BANCA D'ITALIA
EUROSISTEMA

SERVIZIO DI CERTIFICAZIONE A CHIAVE PUBBLICA PER LA FIRMA ELETTRONICA QUALIFICATA

PUBLIC KEY INFRASTRUCTURE (PKI)

DOCUMENTO DI SINTESI

(DISCLOSURE STATEMENT)

Versione 1.1 - 15/06/2017

La Banca d'Italia svolge il servizio di certificazione delle chiavi pubbliche per l'emissione di certificati di firma elettronica qualificata, anche in modalità remota e automatica[1], e per la gestione del loro ciclo di vita.

Il servizio si basa su una infrastruttura tecnico-organizzativa 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 e il ciclo di vita dei certificati e le liste di revoca e sospensione.

Il servizio è svolto in conformità:

- al "Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno" (nel seguito eIDAS) e relativi standard europei;
- alle disposizioni nazionali previste dal Codice dell'Amministrazione Digitale e delle "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" di cui al Decreto del Presidente del Consiglio dei Ministri del 22.02.2013 (DPCM 22.02.2013).

I certificati sono emessi per i seguenti soggetti[2]:

- 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.

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

[1] La "firma remota" è una modalità di firma digitale eseguita con una chiave privata non residente su un dispositivo personale dell'utente (ad es. una smart card) bensì su un apparato hardware sicuro remoto (normalmente un HSM – Hardware Security Module). I dati da firmare, corrispondenti all'impronta calcolata a partire dal documento originale, sono inviati allo HSM su un canale di comunicazione sicuro.
La "firma automatica" consente ad un'applicazione, previa abilitazione del titolare, di apporre la firma digitale per conto di questo ultimo in modo "massivo" su una serie di documenti.

[2] Ai sensi del Codice dell'amministrazione digitale (D. Lgs. 82/2005, art. 34 "Norme particolari per le pubbliche amministrazioni", comma 1).

1. Caratteristiche generali del servizio e contatti del prestatore di servizi

Il ruolo di CA è svolto dalla Banca d'Italia attraverso una componente tecnologica denominata "Servizi di certificazione". Il certificato della CA ha durata ventennale ed è consultabile, con la relativa impronta, sul sito della Banca http://www.bancaditalia.it/firmadigitale, dove sono altresì disponibili:

- il Certification Practice Statement (CPS), che definisce le procedure operative seguite dalla Banca d'Italia (nel seguito Prestatore di servizi fiduciari qualificato) per l'emissione e la gestione del ciclo di vita dei certificati di firma elettronica qualificata rilasciati dalla Certification Authority della Banca d'Italia nonché per l'utilizzo degli stessi. Nel CPS sono anche dettagliati gli obblighi e le responsabilità dei diversi attori e le misure di sicurezza fisiche e logiche previste dal servizio di certificazione;
- le Certificate Policy (CP), che specificano i requisiti e le regole per l'utilizzo dei certificati di firma elettronica qualificata nei diversi contesti.

Il ruolo di Registration Authority (RA) è svolto dalla Banca d'Italia in modalità decentrata – 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 RA deve essere inteso secondo lo schema seguente.

Strutture della Banca d'Italia che agiscono come RA	Richiedente
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	Dipendenti
Servizio Organizzazione	Per le richieste di firma remota o automatica da parte di soggetti che hanno già un certificato di firma qualificata rilasciato dalla Banca d'Italia

Un interlocutore istituzionale (ente o persona giuridica, nel seguito terzo interessato) può chiedere l'emissione di un certificato qualificato 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.

Il titolare del certificato o il terzo interessato possono chiedere alla RA competente la revoca del certificato nei termini descritti al paragrafo 2.

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

Dati identificativi del Prestatore di servizi fiduciari qualificato

Denominazione	Banca d'Italia
Indirizzo della sede legale	Via Nazionale, 91 – 00184 ROMA
Legale Rappresentante	Governatore pro tempore
PEC	org@pec.bancaditalia.it
e-mail	pki@bancaditalia.it
Indirizzo internet	www.bancaditalia.it/firmadigitale
Telefono	06/47921

Richieste di informazioni o chiarimenti possono essere inoltrate ai seguenti contatti.

Responsabile del Certification Practice Statement

Nome	Fabio
Cognome	Bolognesi
PEC	org@pec.bancaditalia.it
e-mail	fabio.bolognesi@bancaditalia.it

2. Tipi di certificati, usi consentiti e procedura di validazione

I certificati digitali emessi dalla Banca d'Italia sono firmati con le chiavi della CA e conformi allo standard ISO/IEC 9594-8 X.509 v3 e alla specifica RFC 5280, che prevede una struttura dati con campi fissi e variabili in relazione all'utilizzo del certificato. Detti certificati sono inoltre conformi alla deliberazione CNIPA 45/2009 e a quanto previsto dallo standard ETSI EN 319 412. 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 dei titolari e della lista di revoca (CRL - Certificate Revocation List);
- certificati di firma elettronica qualificata per le persone fisiche (titolari).

Il certificato del titolare, conformemente ai requisiti dell'allegato I del Regolamento eIDAS e alla Deliberazione CNIPA 45/2009 ove applicabile, contiene:

- l'indicazione che il certificato è qualificato;

- 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 (in mancanza, per i residenti all'estero, il codice fiscale rilasciato dall'Autorità fiscale del Paese di residenza o un analogo codice identificativo) 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 è destinata;
- 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;
- l'indicazione che i dati per la creazione di una firma elettronica connessi ai dati di convalida della firma elettronica sono presenti in un dispositivo per la creazione di una firma elettronica qualificata.

Le informazioni personali contenute nel certificato sono utilizzabili unicamente per identificare il titolare relativamente alle operazioni che è abilitato a compiere, fermo restando che l'utilizzo del certificato è limitato ai rapporti con la Banca d'Italia.

I certificati sono validi per 5 anni. La Banca d'Italia custodisce le informazioni relative al certificato per un periodo non inferiore a 20 anni dalla data di scadenza o revoca del certificato.

Ulteriori dettagli sui profili del certificato sono riportati nel CPS/CP.

2.1. Richieste relative ai certificati di firma qualificata con utilizzo di un dispositivo sicuro in possesso del titolare

Nel seguito si descrivono le procedure operative per le richieste di emissione, sospensione e revoca dei certificati. Per le altre tipologie di richieste inerenti il ciclo di vita dei certificati si fa rimando al CPS/CP.

I moduli per presentare le richieste sono disponibili sul sito http://www.bancaditalia.it/firmadigitale.

Emissione

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. contenere l'attestazione che il richiedente ha ricevuto l'informativa di cui all'art. 13 del D. Lgs. 196/2003;
d. essere corredata di una copia di un valido documento di riconoscimento del richiedente nonché di copia del tesserino contenente il codice fiscale[3] (solo per i soggetti esterni).

Nel caso la richiesta provenga da interlocutori istituzionali (cosiddetto terzo interessato) a favore di proprio personale, il terzo interessato invia una nota di designazione, sottoscritta dal legale rappresentante dell'ente ovvero da altro soggetto a ciò delegato, che 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[4] alla RA competente.

La RA esamina la documentazione ricevuta e, dopo la fase di convalida gestita tramite un sistema di registrazione[5], inoltra le richieste alla CA per l'emissione del certificato.

Una volta emesso il certificato, il dispositivo crittografico qualificato per la firma (smartcard/token USB) viene consegnato al titolare tramite la RA che ha ricevuto la richiesta.

Le informazioni fornite sono trattate mediante procedure informatiche con logiche strettamente correlate alle finalità sopra descritte e con l'impiego di misure di sicurezza

[3] In caso di sottoscrizione con firma digitale non è richiesto alcun documento allegato.

[4] Tramite servizio di recapito certificato (PEC) o da casella di posta elettronica convenzionale, sottoscrivendo la richiesta con firma elettronica qualificata basata su un certificato rilasciato da un prestatore di servizi fiduciari qualificato. Nel caso non fosse possibile utilizzare una firma qualificata, mediante una casella PEC allegando una fotocopia di un valido documento di identificazione del titolare. 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, con posta ordinaria o con consegna a mani, allegando una fotocopia di un valido documento di identificazione del titolare.

[5] Suite applicativa utilizzata per la gestione del flusso delle richieste (emissione, sospensione, rinnovo, riattivazione e revoca dei certificati dei titolari), accessibile solo dal personale della Banca d'Italia abilitato.

idonee a garantire la riservatezza dei dati personali nonché ad evitare l'indebito accesso ai dati ai sensi del D. Lgs. 196/2003.

Sospensione o revoca

Il titolare o il terzo interessato possono chiedere alla RA competente, con apposito modulo, la sospensione o la revoca del certificato al verificarsi delle causali riepilogate nella tabelle seguenti.

Sospensione

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[6]	X	X	X

Revoca

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[7] (previa sospensione)	X	-	-
DETERIORAMENTO DELLA SMARTCARD	X	X	X
MODIFICA DELLA POSIZIONE TITOLARE[8]	-	X	X

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

[7] 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.

[8] Causale da utilizzare ad esempio in caso di cessazione del titolare dall'attività lavorativa.

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[9] (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).

In caso di smarrimento, 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, non venga chiesta dallo stesso soggetto che ha chiesto la sospensione, l'attivazione o la revoca del certificato.

Per i dipendenti della Banca d'Italia, la richiesta è comunicata alla RA dal titolare o dalla Struttura presso la quale questi presta servizio.

Per i soggetti esterni, la richiesta di revoca dovrà essere presentata alla competente RA[10] dal titolare o dal terzo interessato; in tal caso 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 l'emissione di un nuovo certificato.

I certificati sono sospesi o revocati da parte della Banca d'Italia mediante inserimento del relativo numero identificativo (serial number) nella CRL.

---

[9] 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 nota all'utente.

[10] Tramite servizio di recapito certificato (PEC) o da casella di posta elettronica convenzionale, sottoscrivendo la richiesta con firma elettronica qualificata basata su un certificato rilasciato da un prestatore di servizi fiduciari qualificato. Nel caso non fosse possibile utilizzare una firma qualificata, mediante una casella PEC allegando una fotocopia di un valido documento di identificazione del titolare. 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 o in un suo allegato. Qualora non siano possibili le modalità precedenti, con posta ordinaria o con consegna a mani, allegando una fotocopia di un valido documento di identificazione del titolare.

La sospensione e la revoca sono efficaci a partire dal momento dell'inserimento dei certificati nella suddetta lista (per ulteriori dettagli, consultare il CPS/CP).

Un certificato revocato non può essere in nessun caso ripristinato.

La sospensione e la revoca dei certificati sono annotate nel Giornale di controllo 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 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.

I certificati possono essere infine sospesi o revocati dalla Banca d'Italia nei casi previsti dall'art. 36 del D. Lgs. 82/2005[11].

2.2. Richieste relative ai certificati di firma qualificata della tipologia "remota" e "automatica"

Emissione

Le richieste di certificati di firma remota e automatica sono avanzate al Servizio Organizzazione da titolari, di norma dipendenti della Banca d'Italia, che hanno già un certificato di firma qualificata (cfr. par. 1). L'istanza è inviata con mail firmata digitalmente. A seguito delle richieste, i titolari ricevono in modalità cifrata le credenziali (PIN, codice di attivazione per la generazione di una OTP – One Time Password[12]) per l'attivazione della chiave privata contenuta in un apparato hardware sicuro (HSM - Hardware Security Module) custodito dalla CA in locali protetti.

Le istanze relative alla firma automatica devono specificare il nome dell'applicazione delegata a firmare per conto del titolare. A seguito di tali istanze, il titolare riceve in modalità cifrata un PIN con il quale autorizzare, attraverso un'applicazione web dedicata, una procedura informatica della Banca d'Italia deputata ad apporre la firma per suo conto.

L'emissione dei certificati di firma in modalità remota o automatica avviene, a seguito della convalida della registrazione, con un processo completamente automatizzato, su canali di comunicazione sicuri, al termine del quale la chiave privata di firma del titolare è memorizzata nell'HSM.

---

[11] Cessazione dell'attività del certificatore; esecuzione di un provvedimento dell'autorità; a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare; in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

[12] Il servizio di firma remota richiede che il titolare del certificato debba autenticarsi in maniera forte all'infrastruttura di firma, al fine di procedere alla sottoscrizione dello specifico documento. Per la generazione del codice OTP è necessario utilizzare un'apposita app su dispositivo mobile (smartphone) da configurare con il codice di attivazione (*seed*).

Revoca

Data la particolarità dei certificati di firma remota, la revoca può essere richiesta:

- qualora il PIN non sia più recuperabile;
- in caso di variazione della situazione lavorativa del titolare.

Per la firma automatica la revoca è richiesta solo in caso di variazione della situazione lavorativa del titolare.

Limitatamente alla firma remota, qualora invece si verifichi lo smarrimento o il furto del dispositivo mobile che genera il codice OTP, è sufficiente richiedere la sospensione cautelativa del certificato e procedere all'installazione dell'app per la generazione degli OTP su un nuovo dispositivo mobile.

La richiesta di sospensione/riattivazione o revoca del certificato è avanzata dal titolare alla RA con mail sottoscritta digitalmente.

3. Presidi per la gestione e la conservazione sicura delle registrazioni

Tutte le registrazioni e le informazioni relative ai certificati qualificati, nonché tutti gli eventi connessi al loro ciclo di vita sono conservati dalla Banca d'Italia, anche dopo la cessazione delle attività, per almeno 20 anni[13], ciò al fine di fornire prova in eventuali procedimenti.

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 controlli di accessi fisici e logici.

Tutti gli eventi sono registrati ai sensi del Regolamento eIDAS, sulla base delle normative nazionali in materia (DPCM 22.02.2013) e della legge sulla privacy; 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 principali attività di auditing sulle componenti dell'infrastruttura sono svolte effettuando interrogazioni sugli eventi raccolti dal Giornale di controllo, che registra in modo automatico gli eventi rilevanti ai fini della sicurezza.

4. Obblighi del titolare

Si descrivono di seguito gli obblighi cui sono tenuti i titolari dei certificati di firma, fatte salve le specificità connesse alla tipologia remota e automatica per le quali il titolare non ha il possesso di un dispositivo di firma.

[13] Ai sensi sia del Regolamento eIDAS (art. 24, co 2, lett. H) sia del CAD (art 32, co. 3, lett. J).

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

Il titolare del certificato, secondo le modalità indicate nel CPS/CP, 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 sospensione, riattivazione e revoca secondo le procedure riportate nel CPS/CP;
6. richiedere immediatamente la sospensione dei certificati qualificati 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.

4.1. Obblighi del terzo interessato

Il terzo interessato ha l'obbligo di chiedere la revoca e la sospensione dei certificati, secondo le modalità indicate nel CPS/CP, 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.

5. Obblighi per i richiedenti la verifica delle firme

I richiedenti la verifica delle firme 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 verificabili attraverso la consultazione delle lista dei certificati revocati e sospesi con i seguenti protocolli:

- OCSP, http://ocsp.firmadigitale.bancaditalia.it/ocsp
- HTTP, http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
- LDAP: ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList.

I destinatari dei documenti informatici firmati digitalmente devono verificare:

1. la validità del certificato;
2. l'assenza del certificato dalla lista dei certificati revocati e sospesi (cfr. par. 2.1);
3. l'esistenza ed il rispetto di eventuali limitazioni all'uso del certificato utilizzato dal titolare.

6. Limitazione di garanzia ed esonero di responsabilità/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 di un certificato 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 degli obblighi previsti dalla legge e richiamati nel CPS/CP.

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 della firma contenute nel certificato alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;
- sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
- sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare nei casi in cui la Banca d'Italia generi entrambi.

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

6.1. Responsabilità della Banca d'Italia nello svolgimento del servizio

La Banca d'Italia si attiene ai requisiti previsti dal regolamento eIDAS, ai relativi standard ETSI e alle regole tecniche di cui al DPCM 22.02.2013 e successive modificazioni e integrazioni. In particolare:

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. rilascia, rende pubblico e gestisce il certificato qualificato nei modi stabiliti dalle regole tecniche di cui al DPCM 22.02.2013 e nel rispetto del Codice in materia di protezione dei dati personali (D. Lgs. 196/2003) e loro successive modificazioni e integrazioni;
5. specifica nel certificato qualificato, 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;
6. 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 delle firme emesse sulla base del servizio di certificazione;
7. non si rende depositario di dati per la creazione della firma elettronica qualificata del titolare;
8. procede alla tempestiva pubblicazione della revoca e della sospensione del certificato qualificato in caso di richiesta da parte del titolare o del terzo interessato, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità giudiziaria, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dall'eIDAS e dalle regole tecniche di cui al DPCM 22.02.2013 e successive modificazioni e integrazioni;
9. garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
10. assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
11. tiene la registrazione di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
12. non copia, né conserva le chiavi private di firma elettronica qualificata del titolare del certificato;
13. 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;

14. 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;
15. registra l'emissione dei certificati qualificati nel Giornale di controllo con la specificazione della data e dell'ora della generazione; il momento della generazione dei certificati è attestato tramite riferimento temporale;
16. genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'AgID (Agenzia per l'Italia Digitale – organismo di vigilanza nazionale dei prestatori di servizi fiduciari qualificati) per la sottoscrizione dell'Elenco Pubblico dei certificatori e lo pubblica nel proprio Registro dei certificati;
17. fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme e ne garantisce l'interoperabilità (ai sensi dell'eIDAS e del DPCM 22.02.2013, art. 14 Verifica delle firme elettroniche qualificate e digitali)[14];
18. inserisce sul proprio sito un link all'elenco pubblico di fiducia (Trusted List), sottoscritto da AgID, dei prestatori di servizi fiduciari qualificati conformi al regolamento eIDAS, contenente i relativi certificati e le relative chiavi di certificazione;
19. revoca o sospende il certificato qualificato ove abbia notizia della compromissione della chiave privata o del dispositivo per la creazione della firma;
20. adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi del regolamento eIDAS e del D. Lgs. 196/2003;
21. registra i seguenti eventi significativi ai sensi del regolamento eIDAS, del DPCM 22.02.2013 e nel rispetto del D. Lsg. 196/2003:
    - 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.
22. si sottopone, a proprie spese almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità e presenta la pertinente relazione di valutazione di conformità all'AgID;
23. informa l'organismo di vigilanza di eventuali cambiamenti nella prestazione dei propri servizi fiduciari qualificati e dell'intenzione di cessare tali attività;

[14] Il sistema per la verifica delle firme digitali, da utilizzare con una connessione internet attiva, consente di:
- verificare la validità del certificato del firmatario e che l'emittente, che ha rilasciato il certificato, sia un prestatore di servizi qualificato;
- accertare l'integrità del documento firmato;
- verificare la validità della firma nel periodo di vigenza del corrispondente certificato, coerentemente con quanto previsto dalla Deliberazione CNIPA 45/2009 art. 27, comma 3.

Per l'effettuazione della descritta operazione di verifica della firma non è richiesta la disponibilità di dispositivi, quali smartcard e relativi lettori. Il sistema per la verifica delle firme digitali è conforme ai requisiti e al processo per la convalida delle firme elettroniche qualificate previsti dal regolamento eIDAS.

24. dispone di un piano di cessazione che prevede, con congruo anticipo rispetto alla dismissione del servizio, la notifica all'AgID e ai titolari di detto evento e che assicura un servizio con cui rendere disponibili le informazioni sullo stato di revoca dei certificati.

7. Pubblicazioni dei documenti di riferimento

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

- il certificato della CA;
- l'impronta del certificato della CA;
- il CPS/CP;
- il presente documento, PKI Disclosure Statement;
- il manuale di utilizzo del software di firma.

8. Tutela della riservatezza

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.

I documenti e le informazioni disponibili sul sito http://www.bancaditalia.it/firmadigitale sono pubbliche.

Le misure di protezione dei dati adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali previste dal regolamento eIDAS e dal D. Lgs. 196/2003 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. Rimborsi

Riguardo alla responsabilità civile per danni, a norma dell'articolo 13 del Regolamento eIDAS, la Banca d'Italia mantiene risorse finanziarie adeguate nell'ambito degli accantonamenti nelle pertinenti voci del proprio bilancio.

10. Leggi applicabili, reclami e risoluzione delle controversie

La Banca d'Italia, in qualità di Qualified Trust Service Provider, si attiene al "Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno" e relativi standard europei, e dalle disposizioni in materia previste dal Codice dell'Amministrazione Digitale, D. Lgs. 82/2005 e successive modifiche e integrazioni. Si attiene inoltre alle "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" di cui al DPCM 22.02.2013.

In materia di riservatezza, la Banca d'Italia adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi del D. Lgs. 196/2003.

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

11. Licenze, marchi e audit

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[15] 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, parzialmente o totalmente, fatta eccezione degli usi specifici inclusi nel certificato.

La Banca d'Italia, ai sensi del regolamento eIDAS, si sottopone a proprie spese almeno ogni 24 mesi, a una verifica della conformità, da parte di un organismo di valutazione. La Banca presenta la pertinente relazione di valutazione di conformità all'AgID (organismo nazionale di vigilanza dei prestatori di servizi fiduciari qualificati).

[15] Object Identifier Number.

Glossario

Certificato di firma elettronica	Un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona.
Certificato qualificato di firma elettronica	Un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del regolamento eIDAS.
Certificatore	Un prestatore di servizi fiduciari qualificato che emette certificati.
Chiave privata	Elemento della coppia di chiavi asimmetriche destinato a essere utilizzato soltanto dal titolare. Se facente parte di una coppia di chiavi di firma o certificazione è utilizzata per apporre una firma elettronica.
Chiave pubblica	Elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico. Se facente parte della coppia di chiavi di firma o certificazione viene utilizzata per verificare la firma apposta con la corrispondente chiave privata.
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.
Dispositivo per la creazione di una firma elettronica	Un software o hardware configurato utilizzato per creare una firma elettronica.
Dispositivo sicuro per la generazione di una firma elettronica qualificata	Un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del regolamento eIDAS e del DPCM 22.02.2013, nonché apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado di conservare in modo protetto le chiavi private e di generare al suo interno firme elettroniche.
Firma automatica	Particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il

	controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo.
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 avanzata	Una firma elettronica che soddisfi i requisiti di cui all'articolo 26[1] del regolamento eIDAS.
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.
Firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
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.
Giornale di controllo	Insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il prestatore di servizi qualificato, allorché si verificano le condizioni previste da eIDAS/DPCM 22.02.2013 e D. Lgs. 196/2003.
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.

[1] Art. 26 - Una firma elettronica avanzata soddisfa i seguenti requisiti:
a) è connessa unicamente al firmatario;
b) è idonea a identificare il firmatario;
c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Lista dei certificati revocati (CRL)	Elenco elettronico dei certificati che sono stati revocati dal prestatore di servizi 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 che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza - AgID - assegna la qualifica di prestatore di servizi fiduciari qualificato.
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 prestatore di servizi annulla la validità del certificato da un dato momento in poi.
Richiedente	Persona fisica che, anche su designazione del terzo interessato, chiede al prestatore di servizi 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.
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 prestatore di servizi.
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) cui - è attribuita la firma elettronica - ha accesso ai dispositivi per la creazione della firma elettronica - ha richiesto e ottenuto dal prestatore di servizi, 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 (ex DigitPA) – 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 Server
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
Legge 229/2003 art. 10	Legge 29 luglio 2003, n. 229 "Interventi in materia di qualità della regolazione, riassetto normativo e codificazione – legge di semplificazione 2001", pubblicata nella Gazzetta Ufficiale n. 196 del 25 agosto 2003
D.Lgs. 196/2003	Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
CIRCOLARE 6 settembre 2005, n. CNIPA/CR/48	Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Pubblicata nella GU Serie Generale n.213 del 13-9-2005
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[2]
Deliberaz. C.N.I.P.A. 45/2009	Deliberazione C.N.I.P.A. 45 del 21 maggio 2009 modificata dalla determinazione AgID n. 69 del 28 luglio 2010
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
Linee guida per la valutazione della	Linee guida per la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma elettronica – CAD art. 35,

[2] 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.

conformità	comma 5
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

BANCA D'ITALIA
EUROSISTEMA

PUBLIC-KEY CERTIFICATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES

PUBLIC KEY INFRASTRUCTURE (PKI)

PKI DISCLOSURE STATEMENT

Version 1.1 - 15/06/2017

The Bank of Italy carries out the public key certification service for the issue of qualified electronic signature certificates, also in remote mode[1] and through a system operated on behalf of a natural person mode, and for the management of the certificates' lifecycle.

The certification service is based on an organizational and technological infrastructure composed of two components: the Registration Authority (RA), that identifies the applicants for certificates and registers applications related to the lifecycle of certificates, the Certification Authority (CA) that manages the issue and lifecycle of certificates and the revocation and suspension lists.

The service is carried out in compliance with:

- "Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market" (hereafter eIDAS) and related European standards;
- the national provisions "Codice dell'Amministrazione Digitale" (Digital Administration Code) and related technical rules under the Prime Ministerial Decree DPCM 22.02.2013.

Certificates are issued to[2]:

- employees of the Bank of Italy for needs connected with working procedures and,
- institutional interlocutors' representatives, in quite special cases, only to be used in dealings with the Bank of Italy.

Certificates are generated at the competent Head Office Departments of the Bank of Italy with a dedicated system housed in appropriately protected premises.

---

1 In the signature in remote mode, the private key does not reside in a secure device consigned to holders but in a remote device (normally a HSM - Hardware Security Module). Data are exchanged with HSM through a secure network.
The system operated mode is a signature process that enables IT procedures of the Bank of Italy – when delegated by a certificate holder - to sign many documents in an automatic system operated way without requiring the certificate holder to sign each document.

2 In compliance with D.lgs. 82/2005, art. 34 "Norme particolari per le pubbliche amministrazioni", (Specific norms for Public Amministration - clause 1).

1. TSP contact info

The CA role is held by the Bank of Italy using a CA technological component called "Servizi di certificazione". The root CA has a duration of 20 years and is available with its fingerprint on the Bank of Italy website http://www.bancaditalia.it/firmadigitale. On the website are also available:

- the Certification Practice Statement (CPS) that specifies the procedures followed by the Bank of Italy for the issue of qualified electronic signature certificates and the management of lifecycle services. The CPS defines all operational procedures for certification services, from the obligations and responsibilities of the Bank of Italy and subscribers to physical and logical security measures adopted;
- the Certificate Policies (CP) that set forth the requirements and standards to use qualified signature certificates in different contexts.

The role of Registration Authority (RA) is held by the Bank of Italy in a decentralized way by means of its Branches and its Head Office that carry out the following activities:

- acceptance and validation of the requests of certificate issue and management;
- identification and authentication of certificate applicants;
- authorization of the issuance of the requested certificate;
- management of requests related to the lifecycle of certificates.

In the following sections of the document, any reference to the Registration Authority is made according to the following scheme.

Bank Structures acting as RA	Subscriber
Administrative Units of the Branches	With reference to the place where the applicant works: - Bank of Italy employees - in quite special cases, institutional interlocutors' representatives only in dealings with the Bank of Italy
Administrative Units of the Head Office	Bank of Italy employees
Organization Directorate	For remote and system operated mode subscribers that already have qualified certificates issued by the Bank of Italy

An institutional interlocutor (body or legal person) – hereafter third party – is allowed to request the issue of a qualified certificate for another subject (holder), on whose behalf it operates pursuant to an employment or agency relationship. This relationship must be accounted for and guaranteed in the certificate application.

The certificate-holder or the third party can make a request to the competent RA to revoke a certificate as indicated in the section 2.

The Bank of Italy is responsible for the qualified certification service; the relevant tasks are allocated to the Organization Directorate.

Qualified Trust Service Provider

Name	Banca d'Italia
Address	Via Nazionale, 91 – 00184 ROMA
Legal representative	Governor pro tempore
PEC	org@pec.bancaditalia.it
e-mail	pki@bancaditalia.it
Web site	www.bancaditalia.it
Phone	06/47921

For further information, please contact the Certification Practice Statement Responsible.

Person responsible for the Certification Practice Statement

Name	Fabio
Surname	Bolognesi
PEC	org@pec.bancaditalia.it
e-mail	fabio.bolognesi@bancaditalia.it

2. Certificate type, validation procedures and usage

The digital certificates issued by the Bank of Italy are signed with its own certification keys and conform with the standard ISO/IEC X.509 v3 and RFC 5280, which provides for a data structure with fixed and variable fields according to the certificate usage. These certificates also conform with the CNIPA deliberation 45/2009 and with standard ETSI EN 319 412. Following the same classification as the key pairs, the certificates can be classified as:

- CA certificate, related to the certifying key used for signing the holders' certificates and the Certificate Revocation List (CRL);
- qualified signing certificates for natural people (certificate-holders).

The holder's certificate, in accordance with requirements laid down in Annex I of the eIDAS Regulation and with Deliberazione CNIPA 45/2009 where applicable, contains:

- the indication that the certificate is qualified;
- the serial number or other identification code of the certificate;
- the name or corporate or registered name of the Certifying Entity and country in which it is established;
- the holder's identification code at the Certifying Entity;

- the holder's given name, family name, tax identification number (for residents abroad, the tax identification number issued by the tax Authority of the country of residence or similar identification number) and date of birth;
- the certificate's terms of validity;
- the Certifying Entity's digital signature;
- the public key number;
- the usable generation and verification algorithms;
- the certificate signature algorithm;
- the type of the pair of keys according to their assigned use;
- the holder's e-mail address (optional);
- the location where the CA certificate is available free of charge;
- the internet address where the CRL is available;
- the indication that the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device.

The personal data contained in the certificate may be used solely to identify the holder in relation to the transactions that he or she is authorized to carry out, given that the certificate usage is limited to dealings with the Bank of Italy.

The certificate is valid for 5 years. The Bank of Italy holds the information about the certificate for not less than 20 years from the date of expiry or revocation of the certificate.

For further details on certificates' profiles see CPS/CPs.

2.1. Request for issue of qualified electronic signature certificates based on a secure signature creation device held by the holder

The following procedures are related to the issue, suspension and revocation of certificates. Further request procedures are detailed in CPS/CPs.

Application forms are available at http://www.bancaditalia.it/firmadigitale.

Issue

The applicant fills in and subscribes an application – using a specific application form - which must:

a. indicate the applicant's identification data, tax identification number, telephone number (landline or cellular) and e-mail address;
b. contain a declaration in which the applicant attests that the information provided is accurate and undertakes to notify every change therein;

c. contain a declaration attesting that the applicant has received the information note referred to in Article 13 of Legislative Decree 196/2003;
d. be accompanied by copies of the applicant's: valid identification document and tax identification number card[3] (only for external applicants).

In case of requests from an institutional interlocutor (third party) in favor of people on whose behalf they operate pursuant to an employment or agency relationship, the third party sends a designation letter signed by the entity's legal representative or other duly appointed person. The designation letter must:

- contain the personal data of the person designated, the type of certificates to be issued and the purposes for which the certificates are being requested;
- contain a declaration in which the third party attests that it is informed of the contents of the Certification Practice Statement/Certificate Policies and undertakes to fulfill the obligations established for them herein;
- have attached the certificate application form, drawn up and signed by the designated person.

The above-mentioned documentation must be sent[4] to the competent RA .

The RA controls the documentation and, after a validation phase via a Registration Web Application[5], forwards issue requests to the CA.

When the certificate is issued, the holder receives a qualified secure signature creation device (smartcard/token USB) by means of the RA.

Data and documentation provided are handled through automated procedures strictly for the purposes described above and with the use of security measures to ensure the confidentiality of personal data and to prevent illegal access to data pursuant to Legislative Decree n.196/2003.

Suspension or revocation

The holder or the interested third party may request the competent RA – using a specific form - to suspend or revoke a certificate for the causes listed in the following table.

[3] No attachment is required if digital signature is used to subscribe the request.

[4] Via registered delivery service (PEC) or email, signing the application with a qualified signature based on a certified issued by a qualified trust service provider. In case the use of a qualified electronic signature in not possible, via PEC with a copy of a valid identification document of the holder in attachment. The PEC must be compliant to "Codice dell'Amministrazione Digitale" requirements . If previous procedures are not available, mail or hand delivery with a copy of a valid identification document of the holder in attachment.

[5] Application suite used for the management of the requests by flow (issuing, suspension, renewal, reactivation and revocation of certificate holders) used by authorized Banca d'Italia personnel.

Suspension

APPLICANT / CAUSE	HOLDER (external person or employee)	INTERESTED THIRD PARTY (for external people)	BANK OF ITALY (for employees)
LOSS OF SMARTCARD	X	--	--
THEFT OF SMARTCARD	X	--	--
BREACH OF SECURITY	X	--	--
PROLONGED ABSENCE OF THE HOLDER	--	--	X
OTHER[6]	X	X	X

Revocation

APPLICANT / CAUSE	HOLDER (external person or employee)	INTERESTED THIRD PARTY (for external people)	BANK OF ITALY (for employees)
LOSS OF SMARTCARD (after suspension)	X	-	-
THEFT OF SMARTCARD (after suspension)	X	-	-
BREACH OF SECURITY[7] (after suspension)	X	-	-
DETERIORATION OF SMARTCARD	X	X	X
CHANGE OF HOLDER'S POSITION[8]	-	X	X

The Bank of Italy assures a suspension service:

- for urgent requests, due to theft, loss or breach of security, by telephone with a Help Desk[9] (+39 06 47929361) available around the clock on all business days and holidays;
- in other cases, the service is available during office hours (8.30-16.30).

6 "Other" takes into account any other cause that cannot be linked to the ones mentioned above.

7 Breach of security must be taken to mean the occurrence of any event that makes it less than certain that the use of the private keys is attributable to the legitimate holder (e.g. the PIN or PUK is known by other persons).

8 Cause to be cited where, for example, the holder ceases work.

9 For urgent suspension requests, the certificate-holder, at the request of the operator, must prove his or her identity and give the pass-phrase received with certificates.

Where the smartcard is recovered, reactivation of the suspended certificate may be requested. Where on the contrary the theft or loss is confirmed, the holder must submit a request for revocation.
In the case where, within the 12 months of the suspension request, the same person who requested the suspension does not require the activation or revocation of the certificate, the latter is revoked ex-officio.

For employees of the Bank, the request is sent to the RA by holders or by the unit to which the employee belongs.

For external users, the revocation request must be submitted to the competent RA by the holder or third party[10]; in this case the request must be signed by the entity's legal representative or other duly appointed person.

The RA receiving the request, upon verifying its authenticity, initiates the revocation procedure using the registration web application. The RA notifies the holder and, if it is necessary, the interested third party of the revocation of the certificate, specifying the date and time since the certificate is no longer valid.

Except in cases of loss or theft, the holder is required to return the smartcard in his or her possession to the RA after rendering it unfit for use by cutting the microcircuit.
A record will be made of the withdrawal of the smartcard. The RA maintains the record for future reference. The withdrawal of the smartcard is reported through a specific functionality of the web application for the managing the lifecycle of certificates.
Following the revocation of a smartcard due to loss, theft, breach of security or deterioration, the Bank of Italy, acting on its own authority, initiates the procedure for the certificate renewal.

The Bank of Italy suspends or revokes certificates by entering their serial number in the list of suspended or revoked certificates.
The suspension or revocation of a certificate takes effect since the certificate is recorded in the aforesaid list (for further details see CPS/CPs).

Revoked certificates must not be reactivated.

The suspension and the revocation of certificates are entered in the audit log journal with an indication of the date and time of the operation. The revocation and suspension list is updated following every request and published at least every 24 hours.

[10] Via registered delivery service (PEC) or email, signing the application with a qualified signature based on a certified issued by a qualified trust service provider. In case the use of a qualified electronic signature in not possible, via PEC with a copy of a valid identification document of the holder in attachment. The PEC must be compliant to "Codice dell'Amministrazione Digitale" requirements . If previous procedures are not available, mail or hand delivery with a copy of a valid identification document of the holder in attachment.

Where the Bank of Italy becomes aware of suspected abuse, falsification or negligence, it may suspend or revoke certificates after notifying the certificate-holders, except as a matter of urgency.

Certificates may be suspended or revoked by the Bank of Italy in case of circumstances provided for article 36 of d.lgs. 82/2005[11].

2.2. Request for electronic qualified electronic signature certificates in remote or system operated mode

Issue

Application for remote and system operated certificates are sent to the Organization Directorate via an email electronically signed by subscribers, normally Bank of Italy's employees, that have qualified certificates issued by the Bank of Italy (see section 1). After the application, certificate holders receive – in an encrypted mode - secret codes (PIN, activation code to initialize an OTP generator – One Time Password[12]) to activate his/her private key stored in a Hardware Security Module hosted by the CA in secure premises.

For system operated certificates, the application must specify the system that will operate on behalf of the certificate-holder. After the application, certificate holders receive a PIN in an encrypted mode. The PIN must be used to delegate a system of the Bank of Italy to operate on behalf of him/her.

The certificates issuance is carried out via a fully automated process on secure communication channels. At the end of the process, the certificate holder's private key is stored in a HSM (Hardware Security Module).

Revocation

Due to the peculiarity of remote mode certificates, the revocation is possible in case of:

- loss of the PIN;
- change of holder's position.

For system operated certificates, the revocation is possible in case of change of holder's position.

[11] Certifier termination; execution of a measure of an Authority; following the request of the holder or of the third party; in the presence of limiting causes of the holder's ability or misuse or falsification.

[12] The HSM requires the holder strong authentication to the signature infrastructure in order to subscribe specific documents. To generate an OTP code it is necessary to use a mobile (smartphone) with an app conveniently initialized with a seed.

For remote mode, in case of loss or theft of the mobile device where the OTP generator is installed, the holder submits a suspension request and installs the OTP generator on a new mobile device.

The suspension/revocation request must be submitted by the holder to competent RA via email electronically signed.

3. Reliance limits

The Bank of Italy will retain records and information concerning qualified certificates, including all events connected to their life-cycle, for at least twenty years from the time of their issue, also in case of CA termination, inter alia in order to provide proof of the certification in judicial proceedings[13].

The Bank of Italy protects its records archival so that only authorized persons have access to archived data for permitted uses. The data electronically stored are protected against viewing, modification, deletion, or other unauthorized tampering by implementing appropriate physical and logical access controls.

Event logging and retention period are compliant to eIDAS Regulation and national regulations (DPCM 22.02.2013) and to the privacy regulations, in particular logical access by system administrator are logged.
The audit logging procedures on infrastructure components are carried out collecting data on the security information and event management systems of the Bank of Italy (audit log journal), hosted in protected premises.

4. Obligations of subscribers

The following obligations are for certificate-holder excepted the peculiarities related to remote or system operated mode in which case the holder does not have a signature device.

The certificate-holder is required to ensure the safekeeping of the signature device and to adopt every organizational and technical measure to avoid injury to third parties and to use the signature device personally.

The certificate-holder, in accordance with requirements and procedures laid down in CPS/CPs, must also:

[13] eIDAS Regulation (art. 24, par. 2, lett. H) and CAD (art 32, par. 3, lett. J).

1. provide all the information requested by the Bank of Italy, guaranteeing its reliability under his or her own responsibility;
2. notify the Bank of Italy of any changes to the information provided at the time of registration: personal data, residence, telephone numbers, e-mail address, etc.;
3. keep the device containing the private key and secret codes (PIN, PUK and pass-phrase) received from the Bank of Italy separately and with the utmost diligence, in order to ensure their integrity and maximum confidentiality;
4. not use the pair of keys for functions or purposes other than those for which the certificate was issued;
5. transmit suspension, reactivation and revocation requests to the Bank of Italy by the procedures specified in the CPS/CPs;
6. immediately request suspension of the qualified certificates for the keys contained in devices that are defective or no longer in his or her possession;
7. notify the Bank of Italy of loss or theft of the security device.

4.1. Obligations of the interested third party

The interested third party is required to request the suspension and revocation of certificates, by the procedures specified in the CPS/CPs, whenever the premises on which a certificate was issued to the holder no longer exist or in case of the cessation of its own activity (as a result of merger, liquidation, etc.).
In addition, without prejudice to the obligations and responsibilities of the certificate-holder, the third party, as the entity in whose interest the certification service is provided, must adopt every precaution and organizational measure serving to ensure utilization of the certificates in conformity with the rules established by law and by the CPS/CPs.
The interested third party is also required to notify the Bank of Italy promptly of every change in the circumstances indicated at the time of issue of certificates that is relevant for the purposes of its utilization.

5. Certificate status checking obligations of relying parties

Applicants for signature verification are all those persons (natural or legal) who, by participating in an on-line transaction, rely on the certificates issued by the Bank of Italy. Certificates status can be validated using the following protocols:

- OCSP, http://ocsp.firmadigitale.bancaditalia.it/ocsp
- HTTP, http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
- LDAP: ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList.

Applicants for signature verification must verify:

1. the validity of the certificate;
2. the fact that the certificate is not entered on the certificate revocation and suspension list (see section 2.1);
3. the existence of and compliance with any restrictions on the use of the certificate used by the certificate-holder.

6. Limited warranty and disclaimer/limitation of liability

The Bank of Italy will not be liable for:

- the consequences deriving from failure of the certificate-holder to comply with the operating procedures and methods specified in the Certification Practice Statement/Certificate Policies;
- the consequences deriving from a use of a certificate other than that permitted and, in particular, for losses deriving from the use of a certificate in excess of its limits;
- failure to fulfill its obligations for causes beyond its control.

The Bank of Italy is responsible only for fulfilling all the obligations established by law and referred to CPS/CPs.

The Bank of Italy is also liable, if it fails to prove that it acted without fraud or negligence, for losses incurred by those who reasonably relied on:

- the exactness and completeness of the data needed to verify the signature contained in the certificate at the date of issue and on their completeness with respect to the requirements established for qualified certificates;
- the guarantee that at the time of issue of the certificate the signatory possessed signature-creation data corresponding to the signature verification data contained or identified in the certificate;
- the guarantee that the signature creation data and signature verification data can be used in a complementary manner where the Bank of Italy generates both.

In addition, the Bank of Italy will also be liable for injuries caused to third parties as a result of the non-registration or delayed registration of the revocation of certificates or the delayed suspension of certificates.

6.1. Obligations of the Qualified Trust Service Provider

The Bank of Italy must comply with the eIDAS Regulation requirements for qualified trust service providers, related ETSI standards and with the rules referred to in the Decree of 22 February 2013 as amended. In particular the Bank of Italy must:

1. adopt every organizational and technical measure to avoid injury to third parties;
2. identify with certainty the person applying for certification;
3. verify the authenticity of the application;
4. issue, render public and manage the qualified certificate in the manner prescribed by the technical rules referred to DPCM 22.02.2013 as amended and in compliance with Legislative Decree 196/2003 as amended;
5. specify in the qualified certificate, at the request of the applicant and with the consent of the interested third party, the powers of representation or other professional attributes or titles of the certificate-holder, subject to verification of the documentation submitted by the applicant attesting to the existence thereof;
6. give applicants complete and clear information on the certification procedure, the requisite technical features for accessing it, the characteristics of the signatures issued on the basis of the certification service and the restrictions on the use thereof;
7. not act as depositary of data for the creation of the holder's qualified signature;
8. promptly publish the revocation or suspension of a qualified certificate in case of a request by the holder or the interested third party, or where the signature device is no longer in the possession of the certificate-holder or its integrity has been compromised, or judiciary has issued a measure, or the Bank of Italy has learned of causes limiting the holder's capacity or suspects abuse or falsification, as established by eIDAS and by the technical rules referred to in the Decree of 22 February 2013 as amended;
9. provide a secure and prompt service for the revocation and suspension of electronic certificates and ensure the efficient, timely and secure functioning of the lists of issued, suspended and revoked signature certificates;
10. ensure the precise determination of the date and time of issue, revocation and suspension of electronic certificates;
11. retain records of all the information concerning qualified certificates for at least twenty years from the time of their issue, inter alia in order to provide proof of the certification in judicial proceedings;
12. not copy and not conserve the private qualified signature keys of the certificate-holder;
13. prepare all the necessary information, in particular the exact terms and conditions governing the use of certificates, including restrictions on their use, on permanent media and make such information available to applicants for the certification service;
14. use reliable systems for the management of the Certificate Registry with procedures ensuring that only authorized persons can make additions and changes, that the authenticity of the data can be verified, that certificates are accessible for consultation by the public only in the cases permitted by the holder, and that the authorized person will become aware of any event that jeopardizes security. Pertinent items of information may be made accessible on request to third parties that rely on the certificate;
15. record the issue of qualified certificates in the audit log journal, specifying the date and time of generation; the moment of generation of certificates is attested to by means of a time reference;

16. generate a qualified certificate for each of the electronic signature keys that the AgID (Agenzia per l'Italia Digitale - national supervision authority of qualified trust service providers) uses for signing the Public List of qualified trust service providers and publish it in its own Register of Certificates;
17. provide or indicate at least one system that permits signature verification and ensures its interoperability (in accordance with eIDAS and as referred to in Article 14 of the Decree of 22 February 2013 as amended)[14];
18. publish on the website a link to the public list, subscribed by the national supervision authority of trust service providers AgID, of trust service providers (Trusted List) qualified in accordance with the eIDAS Regulation, containing their certificates and CAs key;
19. revoke or suspend a qualified certificate upon learning that the integrity of the private key or of the signature-creation device has been compromised;
20. adopt security measures for the treatment of personal data pursuant to eIDAS and Legislative Decree 196/2003;
21. log the following significant events in accordance with eIDAS, DPCM 22.02.2013 and D.Lsg. 196/2003:
    - CA key's and certificate's life cycle management events;
    - certificate-holders key's and certificate's life cycle management events;
    - cryptographic device's life cycle management events;
    - security related events;
22. be audited at their own expense at least every 24 months by a conformity assessment body and submit the resulting conformity assessment report to AgID;
23. inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;
24. have an up-to-date termination plan to inform of termination, well in advance, the national supervision authority of trust service providers (AgID) and holders of the termination and to assure a revocation status information service.

7. Applicable agreements, CPS, CP

The following documents are available at the Internet website http://www.bancaditalia.it/firmadigitale:

- the CA certificate;
- the CA certificate fingerprint;
- the CPS/CPs;

[14] The digital signature verification system, to be used with an active Internet connection, makes it possible to:
- verify the validity of the signatory's certificate and the issuer's qualification as qualified trust service provider;
- ascertain the integrity of the signed document;
- verify the validity of the signature in the same period validity of the corresponding certificate, in accordance with provisions of the CNIPA deliberation 45/2009, art. 27, paragraph 3.

Devices such as smartcards and their readers do not have to be available in order to perform verification. The digital verification system is compliant with the requirements and the process for the validation of qualified electronic signatures as laid down in eIDAS regulation.

- this document PKI Disclosure Statement;
- the instructions to use the signature software.

8. Privacy policy

Data is handled in compliance with specific security policies mainly by automatic processes and authorized personnel that have access to the data on the basis of authentication systems, in accordance with ICT security policy defined by the Bank of Italy. All information about the certificate-holders that are not publicly available through the certificate or revocation and suspension list online are treated as confidential.

Documents and information available at http://www.bancaditalia.it/firmadigitale are public.

The Bank of Italy must adopt data safety measures for the treatment of personal data in compliance with the minimum safety measures for handling of personal data provided by eIDAS and the Legislative Decree 196/2003 and subsequent amendments and additions.

The Bank of Italy shall be entitled to disclose confidential/private information in response to judicial and administrative processes.

9. Refund policy

With regard to the risk of liability for damages, in accordance with Article 13 of eIDAS Regulation, the Bank of Italy maintains sufficient financial resources, covered by provisions in appropriate balance sheet items.

10. Applicable law, complaints and dispute resolution

The Bank of Italy, as a Qualified Trust Service Provider, adheres to the Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and related European standards, and the relevant provisions of the Legislative Decree no. 82/2005 and subsequent amendments. The Bank of Italy is compliant with the technical rules DPCM 22/02/2013.

In the area of privacy, the Bank of Italy adopts the security measures for the processing of personal data, pursuant to Legislative Decree no. 196/2003.

The jurisdiction for the resolution of disputes concerning the certification service is Rome.

11. TSP and repository licenses, trust marks, and audit

The Bank of Italy is the exclusive owner of all rights related to the electronic certificates issued by CA; the certificate revocation and suspension list; the content of this Certification Practice Statement and the Certificate Policies. Furthermore, the Bank of Italy is the holder of the rights related to any other kind of document, protocol, computer program and hardware, file, directory, database and consultation service that may be generated or used in the area of the PKI activities.

The object identifiers numbers (OIDs) used are the property of Bank of Italy and have been registered by the national competent Authority (UNINFO). No OID assigned to Bank of Italy may be used, partially or fully, except for the specific uses included in the certificate.

The Bank of Italy shall be audited at its own expense at least every 24 months by a conformity assessment body and submit the resulting conformity assessment report to the national supervisory body (AgID).

Glossary

Advanced electronic signature	An electronic signature which meets the requirements set out in Article 26 of eIDAS [1].
Applicant	Natural person who makes a request to the Certifier, for himself or because authorized to act for a third party, to obtain a public and private key pair and a certificate. Once the certificate is issued the applicant becomes the certificate-holder.
Asymmetric encryption	Mathematical operation by which, using two different keys and a specific algorithm, it is possible to decrypt a message encrypted by a key only using the same algorithm and the other key.
Asymmetric keys	Asymmetric public and private key pair in which the two keys are interrelated and are used to sign, cipher and authenticate.
Audit log journal	Set of records to log automatically events that are relevant in compliance with eIDAS/DPCM 22.02.2013 and D.Lsg. 196/2003.
Certificate for electronic signature	An electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.
Certificate Revocation	Operation carried out by Trust Service Provider consisting in the revocation of the validity of a certificate from a specific date and time.
Certificate Revocation List	List of electronic certificates that have been revoked by the certificate authority that issued them. This list, which is part of the Certificate Registry, is signed, maintained and updated by the Certifier.
Certification keys	Key pair used by the Service Provider to sign the Certificates, the Certificate Revocation and Suspension List.
Certifier	A qualified trust service provider who issues certificates.
CRL	See Certificate Revocation List.
Digital Signature	A special type of electronic signature based on a key encryption system with an asymmetric matching pair of keys (public and

[1] Art. 26 - An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

	private) which allows both the card holder (using the private key) and the recipient (using the public key) to prove the source and integrity of the electronic document/group of documents.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
Electronic signature creation device	Configured software or hardware used to create an electronic signature.
Electronic time stamp	Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
Fingerprint of a sequence of binary symbols (bits)	The sequence of binary symbols (bits) of predefined length generated by the application of a suitable hash function to the sequence.
Hash function	A mathematical function that uses a generic sequence of binary symbols to convert data into a fingerprint from which it is impossible to trace the sequence of binary symbols that generated it. The probability of defining two sequences of binary symbols for which the hash function yields the same fingerprint is computationally infeasible.
Holder	The natural person (see signatory) that: - is assigned the electronic signature; - has access to the devices for the creation of the electronic signature; - has requested and obtained from the Service provider, also by designation of a third party, a pair of keys (public and private) and the related certificate.
HSM (Hardware Security Module)	Configured hardware security device, part of the validation system, used as a safe private key storage facility and to generate electronic signatures.
OCSP (online certificate status protocol)	Network protocol used to verify the certificates' validity.
Pass-phrase	A string of both alpha-numeric characters and punctuation marks, known only to the card-holder, who must communicate it to the Help Desk when requesting the urgent suspension of a certificate in case of loss, thief or in case security is jeopardized.
PIN	Personal Identification Number.
PKI (Public Key Infrastructure)	Set of hardware, software, people and procedures needed to create and manage digital certificates and the signature-creation devices.
Private key	The key of an asymmetric key pair used only by the certificate-holder. If the private key is part of a signature pair or an authentication pair it can be used to sign electronically.

Public key	The key of an asymmetric key pair which can be made public. If the public key is part of a signature pair or an authentication pair it can be used to verify the signature given by the matching private key.
PUK	PIN unlock key.
Qualified certificate for electronic signature	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS regulation.
Qualified electronic signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
Qualified electronic signature creation device	An electronic signature creation device that meets the requirements laid down in Annex II of eIDAS and of DPCM 22.02.2013.
Qualified trust service	A trust service that meets the applicable requirements laid down in eIDAS.
Qualified trust service provider'	A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Registration	Collection, authentication and storage of the personal data regarding the applicants for certificates. The registration is a necessary step before accepting the application for certification.
Registry of certificates	The combination of one or more electronic archives that registers all the certificates issued by the Trust Service Provider.
Remote signature	A particular type of qualified electronic signature or digital signature process generated on HSM which ensures exclusive control of private keys by the holder.
Signatory	A natural person who creates an electronic signature.
Subscriber	Legal or natural person bound by agreement with a trust service provider to any subscriber obligations.
Smartcard	Security device with an embedded circuit used for storing the key pair (private and public) and the certificate of the certificate-holder.
System operated signature on behalf of a natural person	Particular automatic system for qualified electronic signature or digital signature performed prior consent of the subscriber that maintains exclusive control of their signing keys, in the absence of timely and continuous supervision by this.
Third party	An institutional interlocutor (body or legal person) which request the issue of a certificate for another subjects, on whose behalf they operate pursuant to an employment or agency relationship.
Time reference	Specific time and date stamp connected to one or more

	documents.
Time validation	Result of the computer procedure with which one or more digital documents are time stamped as to be enforceable against third parties.
USB token	Security device with an embedded circuit used for storing the key pair (private and public) and the certificate of the certificate-holder.
Trust service	An electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services.
Trust service provider	A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider as laid down in the eIDAS regulation.

Acronyms

AgID	Agenzia per l'Italia Digitale (ex DigitPA) - national supervision authority of trust service providers
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 Server
LRA	Local Registration Authority
OCSP	On-line Certificate Status Protocol

PKI	Public Key Infrastructure
RA	Registration Authority
SAN	Storage Area Network

References

Law 59/1997 art. 15, par. 2	Law of 15 March 1997, n. 59 "Devolvement to the Government of the conferment of functions and assignments to regions and other local government bodies, for the reform of the public administration and administrative simplification" published in the S.O. 56/L of the *Gazzetta Ufficiale* n.63 of the 17 march 1997.
Law 229/2003 art. 10	Law of 29 July 2003, n. 229 "Measures regarding regulatory, legislative and codification quality – simplification law 2001", published in the Gazzetta Ufficiale n.196 of 25 August 2003
D.Lgs. 196/2003	Personal Data Protection Code - Legislative Decree no.196 of 30 June 2003
CNIPA/CR/48	C.N.I.P.A. circular 6 September 2005
L.D. 82/2005 "Codice dell'Amministrazione Digitale" (Digital Administration Code - CAD)	Legislative decree 7 March 2005, n. 82 "Digital administration code" published in the S.O. N. 93/L of the Gazzetta Ufficiale n.112 of 16 May 2005[2].
Deliberation 45/2009	C.N.I.P.A. deliberation 45 of 21 May 2009 as amended by AgID decision n. 69 of 28 July 2010
DPCM 19.07.2012	DECREE OF THE PRESIDENT OF THE COUNCIL OF MINISTERS 19 July 2012 Definition of terms of validity of self-certification on the compliance of the automatic signature devices to the safety requirements of the Decree of the President of the Council of Ministers October 30, 2003, and the terms for replacing the automatic signature devices
DPCM 22.02.2013	Specifications for the creation, application and verification of qualified and digital electronic signature, according to items 20 paragraph 3, 24 paragraph 4, 28 paragraph 3, 32 paragraph 3 letter b), 35 paragraph 2, 36 paragraph 2 and 71." Published in the Gazzetta Ufficiale n.117 of 21 May 2013
Conformity assessment guidelines	Guidelines for conformity assessment of the system and authentication procedures used in the generation of the electronic signature in

[2] The "Code", in force since the 1st January, has overridden the D.P.R. 28.12.2000, n.445 provisions regarding electronic signatures, documents and identity cards and the development of Public Administration information systems.

	accordance with art. CAD. 35, paragraph 5
eIDAS Regulation	Regulation (eu) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Published in the EU Official Journal of 28 August 2014 L 257