausiliari,o=Banca%20d'Italia/00950501007,l=Roma,c=IT?certificateRevocationList	URL=http://www.certificazione.bancaditalia.it/crl/crlaus.crl URL=ldap://ldap.certificazione.bancaditalia.it/cn=Banca%20d'Italia%20CA%20ausiliaria,ou=Servizi%20di%20certificazione%20ausiliari,o=Banca%20d'Italia/00950501007,l=Roma,c=IT?certificateRevocationList

Externals		
Field	**Encryption**	**Authentication**
Version	V3	V3
Serial Number	<random bytes>	<random bytes>

Signature	SHA256WithRSAEncryption	SHA256WithRSAEncryption
Issuer	CN = Banca d'Italia CA ausiliaria OU = Servizi di certificazione ausiliari O = Banca d'Italia/00950501007 L=Roma C = IT	CN = Banca d'Italia CA ausiliaria OU = Servizi di certificazione ausiliari O = Banca d'Italia/00950501007 L=Roma C = IT
Validity	<5 y>	<5 y>
Subject	SERIALNUMBER = TIN<Country Code>-<Tax identification number> CN = <Last Name Name> G = <Name> SN = < Last Name> dnQualifier = <IUT> C = IT	SERIALNUMBER = TIN<Country Code>-<Tax identification number> CN = <Last Name Name > G = <Name> SN = < Last Name> dnQualifier = <IUT> C = IT
SubjectPublicKeyInfo	<RSA 2048 bit PublicKey>	< RSA 2048 bit PublicKey >
Extensions		
AuthorityKeyIdentifier (AKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>
SubjectKeyIdentifier (SKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>
KeyUsage	Digital Signature, Key Encipherment	Digital Signature, key Encipherment
Extended KEyUsage	Email protection	Client Authentication Smart card Logon
SubjectAlternateName (SAN)	Name RFC822=<subscriber email> User Principal Name = userid@domain	Name RFC822=<subscriber email> User Principal Name = userid@domain
Certificate Policies	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2.2 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [2,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.3.2.1 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [2,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente

	Definizione: Testo avviso=L'utilizzo del certificato e' limitato ai rapporti con la Banca d'Italia. The certificate may be used only for relations with the Bank of Italy	Definizione: Testo avviso=L'utilizzo del certificato e' limitato ai rapporti con la Banca d'Italia. The certificate may be used only for relations with the Bank of Italy
AuthorityInformationAccess (AIA)	[1]Accesso alle informazioni sull'autorità Metodo di accesso=Autorità emittente il certificato (1.3.6.1.5.5.7.48.2) Nome alternativo: URL=http://www.bancaditalia.it/footer/firmadigitale/BdI_CA_ausiliaria.cer [2]Accesso alle informazioni sull'autorità Metodo di accesso=Protocollo di stato del certificato online (1.3.6.1.5.5.7.48.1) Nome alternativo: URL=http://ocsp.certificazione.bancaditalia.it/ocsp	[1]Accesso alle informazioni sull'autorità Metodo di accesso=Autorità emittente il certificato (1.3.6.1.5.5.7.48.2) Nome alternativo: URL=http://www.bancaditalia.it/footer/firmadigitale/BdI_CA_ausiliaria.cer [2]Accesso alle informazioni sull'autorità Metodo di accesso=Protocollo di stato del certificato online (1.3.6.1.5.5.7.48.1) Nome alternativo: URL=http://ocsp.certificazione.bancaditalia.it/ocsp
CRLDistributionPoints (CDP)	URL=ldap://ldap.certificazione.bancaditalia.it/cn=Banca%20d'Italia%20CA%20ausiliaria,ou=Servizi%20di%20certificazione%20ausiliari,o=Banca%20d'Italia/00950501007,l=Roma,c=IT?certificateRevocationList URL=http://www.certificazione.bancaditalia.it/crl/crlaus.crl	URL=ldap://ldap.certificazione.bancaditalia.it/cn=Banca%20d'Italia%20CA%20ausiliaria,ou=Servizi%20di%20certificazione%20ausiliari,o=Banca%20d'Italia/00950501007,l=Roma,c=IT?certificateRevocationList URL=http://www.certificazione.bancaditalia.it/crl/crlaus.crl

7.2 Profilo della CRL

Il Registro dei certificati contiene i certificati emessi dalla Banca d'Italia e la lista dei certificati revocati e sospesi. La revoca, la sospensione e la successiva riattivazione dei certificati sono annotate con l'indicazione della data e dell'ora di esecuzione dell'operazione. Del Registro dei certificati (cd. directory master) esistono una o più copie operative (cd. directory shadow). Il directory master è aggiornato ad ogni richiesta di emissione, sospensione e revoca di certificati; la copia operativa replica il contenuto della copia di riferimento. Tutte le operazioni che modificano il contenuto del directory master sono registrate; le copie operative sono aggiornate ogni volta che viene aggiornato il directory master.
Il directory master, che non è accessibile dall'esterno, è allocato su un'infrastruttura sicura all'interno della rete della Banca d'Italia a cui accede solo la CA per registrare i certificati emessi e la lista dei certificati revocati e sospesi. Alla copia operativa si accede anche dall'esterno.

La pubblicazione della CRL avviene al massimo ogni 24 ore. La revoca del certificato avviene entro un'ora dall'identificazione del richiedente e della verifica dell'autenticità della richiesta.

La CRL è conforme allo standard internazionale ISO/IEC 9594-8 X.509 v2 e alla specifica pubblica RFC 5280 ed è firmata con algoritmo sha256WithRSAEncryption. Oltre ai dati obbligatori, la CRL contiene:

- il campo nextUpdate (data prevista per la prossima emissione della CRL);
- l'estensione CRLNumber (identificativo della versione della CRL).

Inoltre, in corrispondenza di ogni voce della CRL è presente l'estensione reasonCode che indica la motivazione della sospensione o revoca.

L'accesso alla CRL è disponibile agli indirizzi Internet sotto riportati:

- OCSP - http://ocsp.certificazione.bancaditalia.it/ocsp
- HTTP - http://www.certificazione.bancaditalia.it/crl/crlaus.crl
- LDAP: ldap://ldap.certificazione.bancaditalia.it/cn=Banca%20d'Italia%20CA%20ausiliaria,ou=Servizi%20di%20certificazione%20ausiliari%20,o=Banca%20d'Italia/00950501007,L=Roma,c=IT?certificateRevocationList [23].

7.3 Profilo del OCSP[24]

L'OCSP di Banca d'Italia è conforme alla specifica RFC 6960, 2560 e 5019.
Le chiavi di firma dell'OCSP response sono custodite in una partizione dedicata dell'HSM e separata da quella contenente le chiavi di root CA.
L'accesso al servizio OCSP è disponibile all'indirizzo Internet http://ocsp.certificazione.bancaditalia.it/ocsp.

[23] L'accesso alla copia operativa del Registro dei certificati avviene secondo il protocollo LDAP come definito nelle specifiche pubbliche RFC 1777 e successivi aggiornamenti, ovvero tramite indicazione della URL secondo quanto definito nella norma RFC 2255.
[24] Online Certificate Status Protocol, protocollo per ottenere informazioni tempestive sullo stato di revoca di un determinato certificato.

8 Valutazioni di conformità

8.1 Frequenza e condizioni delle valutazioni

Nell’ambito del Sistema Europeo delle Banche Centrali (ESCB), la CA Ausiliaria è sottoposta ad una valutazione della conformità al ESCB Certificate Acceptance Framework almeno ogni 3 anni.

8.2 Identità/qualifica dei valutatori

Le verifiche sono svolte da soggetti indipendenti dalla Banca d'Italia.

8.3 Relazione fra valutatori e ente valutato

Non esiste alcuna relazione societaria o professionale pregressa tra la Banca d’Italia e gli auditor esterni che possa in alcun modo influenzare l’esito delle verifiche svolte.

8.4 Argomenti considerati dalla valutazione

La valutazione di conformità svolta dagli auditor esterni è finalizzata a verificare la conformità della Banca d’Italia e dei servizi forniti ai requisiti dello schema di accreditamento.

8.5 Azioni da intraprendere a seguito di mancanza di conformità

Nel caso di non-conformità, la Banca d’Italia adotta le necessarie misure correttive.

8.6 Comunicazione dei risultati

La valutazione di conformità è inviata alla funzione competente della Banca d’Italia responsabile del servizio di certificazione.

9 ALTRI ASPETTI

9.1 Tariffe

Non è prevista l'applicazione di tariffe.

9.2 Responsabilità finanziaria

Riguardo alla responsabilità civile per danni la Banca d'Italia mantiene risorse finanziarie adeguate nell'ambito degli accantonamenti presenti nelle pertinenti voci del proprio bilancio.

9.3 Riservatezza delle informazioni

Il trattamento dei dati è effettuato secondo processi prevalentemente automatizzati curati da operatori autorizzati che accedono ai dati previa autenticazione, nel rispetto delle policy di sicurezza definite dalla Banca d'Italia.
Tutte le informazioni sui titolari non disponibili al pubblico attraverso il certificato o la lista di revoca e sospensione online sono trattate come riservate. In particolare:

- i dati del titolare e relative richieste di emissione;
- le chiavi private conservate dai titolari e le informazioni necessarie per il recupero di tali chiavi private;
- i dati transazionali (sia record completi, che le tracce di audit sulle operazioni);
- i piani d'emergenza e i piani di disaster recovery;
- le misure di sicurezza delle operazioni hardware e software relative ai servizi di certificazione.

I documenti e le informazioni sul servizio di certificazione raggiungibili dal sito www.bancaditalia.it/firmadigitale sono pubblici.

I dipendenti della Banca d'Italia sono vincolati dal segreto professionale. Il personale esterno alla Banca d'Italia che collabora allo svolgimento del servizio di certificazione della PKI è tenuto al segreto professionale nell'ambito degli obblighi contrattuali con la Banca d'Italia.

9.4 Profili di privacy delle informazioni personali

Le misure di protezione delle informazioni personali dei titolari dei certificati adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali previste dalla normativa europea e nazionale in materia di protezione dei dati personali e successive modifiche e integrazioni.

La Banca d'Italia ha il diritto di rivelare informazioni riservate/confidenziali in risposta a procedimenti giudiziari e amministrativi.

9.5 Diritti di proprietà intellettuale

La Banca d'Italia ha la proprietà intellettuale di tutti i certificati elettronici emessi dalla CA; della lista di revoca e sospensione dei certificati; del CPS e delle CP. Inoltre, la Banca

d'Italia è titolare dei diritti relativi a qualsiasi altro tipo di documento, protocollo, programma informatico e hardware, file, directory, database e servizio di consultazione che possono essere generati o utilizzati per le attività inerenti la PKI.

Gli OID utilizzati sono di proprietà della Banca d'Italia e sono stati registrati presso l'ente nazionale competente per il rilascio di tali codici (UNINFO). Nessun OID assegnato a Banca d'Italia può essere utilizzato da altri soggetti, parzialmente o totalmente, fatta eccezione degli usi consentiti, come specificato nel certificato.

9.6 Obblighi e responsabilità

Obblighi del prestatore di servizi

La Banca d'Italia:

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
2. identifica con certezza la persona che effettua la richiesta di certificazione;
3. si accerta dell'autenticità della richiesta;
4. specifica nel certificato, su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;
5. informa i richiedenti in modo compiuto e chiaro sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso dei certificati;
6. procede alla tempestiva pubblicazione della revoca e della sospensione del certificato in caso di richiesta da parte del titolare o del terzo interessato, di perdita del possesso o della compromissione del dispositivo che contiene le chiavi private, di provvedimento dell'autorità giudiziaria, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni;
7. garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati emessi, sospesi e revocati;
8. assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
9. tiene la registrazione di tutte le informazioni relative al certificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
10. non copia, né conserva le chiavi private di autenticazione del titolare del certificato;
11. predispone su mezzi di comunicazione durevoli e rende disponibili ai richiedenti il servizio di certificazione tutte le informazioni utili, tra cui in particolare gli esatti termini e condizioni relativi all'uso del certificato, compresa ogni limitazione dell'uso;
12. utilizza sistemi affidabili per la gestione del Registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

13. registra l'emissione dei certificati con la specificazione della data e dell'ora della generazione; il momento della generazione dei certificati è attestato tramite riferimento temporale;
14. revoca o sospende il certificato ove abbia notizia della compromissione della chiave privata o del dispositivo che contiene la chiave privata;
15. adotta adeguate misure di sicurezza per il trattamento dei dati personali, ai sensi del Regolamento eIDAS e dalla normativa europea e nazionale in materia di protezione dei dati personali;
16. registra i seguenti eventi significativi:
    - gli eventi di gestione del ciclo di vita del certificato e delle chiavi di CA;
    - gli eventi di gestione del ciclo di vita dei certificati e delle chiavi dei titolari;
    - gli eventi di gestione del ciclo di vita dei supporti crittografici;
    - gli eventi relativi alla sicurezza;
17. dispone di un piano di cessazione che prevede, con congruo anticipo rispetto alla dismissione del servizio, la notifica ai soggetti istituzionali rilevanti e ai titolari di detto evento e che assicura un servizio con cui rendere disponibili le informazioni sullo stato di revoca dei certificati.

Obblighi del titolare

Il titolare è tenuto ad assicurare la custodia del dispositivo che contiene la chiave privata e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri nonché a utilizzare personalmente il dispositivo.

Il titolare del certificato, secondo le modalità indicate nel presente documento, deve altresì:

1. fornire tutte le informazioni richieste dalla Banca d'Italia, garantendone l'attendibilità sotto la propria responsabilità;
2. comunicare alla Banca d'Italia eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica (e-mail), ecc.;
3. conservare con la massima diligenza e separatamente il dispositivo che contiene la chiave privata e i codici segreti (PIN, PUK e pass-phrase) ricevuti dalla Banca d'Italia, al fine di garantirne l'integrità e la massima riservatezza;
4. non utilizzare la coppia di chiavi per funzioni e finalità diverse da quelle per le quali il certificato è stato emesso;
5. inoltrare alla Banca d'Italia le richieste di rinnovo, sospensione, riattivazione e revoca secondo le procedure riportate nel presente CPS/CP;
6. richiedere immediatamente la sospensione dei certificati relativi alle chiavi contenute in dispositivi difettosi o di cui abbia perduto il possesso;
7. comunicare alla Banca d'Italia lo smarrimento o la sottrazione del dispositivo di sicurezza che contiene la chiave privata.

Obblighi del terzo interessato

Il terzo interessato ha l'obbligo di chiedere la revoca e la sospensione dei certificati, secondo le modalità indicate nel presente documento, ogniqualvolta vengano meno i presupposti in base ai quali il certificato è stato rilasciato al titolare ovvero in caso di cessazione della propria attività (per operazioni di fusione, liquidazione ecc.).
Inoltre - fermi restando gli obblighi e le responsabilità che fanno capo al titolare dei certificati - il terzo, in quanto soggetto nel cui interesse è svolto il servizio di certificazione, adotta tutte le cautele e le misure organizzative funzionali a un utilizzo dei certificati conforme alle prescrizioni previste dalla legge e dal CPS/CP.
Il terzo interessato ha altresì l'obbligo di comunicare tempestivamente alla Banca d'Italia ogni modifica delle circostanze, indicate al momento del rilascio del certificato, rilevanti ai fini del suo utilizzo.

Obblighi dei richiedenti

I richiedenti la verifica di un certificato devono controllare:

1. la validità del certificato;
2. l'assenza del certificato dalla lista dei certificati revocati e sospesi;
3. l'esistenza ed il rispetto di eventuali limitazioni all'uso del certificato utilizzato dal titolare.

9.7 Limitazioni degli obblighi

Confronta paragrafo 9.8.

9.8 Limitazioni delle responsabilità

La Banca d'Italia non assume responsabilità:

- per le conseguenze derivanti dal mancato rispetto, da parte del titolare del certificato, delle procedure e delle modalità operative specificate nel CPS/CP;
- per le conseguenze derivanti da un uso dei certificati diverso da quello consentito e in particolare per i danni derivanti dall'uso dei certificati che ecceda i limiti posti dallo stesso;
- per il mancato adempimento degli obblighi previsti a suo carico dovuto a cause ad essa non imputabili.

La Banca d'Italia è esclusivamente responsabile dell'adempimento di tutti gli obblighi previsti dalla legge e richiamati nel presente documento.

In particolare, la Banca d'Italia è responsabile, se non prova di aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:

- sull'esattezza e sulla completezza delle informazioni necessarie alla verifica delle informazioni contenute nel certificato alla data del rilascio e sulla loro completezza;
- sulla garanzia che al momento del rilascio del certificato il titolare detenesse i dati per la creazione del certificato corrispondenti ai dati per la verifica dello stesso.

La Banca d'Italia è inoltre responsabile dei danni provocati ai terzi per effetto della mancata o non tempestiva registrazione della revoca o della non tempestiva sospensione del certificato.

9.9 Indennità

Riguardo alla responsabilità civile per danni la Banca d'Italia mantiene risorse finanziarie adeguate nell'ambito degli accantonamenti presenti nelle pertinenti voci del proprio bilancio.

9.10 Durata e termine del documento

Il presente CPS/CP è il documento di riferimento per i titolari che abbiano un certificato rilasciato dalla Banca d'Italia in corso di validità ed entra in vigore dal momento in cui viene pubblicato sul sito Internet della Banca d'Italia e rimane valido finché non sia rilasciata una nuova versione del CPS/CP o sia cessato il servizio di certificazione.

9.11 Comunicazioni con le controparti

Tutte le notifiche e le richieste o altre tipologie di comunicazioni sono effettuate dalla Banca d'Italia tramite e-mail o servizio di recapito certificato (PEC).

I titolari comunicano con la Banca d'Italia con le modalità descritte nei capitoli 3 e 4.

I contatti della Banca d'Italia cui fare riferimento sono contenuti nel paragrafo 1.5.

9.12 Modifiche delle condizioni

Eventuali modifiche al presente documento sono effettuate tramite suoi aggiornamenti integrali o parziali.

Le nuove versioni sono indicate con un numero intero seguito da un decimale uguale a zero. Le modifiche minori sono indicate con un numero decimale maggiore di zero.

Le nuove versioni sono rese disponibili agli utenti nel sito Internet della Banca d'Italia.

9.13 Risoluzione delle controversie

Foro competente per la risoluzione delle controversie legate allo svolgimento del servizio di certificazione è quello di Roma.

9.14 Legge applicabile

La Banca d'Italia si attiene alle disposizioni in materia previste dal Codice dell'Amministrazione Digitale, D.Lgs. 82/2005 e successive modifiche e integrazioni.

In materia di riservatezza, la Banca d'Italia adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi della normativa europea e nazionale in materia di protezione dei dati personali.

9.15 Conformità del servizio alla legislazione vigente

La Banca d'Italia svolge il servizio di certificazione delle chiavi pubbliche conformemente alla normativa di cui al paragrafo precedente.

La Banca d'Italia si sottopone a proprie spese a una verifica da parte di un organismo di valutazione della conformità di cui al paragrafo 8.1.

9.16 Disposizioni di altro tipo

Non ci sono ulteriori disposizioni rispetto a quanto riportato nei precedenti paragrafi del presente documento.

9.17 Altre disposizioni

Non ci sono ulteriori disposizioni rispetto a quanto riportato nei precedenti paragrafi del presente documento.