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 1.2 - 30/05/2019

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 (sospensione, revoca, rinnovo).

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.

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 (sospensione, revoca, rinnovo, archiviazione) 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 e dell'organizzazione di appartenenza;
- 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	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
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
Help Desk7 per le richieste di sospensione d'urgenza	06/47929361

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 alle indicazioni fornite dall'AgID 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 alle indicazioni fornite dall'AgID ove applicabili, 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 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 lista dei certificati revocati;
- 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.

La Banca d'Italia custodisce le informazioni relative al certificato per un periodo pari a 20 anni dalla data di emissione.

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 (secure signature creation device)

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.

Emissione

Il richiedente redige e sottoscrive, con apposito modulo (disponibile sul sito www.bancaditalia.it/firmadigitale), l'istanza che deve:

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

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

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

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[3] alla RA competente.

La RA esamina la documentazione ricevuta e, dopo la fase di convalida gestita tramite un sistema di registrazione[4], 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.

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

[4] 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.

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

Sospensione o revoca

Il titolare o il terzo interessato possono chiedere alla RA competente, con apposito modulo (disponibile sul sito www.bancaditalia.it/firmadigitale), 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[5]	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[6] (previa sospensione)	X	-	-
DETERIORAMENTO DELLA	X	X	X

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

[6] 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.

RICHIEDENTE / CAUSALE	TITOLARE (soggetto esterno o dipendente)	TERZO INTERESSATO (per i soggetti esterni)	BANCA D'ITALIA (per i dipendenti)
SMARTCARD			
MODIFICA DELLA POSIZIONE TITOLARE[7]	-	X	X

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[8] (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[9] 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.

---

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

8 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.

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

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.
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[10].

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 e-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[11]) 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

[10] 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.

[11] 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*).

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. I titolari dei certificati sono responsabili del corretto utilizzo e della custodia degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma.

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 e-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[12], 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 normativa europea e nazionale in materia di protezione dei dati personali; in particolare viene effettuata la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

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

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.

Il titolare è tenuto ad assicurare la custodia del dispositivo di firma, o degli strumenti di autenticazione informatica per l'utilizzo 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. l'integrità del documento;
2. la validità del certificato qualificato al momento della firma (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.

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 della normativa europea e nazionale in materia di protezione dei dati personali 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 o degli strumenti di autenticazione informatica per l’utilizzo 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 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];
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. adotta adeguate misure di sicurezza per il trattamento dei dati personali, ai sensi del regolamento eIDAS e dalla normativa europea e nazionale in materia di protezione dei dati personali;
20. registra i seguenti eventi significativi ai sensi del regolamento eIDAS, del DPCM 22.02.2013 e dalla normativa europea e nazionale in materia di protezione dei dati personali:
    - gli eventi di gestione del ciclo di vita del certificato e delle chiavi di CA;

---

13 A seguito dell'emissione dei certificati di firma in modalità remota la chiave privata di firma del titolare è memorizzata in un HSM custodito in locali protetti della CA: in ogni caso l'infrastruttura garantisce il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.

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.

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.

- 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.

21. 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;
22. informa l'organismo di vigilanza di eventuali cambiamenti nella prestazione dei propri servizi fiduciari qualificati e dell'intenzione di cessare tali attività;
23. 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/footer/firmadigitale/index.html 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.

Le seguenti informazioni sono considerate pubbliche:

- CPS/CP;
- la lista dei certificati revocati e sospesi.

Le misure di protezione dei dati adottate sono conformi alle misure di sicurezza per il trattamento dei dati personali previste dal regolamento eIDAS e dalla normativa europea e nazionale in materia di protezione dei dati personali e successive modifiche e integrazioni.

La Banca d'Italia ha il diritto di rivelare informazioni riservate/confidenziali se, in buona fede, ritenga che:

- la divulgazione sia necessaria in risposta a citazioni e mandati di perquisizione;
- la divulgazione sia necessaria in risposta a procedimenti giudiziari, amministrativi o altro.

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

9. Rimborsi

Riguardo alla responsabilità civile per danni, a norma dell'articolo 13 del Regolamento eIDAS, la Banca d'Italia mantiene risorse finanziarie adeguate prevedendo opportuni 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 alle 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.

La Banca d'Italia adotta le misure di sicurezza per il trattamento dei dati personali ai sensi della legislazione europea e nazionale in materia.

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 dalla normativa europea e nazionale in materia di protezione dei dati personali.
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

[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.

	elettronici e dei relativi dispositivi di firma.
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.
Sistema di registrazione (Registration Web Application)	Suite applicativa utilizzata per la gestione del flusso delle richieste (emissione, sospensione, rinnovo, riattivazione e revoca dei certificati dei titolari), accessibile solo dal personale abilitato.
Smartcard	Dispositivo di sicurezza sul quale risiedono la coppia di chiavi (pubblica e privata) e il certificato del titolare.
Sospensione del certificato	Operazione con cui il prestatore di servizi sospende la validità del certificato per un periodo di tempo.
Sottoscrittore	Persona fisica o giuridica che deve rispettare gli obblighi per la sottoscrizione previsti dal 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
D.Lgs. 196/2003	Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali e successive modifiche e integrazioni
DETERMINAZIONE N. 185/2017	Emanazione del regolamento recante le modalità con cui i soggetti che intendono avviare la prestazione di servizi fiduciari qualificati presentano all'AgID domanda di qualificazione ai sensi dell'art. 29 del decreto legislativo 7 marzo 2005, n. 82
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]
DETERMINAZIONE N. 121/2019	Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate
DPCM 19.07.2012	DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 19 luglio 2012 Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma
DPCM 22.02.2013	DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 . Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera *b)*, 35, comma 2, 36, comma 2, e 71. Pubblicato nella Gazzetta Ufficiale del 21 maggio 2013 n. 117
Linee guida per la valutazione della conformità	Linee guida per la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma elettronica – CAD art. 35, comma 5

[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.

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