BANCA D'ITALIA
EUROSISTEMA

PUBLIC KEY CERTIFICATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES

PUBLIC KEY INFRASTRUCTURE (PKI)

CERTIFICATION PRACTICE STATEMENT
CERTIFICATE POLICY

Version 1.4 - 01/02/2022

Glossary

The following definitions refer also to eIDAS and Legislative Decree 7 March 2005, n. 82 as amended.

Advanced electronic signature	An electronic signature that 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 European and national legislation on personal data protection.
Certificate for electronic signature	An electronic attestation that 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Certificate Revocation List	List of electronic certificates that have been revoked by the certificate authority that issued them.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 (Certificate Revocation List)	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 private) which allows both the card holder (using the private

[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.

	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 that 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 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 that can be made public. If the public key is part of a signature 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.
Registration web application	Software used to manage the lifecycle of certificates, accessible only by authorized personnel
Registry of certificates	The combination of one or more electronic archives that register 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.
Suspension	Procedure used by the Certifier to suspend the certificate’s validity only for a defined period of time.
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.
D.Lgs. 196/2003	Personal Data Protection Code - Legislative Decree no.196 of 30 June 2003 and subsequent amendments and additions.
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
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].
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	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 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
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[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.

1. INTRODUCTION

1.1 Overview

The Bank of Italy carries out the public key certification service for the issue of qualified electronic signature certificates and for the management of the certificates' lifecycle, in accordance with:

- "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" (hereafter eIDAS) and related European standards;
- the national provisions "Codice dell'Amministrazione Digitale" (Digital Administration Code) and related technical rules under the Decree issued by the President of the Council of Ministers on 22 February 2013 (hereafter DPCM 22.02.2013).

Certificates are issued to[3]:

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

The service is based on an organizational and technical infrastructure – Public Key Infrastructure - composed of two components: the Registration Authority (RA), that identifies applicants for certificates and registers applications related to the lifecycle of certificates, the Certification Authority (CA) that manages the issue and lifecycle of the certificates and suspension and revocation lists. In addition, the PKI consists also of the following components:

- Reference copy of the Certificate Registry (directory master), component used by the Certification Authority for the publication of certificates and certification and revocation list;
- Operational Copy of the Certificate Registry (directory shadow), a component used by the certificate-holder and by applications to download certificates and suspension and revocation list;
- Audit log journal, to log automatically events that are relevant for security;
- Registration Web application, application suite used for the management of the requests flow (issuing, suspension, rekey, reactivation and revocation of certificate-holders);
- Online Certificate Status Protocol (OCSP) service, a verification service to check certificate validity.

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

This document contains the policies for the public key certification service for qualified electronic signatures carried out by the Bank of Italy (hereinafter qualified trust service Provider):

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

- Certification Practice Statement (CPS) that specifies the operational procedures for the issue, the management and the usage of qualified electronic signature certificates. The document defines also the obligations and responsibilities of the Bank of Italy and subscribers and the physical and logical security measures adopted;
- Certificate Policies (CP) that set forth the requirements and standards to use qualified signature certificates in different contexts. In particular they concern the issuance and management of the following types of certificates:
  - qualified electronic signature (using a qualified signature creation device hold by the signatory);
  - qualified electronic signature in remote mode and through a system that will operate on behalf of a natural person, in compliance with the DPCM 22.02.2013[4].

The CPS/CPs contain the terms and conditions for the use of certificates, including any limitations, addressed to persons that have dealings with the Bank of Italy: signatories, interested third parties (see the glossary), relying parties. These terms and conditions become effective upon a subject becomes holder (hereinafter referred as subscriber or signatory or certificate-holder) of a certificate issued by the Bank of Italy.

The document content, layout and format are compliant with the Internet Engineering Task Force standards (IETF) RFC 3647.

1.2 Document name and identification

This document is available for consultation, in English and Italian, at the following website http://www.bancaditalia.it/firmadigitale and contains the version 1.4 dated 01 February 2022 of:

- the CPS, referenced by the following Object Identifier Number (O.I.D.) 1.3.76.38.1.1.1;
- the CPs referenced by the OIDs:
  - 1.3.76.38.1.1.1.1[5] qualified certificates requiring a qualified electronic signature creation device;
  - 1.3.76.38.1.1.1.2 qualified certificates in remote mode;
  - 1.3.76.38.1.1.1.3 qualified certificates through a system that will operate on behalf of a natural person.

[4] Remote and system operated signature mode are available only for the Bank of Italy employees.

[5] OIDs have been registered by the competent national authority (UNINFO).

In case a section (or subsection) of these CPS/CPs is applicable to a specific certificate profile, one of the tags will be used:

- [1.3.76.38.1.1.1.2 REMOTE];
- [1.3.76.38.1.1.1.3 SYSTEM OPERATED].

When not specified, the policy is valid for all certificates' profiles.

The document version and the date of the last update are reported on the frontispiece. The version is identified on each page.

1.3 PKI participants

1.3.1 Certification authorities

The CA role is held in a centralized way by the Bank of Italy using a CA technological component called "Servizi di certificazione"[6]. The CA issues qualified electronic signature certificates, also in remote mode and through a system that will operate on behalf of a natural person.

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

Qualified Trust Service Provider

Name	Banca d'Italia
Address	Via Nazionale, 91 – 00184 ROMA
Legal representative	Governor pro tempore
PEC	svi@pec.bancaditalia.it
e-mail	pki@bancaditalia.it
Web site	www.bancaditalia.it
Phone	+39 06 47921
Help Desk for urgent suspension requests[7]	+39 06 47929361

The CA certificate has a duration of 20 years and is available with its fingerprint on the Bank of Italy website http://www.bancaditalia.it/firmadigitale. For details on the CA certificate's profile, see section 7.

[6] The CA of the Bank of Italy is based on a single level.
[7] See section 4.9.

1.3.2 Registration authorities

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 applications for certificates issue and management;
- registration of the applicants;
- authorization of the issuance of the requested certificates;
- management of requests related to the lifecycle of certificates.

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

Bank of Italy Structures acting as RA	Subject applying for a certificate's request
Administrative Units of the Branches	With reference to the place where the applicant works: - Bank of Italy employees; - in quite special cases, to institutional interlocutor's representatives only in dealings with the Bank of Italy
Administrative Units of Head Office	With reference to the place where the applicant works: - Bank of Italy employees; - in quite special cases, to institutional interlocutor's representatives only in dealings with the Bank of Italy
IT Planning Directorate	For remote and system operated mode subscribers that already have qualified certificates issued by the Bank of Italy [1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

<u>Obligations of the Qualified Trust Service Provider</u>

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 DPCM 22.02.2013 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 22.03.2013 as amended and in compliance with European and national legislation on personal data protection;
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 authentication tools are no longer in the possession of the certificate-holder or their integrity have 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 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[8];
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)[9];

[8] For qualified certificates in remote mode, the private key is stored in a HSM, held in protected premises. The infrastructure ensures exclusive control of private keys by the holder.

[9] The digital signature verification system, to be used with an Internet connection established, 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.

Devices such as smartcards and their readers do not have to be available in order to perform verification.

18. publish on the website a link to the public list of trust service providers (Trusted List) qualified in accordance with the eIDAS Regulation, containing their certificates and CAs key;
19. adopt security measures for the treatment of personal data pursuant to eIDAS and European and national legislation on personal data protection;
20. log the following significant events in accordance with eIDAS, DPCM 22.02.2013 and European and national legislation on personal data protection:
    - 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;
21. 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;
22. inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;
23. have an up-to-date termination plan to inform of the termination, well in advance, the national supervision authority of trust service providers (AgID) and holders and to assure a revocation status information service.

1.3.3 Signatories and third parties

Hereinafter, signatory is also referred as subscriber or certificate-holder (holder) to make reference to a natural person who receives a certificate issued by the Bank of Italy.

A third party is an institutional interlocutor (body or legal person) 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.

Certificates are issued to employees of the Bank of Italy for needs connected with working procedures and, in quite special cases, to institutional interlocutor's representatives only in dealings with the Bank of Italy.

Certificates are not issued to legal persons.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

Subscribers having already qualified certificates on security device issued by the Bank of Italy are allowed to request qualified certificates for remote electronic subscription or to subscribe through a system operated on behalf of a natural person.

The digital signature verification system is compliant with the requirements and the process for the validation of qualified electronic signatures provided by eIDAS.

Obligations of the certificate-holder

The certificate-holder is required to ensure the safekeeping of the signature device or authentication tools 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 the present document, must also:

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 renewal, 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.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

Remote or system operated mode not requires the possession of a device containing the private key then, with reference to the previous point 3, the certificate-holder has to conserve authentication tools.

Obligations of the interested third party

The interested third party is required to request the suspension and revocation of certificates, according to 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 CSP/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.

1.3.4 Relying parties

All those persons (natural or legal) who, by participating in an on-line transaction, rely upon the certificates issued by the Bank of Italy and verify the validity of a digital signature using a the online services offered by the Bank of Italy.

<u>Obligations of relying party</u>

Parties verifying a digital signature must verify:

1. the integrity of the document;
2. the validity of the qualified certificate at the time of signature (the fact that the certificate is not entered on the certificate revocation and suspension list);
3. the existence of and compliance with any restrictions on the use of the certificate used by the certificate-holder.

1.3.5 Other participants

There are no further participants other than the ones of previous sections.

1.4 Certificate usage

Certificates are issued to employees of the Bank of Italy for needs connected with working procedures and, in quite special cases, to institutional interlocutor's representatives only in dealings with the Bank of Italy.

The key pairs generated by the qualified certification service of the Bank of Italy are used as:

1. certification keys (hereafter CA keys or root CA keys), used by the Bank of Italy to electronically sign subscriber's certificate and revocation and suspension list;
2. certificate-holder's keys, consigned to natural person by the Bank of Italy in order to be able to use a qualified electronic signature.

A key pair shall not be used for any other purpose except the one for that it is generated. The certificate indicates the key usage.

It is explicitly to not use holder's certificate:

- as CA certificates;
- for different purposes other than outlined in the certification request;
- outside of their given validity period;
- after revocation by the CA;
- for different purposes other than those ones foreseen in usage limitation.

1.5 Policy administration

The Bank of Italy prepares and publishes the present document; a document update is performed in case of relevant changes to the infrastructure or to the regulations.

The person responsible for the document is:

Name	Stefano
Surname	Massi
PEC	svi@pec.bancaditalia.it
e-mail	stefano.massi@bancaditalia.it

Possible amendments are approved by the responsible of the document and, in case of particular importance, are notified to national supervision authority and to the entity that has carried out the conformity assessment of the service. Amendments may be made by updating this entire document or by addendum and are indicated through new version numbers[10].

The Bank of Italy publishes the latest version of the document on its website http://www.bancaditalia.it/firmadigitale.

1.6 Definitions and acronyms

Definitions, acronyms, and references are provided at the beginning of the document.

[10] In particular, new versions are indicated with an integer followed by a decimal that is zero. Minor changes are indicated through one decimal number greater than zero.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

The Bank of Italy manages and is directly responsible for the contents and the publication of the status of issued certificates, of the specific policies and of the procedures that govern the certification service.

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

- the CA certificate;
- the CA certificate fingerprint;
- this document (CPS/CPs) and its summary document (Disclosure Statement);
- instructions to use software to sign.

The Bank of Italy manages and publishes the list of revoked and suspended certificates in order to provide information on the status of certificates. The revocation and suspension list is updated following every request and is published at least every 24 hours. The revocation and suspension list can be consulted, free of charge, on one of the following links:

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

Access to the repositories for updating is possible by specific workstations only to personnel authorized to work on the PKI infrastructure of the Bank of Italy.

3 IDENTIFICATION AND AUTHENTICATION

The Bank of Italy, which acts as RA, identifies the applicant for a certificate and ensures the authenticity of the request as described in the following sections.

The identification and authentication of the certificate-holder take place at the application for the first issue.

3.1 Naming

Digital certificates issued by the Bank of Italy are unambiguously identified by a certificate serial number, while the certificate-holders are identified by an unambiguous holder identification number (I.U.T).

The issued certificates contain the Distinguished Name (or DN) of the issuing authority and of the subscriber of the certificate respectively in the issuer name and subject name fields.
The Bank of Italy ensures that the distinguished names of the certificate-holder are unique by means of the usage of the tax identification number.
Anonymous users as well as pseudonyms for signatory are not supported since DN identifies the subject to which the provisions of this document are applied.

Naming in certificates are as specified in Recommendation ITU-T X.509 and in accordance with ETSI EN 319 412 standard.

3.2 Initial identity validation

The Bank of Italy employees are already identified and authenticated by the Bank of Italy that has all employees documents (personnel record) after their hiring. Without prejudice to the requirements of law, the identification and authentication process for the Bank of Italy employees takes place by direct personal knowledge and could be a little different than the process for externals holders.
The designation of the applicant by third parties entities is not applicable to internal employees.
That said, if all other things being equal, the following rules are valid for employees and the external persons.

Persons external to the Bank of Italy who apply for the issue of certificates must be designated by the entities (interested third parties) on whose behalf they operate pursuant to an employment or agency relationship. Third parties send to RA a designation letter with the holder's certificate application in attachment (see section 4.1).
For persons external to the Bank of Italy, the identification and authentication phase is completed by the RA at the delivery of the certificates. On such occasion, the RA will invite the certificate-holder to come to the RA for the purpose of identification and authentication based on a currently valid document from among the following:

1) passport;
2) driving license;
3) watercraft license;
4) pension account book;
5) gun permit;
6) heating plant operator’s license;
7) identity card, with photography and stamp, issued by an EU member state.

These documents are approved by the national supervisory body for trust service provider in compliance with the provisions of Italian law (Decree of the President of the Republic, 28 December 2000, n. 445 art. 35).

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 eIDAS and European and national legislation on personal data protection.

3.3 Identification and authentication for re-key requests

The qualified electronic signature certificates issued to holders have a maximum validity of 5 years.

A certificate re-key takes place when the certificate is about to expire; a certificate with a new public key is issued.

The Bank of Italy employees do not have to require a certificate re-key because they receive an automatic message when the certificate is about to expire. The holder uses a specific web application to start the re-key process on its smartcard in a decentralized way. The holder is identified and authenticated directly by the web application by means of his/her smartcard and user credentials.

When the certificate is about to expire, the external users (third parties) receive a communication by the Bank of Italy to ask if it is necessary to issue a set of certificates identical to those expiring for each holder. If the answer is affirmative, the interested third party must send the competent RA a designation note with holder’s application in attachment (see section 4.7).

The identification and authentication phase is completed as described in section 3.2, at smartcard delivery, when the holders show a valid identification document. On such occasion the RA withdraws the smartcard containing the expiring certificate and renders it unfit for use by cutting the microcircuit.

The RA verifies that the request is authentic on the basis of the data provided by the subscriber during the enrollment phase; the following elements contained in the request are verified:

- data of the holder of the certificate;
- previous designation of the holder by the interested third party.

3.4 Identification and authentication for revocation request

For the Bank of Italy employees (identified and authenticated by the competent RA as described in section 3.2) the application for revocation can be submitted by the holder or the unit for he/she belongs to.

For persons external to the Bank of Italy (identified and authenticated by the competent RA as described in section 3.2), the application for revocation can be submitted by the holder or the third party.

The RA verifies that the request is authentic on the basis of the data provided by the subscriber during the enrollment phase; the following elements contained in the request are verified:

- data of the holder of the certificate;
- previous designation of the holder by the interested third party.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The certification service carried out by the Bank of Italy concerns the issuance, renewal, suspension and revocation of certificates and the maintenance and publication of the list of revoked and suspended certificates that allows the status verification of the certificates.

Applications for the issue of certificate are managed by the Bank of Italy through human resources, technological assets and operating procedures defined in this document.

The application are processed through a web application accessible exclusively on the internal network of the Bank of Italy by authorized personnel.

Application forms relating to the certificates' lifecycle are available at www.bancaditalia.it/firmadigitale.

4.1 Certificate Application

The applicants are the natural people indicated in section 1.3.3.

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) be accompanied by copies of the applicant's: valid identification document and tax identification number card (only for external applicants).

When signing the application, the applicant declares to:

- be informed of the conditions of use of the certificates identified in this document and in the supplementary regulations issued by the Bank of Italy and to undertake not to use them for purposes other than those provided for in the provisions of the Bank of Italy;
- be aware that, since the receipt of the smartcard, he/she can communicate with the Help Desk of the Bank of Italy only at the times and in the days specified in the present document;
- have received the data protection policy.

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 CPS/CPs and undertakes to fulfill the obligations established for it herein;
- have attached the certificate application form, drawn up and signed by the designated person.

The above-mentioned documentation must be sent[11] to the competent RA.

[1.3.76.38.1.1.1.2 REMOTE]

In case of remote signature, applications are sent to the IT Planning Directorate via an e-mail electronically signed.

[1.3.76.38.1.1.1.3 SYSTEM OPERATED]

Applications for system operated certificates are sent to the IT Planning Directorate via an e-mail electronically. The application must also specify the system that will operate on behalf of the certificate-holder.

4.2 Certificate application processing

The RA controls the received documentation and enters the holder’s data in the Registration Web application.

Any rejection of the application is communicated by the RA to the applicant and (if present) to the interested third party.

Request validation is performed by the RA that receives the request and is managed via the same web application used to register holder’s application. After the approval, the RA forwards issue request to the CA infrastructure to proceed with the certification issuance.

4.3 Certificate issuance

The certificate is issued by the competent structures of the Head Office of the Bank of Italy with a dedicated system, located in a protected premises. The issuance of certificates is carried out in one of the following ways:

- decentralized, used to issue certificates for employees of the Bank of Italy[12];

[11] Via registered delivery service (PEC) or e-mail. 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, via mail or hand delivery.

[12] The shipping and delivery of the smartcard to the holder is not required because the holder is provided with a badge equipped with a cryptographic chip, received when hired. The employee authenticates, over HTTPS on the internal network of the Bank of Italy, to a web application for the certificate issuance. Once logged in, the web application interacts with the smartcard in order to check that the employee logged is actually associated with the detected smartcard. If successful, the application requests the applicant to choose PIN and PUK - that are appropriately stored in the smartcard - as well as a pass-phrase to be used for the recognition of the holder by help-desk in

- centralized[13], generally used for the issue of suspended certificates for external holders. At the end of issue operations the technical function of the Bank of Italy sends[14] the smartcards and its secret codes (PIN, PUK, pass-phrase) to the RA.

After a certificate is generated, the certificate requested and the related private key; and the CA certificates have been registered on the holder's smartcard.

At the completion of the process, the holder's certificate will be entered in the Certificate Registry; the date and time of issue will be logged.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

After the application has been recorded and validated by the RA, the certificates issuance is carried out via a fully automated process on secure communication channels (see section 6.7 Network Security Controls). At the end of the process, the certificate-holder's private key is stored in a HSM (Hardware Security Module) hosted in protected premises of the CA.
The secret codes to activate the private key are sent to holders by an encrypted message (see section 4.4).

The Bank of Italy shall inform the subscribers of the certificate issuance and shall communicate their availability through the RA for external holders or through automated functions for employees.

4.4 Certificate acceptance

The employees, when hired, receive the personal badge where to install the certificate and the acceptance procedure is closed by installing the certificate on the smartcard (decentralized mode).

For external holders, the RA - after receiving the envelopes containing the smartcard and the secret codes (PIN, PUK and pass-phrase)[15] - will invite the certificate-holder to come

the event of a suspension of certificates in emergency. At the end of this first phase, the system generates a cryptographic key pair. The certificate's private key is generated directly within the smartcard chip; the public key is sent to the CA server for certificate generation within the protected premises (in accordance with eIDAS and art. 33 par. 1 DPCM 22.02.2013). The possession of the private key by the certificate-holder is attested by the fact that requests are sent to the CA via a web application that checked (log phase) the association between the applicant and the smartcard. The CA sends back to the web application the related certificates; the web application inserts certificates on the smartcard.

[13] The issuance certificates process and the production of a secure signature device (smartcards, USB tokens) is managed by the competent Technical Function at the Head Office of the Bank of Italy. The authorized operator authenticates, using keys and certificates stored on specific smartcards, to the web application for the certificates issue by opening a session to the Certification Authority. The operator generates the smart card containing the private key and the public key of the certificate-holder.

[14] With separate carriers.

[15] The PIN must be entered in order to carry out signature and other operations connected with the use of certificates and may be changed by the holder the first time he or she uses the device. The PUK serves to unblock the smartcard after the wrong PIN has been entered a pre-determined number of times.

to the RA for the purpose of identification with a valid document (as described in section 3.2). After performing identification, the RA will deliver the envelopes containing the smartcard and secret codes and indicates to the applicant where the present document is available. Certificates are suspended until the delivery of the smartcard. After the delivery, the RA activates the certificate and registers the delivery using the Registration Web application.

A record will be made of the delivery of qualified electronic signature creation devices. The RA maintains the record for future reference.

[1.3.76.38.1.1.1.2 REMOTE]

Certificate-holders receive secret codes encrypted (PIN, seed[16] to initialize an OTP generator – One Time Password) via e-mail or envelope to activate their private key stored in a HSM. When requested by the signature infrastructure, the certificate-holder must authenticate using username and two factors:

- PIN, verified by HSM;
- OTP, which is generated each time a signature operation is carried out and is checked by HSM.

[1.3.76.38.1.1.1.3 SYSTEM OPERATED]

Certificate-holders receive a PIN encrypted. The PIN must be used to delegate a system to operate on their behalf and is requested by the web application dedicated to make association between certificate-holders and system operations (see section 6.4).

4.5 Key pair and certificate usage

The qualified signature key pair gives proof of the source and integrity of the electronic document/group of documents. Each key pair is assigned to one and only certificate-holder.

Certificate-holders are responsible for the correct use of certificates and safekeeping of the devices containing them or authentication tools; certificate-holders must use them only for the purposes for which they were issued, keep them in their own exclusive possession and inform the Bank of Italy, by the prescribed procedures, of every event that might compromise their functionality. In particular, certificate-holders conserve 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. Holders must protect their private keys from unauthorized use and stop using the private key after its expiration or revocation of the certificate.

Holders must independently assess:

- that the certificate is used in accordance with extensions of the KeyUsage and ExtendedKeyUsage fields included in the certificate.
- the status of the certificate and use it only if the status is "valid".

[16] It is necessary a mobile (smartphone) with an app conveniently initialized with a seed in order to generate an OTP code.

Relying parties must assess if a given certificate is appropriate for the specific purpose indicated in the present document.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

Certificate-holder’s private keys are stored in a server with security countermeasures (HSM) on dedicated and protected premise of the Bank of Italy. Certificate-holders are responsible for authentication tools to use for signing.

HSM requires a two factors authentication. All operation and communication are carried out in a secured infrastructure (see section 6.7 Network Security Controls).

[1.3.76.38.1.1.1.3 SYSTEM OPERATED]

The circumstance that the signature is made by the use of a system operated procedure is specified in the certificate (“CertificatePolicies” field).

4.6 Certificate renewal[17]

The Bank of Italy renews certificates changing the subscribers’ public key (see section 4.7).

For the scope of this document, every reference to a renewal procedure means the issue of a new certificate with a new key pair (re-key).

4.7 Certificate re-key

With a certificate re-key[18], the Bank of Italy issues to certificate-holders new certificates with new public keys.

For the Bank of Italy employees, when the expiration of certificates approaches, an e-mail message invites the employees to access the web application in order to start the re-key process.
The process of re-key in decentralized mode (for employees) involves the reuse of the smartcard already held by the holder. The possession of the private key by the certificate-holder is attested by the fact that requests are sent to the CA via a web application that checked (log phase) the association between the applicant and the smartcard.
The transaction involves the deletion of the expiring certificate on the smartcard.

For external applicants, when the expiration of certificates approaches, the RA will ask interested third parties whether, for each holder, it is necessary to issue a certificate.
If the answer is affirmative, the interested third party must send the competent RA a note signed by its legal representative or other duly appointed person, indicating the holder data

[17] RFC 3647 provides as renewal the issue of a new certificate without changing the holder’s public key.

[18] This procedure is also indicated as renewal in the application form.

and the purposes for which re-key is requested; the holder's application for re-key, signed by the holder, must be attached to such note[19].
The RA will invite the certificate-holder to come to the RA for the purpose of identification and for delivery of the new smartcard containing the renewed certificates and related secret codes; on such occasion the smartcard containing the expiring certificates will be withdrawn after they have been rendered unfit for use by cutting the microcircuit. The holder is identified by a valid document.
A record will be made of the delivery. The RA maintains the record for future reference. Delivery of the new smartcard and the related secret codes will give rise to the subsequent activation of the certificates.

Following a revocation due to loss, theft, breach of security or deterioration, the Bank of Italy, acting on its own authority, initiates the procedure for certificate re-key.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

With reference to remote and system operated modes, certificate re-key is automatic.

4.8 Certificate modification

The certificate-holder must notify the Bank of Italy any changes to the information provided at the time of registration: personal data, residence, telephone numbers, e-mail address, etc.

Where changes impacts on certificate contents, a new certificate will be issued according the re-key procedure.

[19] Via registered delivery service (PEC) or e-mail.. The PEC must be compliant to "Codice dell'Amministrazione Digitale" requirements. If previous procedures are not available, via mail or hand delivery. The application is signed with a qualified signature. If a qualified signature is not available, it is necessary a copy of a valid identification document of the holder in attachment.

4.9 Certificate revocation and suspension[20]

Revocation

The holder or the interested third party may request - using application forms available on www.bancaditalia.it/firmadigitale - the competent RA to revoke a certificate for the causes listed in the following table.

In case of loss, theft or breach of security of the smartcard, the holder must contact the Help Desk for urgent suspension (see below).
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 certificate is revoked ex-officio.

APPLICANT **CAUSE**	**HOLDER** **(external person or employee)**	**INTERESTED THIRD PARTY** **(for external person)**	**BANK OF ITALY** **(for employee)**
LOSS OF SMARTCARD (after suspension)	X	-	-
THEFT OF SMARTCARD (after suspension)	X	-	-
BREACH OF SECURITY[21] (after suspension)	X	-	-
DETERIORATION OF SMARTCARD	X	X	X
CHANGE OF HOLDER'S POSITION[22]	-	X	X

For employees of the Bank of Italy, the request is sent to the RA by holders or by the unit to which the employee belongs. The RA inserts the request it into the Registration Web application (web application for the managing the lifecycle of certificates).

[20] When a certificate is revoked, its validity is terminated in advance. When a certificate is suspended, its validity is interrupted temporarily.

[21] 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).

[22] Cause to be cited where, for example, the holder ceases to work.

For external users, the revocation request must be submitted by the holder or the third party to the competent RA[23]. Where the request is submitted by the interested third party, it 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 needed, 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 directly or have it delivered 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 certificate renewal.

The Certifier suspends or revokes certificates by entering their serial number in the list of revoked and suspended certificates.
The suspension and revocation of a certificate take effect since the certificate is recorded in the aforesaid list (see section 7).

Revoked certificates must not be reactivated.

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

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

Certificates may be suspended or revoked by the Bank of Italy in case of circumstances provided for article 36 of D.Lgs. 82/2005[24].

[23] Via registered delivery service (PEC) or email. The PEC must be compliant to "Codice dell'Amministrazione Digitale" requirements. If previous procedures are not available, via mail or hand delivery. The application is signed with a qualified signature. If a qualified signature is not available, it is necessary a copy of a valid identification document of the holder in attachment.

[24] Qualified Trust Service Provider activities 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

Revocation and suspension for signature in remote mode or system operated on behalf of a natural person mode

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

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.

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.

Revocation of the certificates for the keys of the Certifying Entity

The Certifying Entity will revoke the certificate for CA key pair exclusively in the following cases:

- breach of security of the private key, i.e. an event compromising the reliability of its security features;
- cessation of the activity.

The revocation is implemented by inclusion of the certificate in the certificate revocation and suspension list and is notified to AgID within 24 hours and to all holders of certificates issued by the Certifying Entity that are signed with the private key belonging to the revoked pair.

Where the revocation is due to breach of security of the Bank of Italy’s private key, the Certifying Entity, acting on its own authority, revokes all the certificates signed with the before mentioned key.

Suspension

The holder or interested third party may request that a certificate’s validity be suspended for the causes listed in the following table.

APPLICANT CAUSE	HOLDER (external person or employee)	INTERESTED THIRD PARTY (for external person)	BANK OF ITALY (for employee)
LOSS OF SMARTCARD	X	--	--
THEFT OF SMARTCARD	X	--	--
BREACH OF SECURITY	X	--	--
PROLONGED ABSENCE OF THE HOLDER	--	--	X
OTHER[25]	X	X	X

Where the cause indicated is "other", suitable reasons must be provided.

For employees of the Bank of Italy, the request is sent to the RA by holders or by the unit to which the employee belongs or by the holder to Help-desk in case of emergency. The RA inserts the request it into the Registration Web application (web application for the managing the lifecycle of certificates).

For external users, the suspension request must be submitted by holder to the competent RA [26]. Where the request is submitted by the interested third party, it must be signed by the entity's legal representative or other duly appointed person.

The RA, verified the authenticity of the request, initiates the suspension procedure using the specific functionality of the web application for the managing the lifecycle of certificates.
The RA shall inform the holder and the interested third party, preferably by e-mail, about certificate suspension specifying the date and time since certificate is no longer valid.

Suspended certificates will be entered in the certificate revocation and suspension list, published in the Certificate Registry.

[25] Any other cause; for example, requests for revocation that interested third parties must submit in the event of cessation of their activity as a result of merger, liquidation, etc.

[26] Via registered delivery service (PEC) or e-mail. The PEC must be compliant to "Codice dell'Amministrazione Digitale" requirements. If previous procedures are not available, via mail or hand delivery. The application is signed with a qualified signature. If a qualified signature is not available, it is necessary a copy of a valid identification document of the holder in attachment.

Availability of the suspension service

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 (+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).

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 identity of the person submitting the request is not established, the certificate will be suspended on a precautionary basis. Within the subsequent 24 hours the person submitting the request must provide elements enabling him or her to be identified.

Reactivation of suspended certificates

The reactivation of a certificate must be requested by the same person who submitted the suspension request, by sending a reactivation request containing the identification data of the certificate-holder to the RA.
The reactivation request must be submitted in the same manner and by the same procedure described above for suspension requests other than urgent suspension requests.

The CA will reactivate the certificate by cancelling it from the certificate revocation and suspension list.

The RA notifies the holder and the interested third party of the reactivation of the certificate, specifying the date and time since the certificate is active again.

4.10 Certificate status services

The Bank of Italy provides a safe and timely service for revocation and suspension of electronic certificates as well as an efficient, timely and safe service of CRL.
The management of the certificate registry is done in order to ensure that only authorized persons can make entries and changes, that the authenticity of the information is verifiable, and that the authorized operator should be aware of any event that compromises the security requirements.
For further detail see section 7.

4.11 End of subscription

The certificate is no longer valid when it:

- expires and no effort was made to apply for the issue of a new certificate;
- is revoked.

4.12 Key escrow and recovery of CA keys[27]

The Bank of Italy has stored a backup copy of the certification key with the same security level in order to face a HSM out of order. In that case, a certification key recovery is carried out.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

For remote and system operated certificates, the private key is in HSM provided that only the holder can activate it as described in the present document (see section 6.4).

[27] “The Bank of Italy does not copy and not conserve the private qualified signature keys.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The Bank of Italy has defined specific policies for the confidentiality of information and ICT security and is compliant with European and national legislation on personal data protection.
The PKI infrastructure periodically receives a security assessment.

The Bank of Italy's PKI is included among business continuity measures foreseen for ICT essential services .

The Bank of Italy has a Business Continuity Plan to limit the adverse effects due to events of different nature, such as unavailability of logistical resources (structures, electricity), ICT (PCs, central systems, networks) and human resources. The Business Continuity Plan:

- lists critical processes and related responsible functions;
- establishes organizational and managerial roles and responsibilities at different levels;
- lists the recovery sites and protocols to use them;
- identifies personnel to ensure business continuity;
- contains procedural rules and information required for the activation and management of emergencies situations;
- establishes the rules to communicate in emergency situations;
- regulates how to go back to normal operating conditions.

5.1 Physical controls

5.1.1 Site location and construction

Bank of Italy's PKI infrastructure is located both in a primary and recovery secondary site. The premises are equipped with volumetric protection against intrusion.
The infrastructure has a high reliable configuration for recovery in case of disaster through:

- hardware and software physically installed on premise, at the primary site and the secondary site, linked together through a fiber optics network;
- Storage Area Network (SAN) configured in a synchronous remote copy with a secondary site.

Both sites are monitored and assisted by a access control service during office hours and protect by specific checkpoints during closing time.

5.1.2 Physical access

The operational activities of CA, all the activities related to the lifecycle of the certification process occur within premises that can be accessed only by authorized personnel, with restrictive physical tiers. The access is regulated by turnstile and a dedicated control system for PKI premises logs accesses on the audit log journal. Employee badges are used as proximity readers to grant access. The PKI time reference system is used to record access time in PKI premises and on procedures.

Located outside the PKI premises are the components that interoperate both with the Bank of Italy PKI network and with Internet, and the workstations to record users' credentials, and to submit requests to CA.
The workstations for the approval of the certificates issue requests do not require a physical security level higher than that of normal workstations.

5.1.3 Power and air conditioning

The datacenters of the Bank of Italy have redundant systems. The air-conditioning systems regulate temperature and control humidity. A supervision system monitors the state of technological systems (electrical and air conditioning systems) 24/7 all year round and allows to locate any anomaly quickly.

5.1.4 Water exposures

The system detects the presence of water due to breakage of the pipes and/or the air conditioning components, as well as to the eventual loss on waste water pipes in order to minimize the impact from exposure to water.

5.1.5 Fire prevention and protection

The prevention and protection measures have been designed in order to meet the local requirements of fire safety.
The fire prevention and protection system is composed by a smoke detection system and a fire suppression system.

5.1.6 Media storage

Devices containing personal data are processed according to the European and national legislation on personal data protection.

All media storage containing software and data, audit logs, archives, or backup information are stored within the datacenters of the Bank of Italy with adequate physical and logical access controls designed to limit access only to authorized personnel and protect such media from accidental damage.

Encryption materials are protected by locked safes, cabinets and containers. The opening and closing of cabinets or containers is recorded for audit checks.

5.1.7 Waste disposal

Before disposal cryptographic devices are physically destroyed or reset according to the manufacturers guidance.

5.1.8 Off-site backup

The Bank of Italy performs backups of critical system data, audit logs and other information necessary to recovery data correctly.

The secondary site is in synchronous remote copy.

5.2 Procedural controls

Certification Authority functions are carried out at the Head Office. The applicants data transmission from the RA to the CA takes place through a specific application within the corporate intranet.

Trusted roles for certification service management are appointed in accordance with eIDAS and DPCM 22.02.2013 (art. 39)are distributed among different Directorate of the Bank of Italy as reported in the following table and.

Roles	IT Operations Directorate (GES)	IT Development Directorate (SVI)	Internal Audit Directorate (REV)	Property Directorate (IMM)	Services and Logistics Directorate (LOS)
Certification service responsible		X			
Infrastructure evolution responsible (design and implementation of the IT architecture)		X			
Infrastructure security controls (Pre-Production Security Assessment)		X			
Application platform evolution responsible (design and implementation of applications)		X			
Physical Security Officer				X	
Logical Security Officer and Responsible for administration of technological components	X				
Security Officer (Security audits of infrastructure and applications during operations)	X				
Operations systems responsible	X				
Technical Services Manager	X				
Responsible of logistics services					X
Responsible of audits and			X		

inspections (auditing)					

The following roles are responsible for processing the data in accordance with European and national legislation on personal data protection: the Directors of Branches and Heads of Structures who register the requests; the Head of the IT Development Directorate that is the structure responsible for the certification service; the Head of Operations Directorate, which manages the issue of the certificates and the Help Desk activities; authorized personnel.

The Bank of Italy considers the following categories as trusted persons upon the existence of an employment relationship and/or a partnership:

- staff responsible for the administration of security (security officer);
- personnel authorized to install, configure and maintain the management systems of the certification service (system administrator);
- staff responsible for the daily management of the systems and authorized to perform backups (system operator);
- personnel authorized to consult archives and audit logs (system auditor).

The most critical functions are carried out with procedures based on "four eyes" control and a strong authentication process. Access to cryptographic modules is carried out by security officers and at least two trust roles are needed for the access.

Trust persons are all employees, contractors and consultants who may have a significant impact on:

- the information validation in certificate applications;
- acceptance, rejection or other certificate requests or revocation, renewal or enrollment requests;
- the certificate issuance or revocation, including personnel having access to restricted archives;
- processing of information and applications submitted by the subscriber.

5.3 Personnel controls

The service staff has the necessary experience in the design, development and management of PKI services and has received adequate training on the procedures and tools to be used in various operating phases.

In case of unauthorized actions or other violations of the policies and procedures of the Bank of Italy, the appropriate disciplinary measures are decided and are commensurate with the frequency and severity of actions.

The maintenance of the infrastructure is guaranteed through specialized support and maintenance services for the various components provided by third-party companies that operate, when necessary, on site following the guidelines set out by the Bank of Italy staff responsible of the management and infrastructure development. For professional services provided by external parties, a screening of consultants based on Curricula Vitae is performed.

The duties of the Bank of Italy employees are set out in the “Regolamento del personale” (rules for employees); duties of external parties are set out in the general conditions of contract for professional services.

5.4 Audit logging procedures

The audit logging procedures on PKI components are carried out using the audit log journal that automatically logs events relevant for security. The audit log journal is hosted in protected premises. In particular, the information stored within the audit log journal are:

- physical access to dedicated PKI premises;
- access to the procedure to issue certificates via administration console;
- sessions on CA systems and Directory Master;
- sessions on workstations for administrating, auditing, approving and for the certificate issue;
- issue, renewal, suspension, reactivation and revocation of certificates issued and publication of the revocation and suspension list on the copy of the certificate Reference Registry;
- alignment between the Operational and Reference copy of the certificate registry;
- customizing of signature devices;
- change in the Reference copy of the Register of certificates limited to the revocation and suspension list.

Operations to controls audit logs are carried out by dedicated workstation using a strong authentication and encrypted communication channels.
The Bank of Italy examines its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents on the CA and RA infrastructures.

Audit logs are available for 12 months and will be stored in order to provide proof of the certification in judicial proceedings even in the event of CA termination.

Event logging and retention period are compliant to eIDAS and national regulations (DPCM 22.02.2013) and to European and national legislation on personal data protection, in particular logical access to systems and electronic archives by system administrator are logged.

The troubleshooting activities related to system and application problems are performed using the information contained in all application infrastructure log files.
Logs file are examined weekly to identify possible security or operational anomalies.
Troubleshooting on log files includes: verifying the log file itself has not been tampered with, the inspection of all the logs of the file and an assessment of alerts or anomalies in the log file.
Audit logs and logs file are protected in such a way that confidentiality and integrity is guaranteed and unauthorized access is prevented. Incremental backups of audit logs are created every day and full backups are made weekly.

5.5 Records archival

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

The Bank of Italy must retain records of all the information concerning certificates from the time of their issue for twenty years, inter alia in order to provide proof of the certification in judicial proceedings.

Audit log records are stored for 20 years.

A incremental backup of records concerning information on the issued certificates is carried out every day, while a full backup is made weekly.

Back-up of CA key pairs are carried out as explained in section 6.

5.6 Key changeover

The certification keys are valid for 20 years. A CA certificate expires at least two years after the expiration of the certificates issued by the CA.
The Bank of Italy, ninety days before the expiry of the certificate relating to a certification key, will start the replacement procedure, generating a new certification key pair.
The replacement procedure will be carried out with the same requirements used for the generation and use of keys of the qualified trust service Provider (art. 30 DPCM 22.02.2103) taking care that the CA certificate expires at least two years after the expiration of the certificates issued to holders.
In addition to the certificate (self-signed) relating to the new pair of above certification keys, the Bank of Italy will generate:

- a certificate of the new CA public key signed with the private key of the old CA key pairs;
- a certificate of the old CA public key signed with the new CA private key.

CA certificates above mentioned will be sent to AgID for updating the Trusted List.

5.7 Compromise and disaster recovery

The Bank of Italy shall revoke its certificate of CA key pairs in case of private key compromise, as diminished reliability of key security characteristics or CA termination, according to the procedure given in section 4.9.

The Bank of Italy provides technical and organizational system to manage all events that determine impacts on system availability (malfunctions), the integrity and confidentiality of the treated information (security incidents). In reference to the PKI, the following are considered of particular importance:

- failure to publish the list of revoked or suspended certificates (CRL);
- failure to update within due periods the aforementioned lists;
- failures in CA Service and HSM devices that contain private keys.

Even in the absence of security incidents, vulnerabilities in operating systems and computer procedures are annually identified and analyzed and patching is periodically done.

In case of security incidents that can have particular impact on the certification service and on personal data, the Bank of Italy shall inform, within 24 hours since the incident has been identified, AgID and the national supervisory authority for privacy and where applicable, the concerned authorities, about all breaches of security or loss of integrity that

had a significant impact on the service provided or on held personal data (eIDAS Regulation, art. 19).
If the accident could have impacts on the holder of the certificate, the Certifier shall inform the holder using the contact information provided during registration.

In case of unavailability of all hardware and software or telecommunications infrastructure of the primary site, specific procedures for disaster recovery take place in order to restore, at the secondary site, the processing situation immediately prior to the disastrous event, with no data loss for all computer procedures and infrastructure services. New certificates will be not issued for external staff until systems of the primary site will be recovered.

5.8 CA termination

In case of termination, the Bank of Italy will not appoint a qualified trust service provider as substitute and will implement the following termination plan.

- At least 60 days before the scheduled date of termination, the Bank of Italy will:

  1. inform the national supervision authority of qualified trust service providers (AgID), all users of the CA service and all other relevant institutional parties ;
  2. notify holders that all certificates not expired at the time of cessation will be revoked (CAD art. 37, comma 1);
  3. retain records and 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 legal and/or administrative proceedings (eIDAS Regulation art. 24, par. 2, lett. H - CAD art 32, par. 3, lett. J);
  4. plan the destruction of the private keys used to sign in remote mode and related cryptographic modules;
  5. agree with AgID procedures to make available information about revoked certificates.

- At the date of termination, the Bank of Italy will:

  1. revoke active certificates belonging to the terminated CA;
  2. destroy private keys to sign in remote mode and related cryptographic modules to avoid possible regeneration. A record is made of this operation;

1. update the certificate revocation and suspension list for the last time and make the CA key pair unusable.

6 TECHNICAL SECURITY CONTROLS

The PKI is logically separated from other IT infrastructure of the Bank of Italy and has its own network equipment, physical servers and virtual machines, management console. The hardware installed at the primary and secondary site is:

- computers, storage systems, interconnection and perimeter devices, located for each site, in special cabinets (rack);
- console workstations for each site for the configuration management.

The servers are configured in cluster, which allows to ensure the recovery of the main application and system resources.

Certificates requests are carried out through a web application accessible exclusively on the internal network of the Bank of Italy.

6.1 Key pair generation and installation

The following keys are generated by the CA:

- certifying keys, used by the Bank of Italy to sign electronically the certificate-holder's certificate and the revocation and suspension list. The CA certification keys are valid for 20 years. Certificates issued to holders have a shorter validity period than the certification keys.
- qualified electronic signature keys, given to the certificate-holder by the Certifier, also to sign in remote and system operated mode. Each key pair is attributed to a single holder.

Each key pair can be used only for the type of operations it has been created for.

The type of operation which can be performed with the key pair is reported in the certificate.

Key pairs generation

The CA key pair generation takes place in a physically secure environment, following a procedure that requires the combined intervention of at least two different people ("dual control"). The operation of the procedure ("key ceremony") is recorded in a report kept by the security officer.

The end-user key pair generation takes place within the qualified secure device.

The key pairs (public and private) are generated by the Bank of Italy using devices and procedures that guarantee – in compliance with the current scientific and technological knowledge - the uniqueness and the solidity of the generated key pair and the secrecy of the private key. The aforementioned device and procedures guarantee:

- the generation of asymmetric key pairs with the same generation probability of all the possible key pairs;
- the electronic identification of the person who starts the generation procedure;
- protection of the private key from unauthorized access
- the cipher cryptographic elaborations;
- the correspondence of the pair to the requirements due to the generation and verification algorithms used;

- that during qualified signing operations and other operations connected to the use of certificates the signature module never communicates the private keys of the certificate-holder externally.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

The key pair for remote and system operated qualified electronic signature is different from all others in the possession of the holder.

Key length and algorithms

Key pairs shall have an adequate size in order to prevent others from determining the private key using cryptanalysis.

The certification keys are 4096 bit long.

The holders' keys are 2048 bit long.

The algorithm used for the generation of the keys is RSA (Rivest-Shamir-Adleman algorithm) with a public key exponent of 65537 value (0x10001).

The hash function to generate fingerprints is SHA256encryption.

Certificates generation and installation

The certificate is generated using a system dedicated only to this function and in a protected space. The procedures to install the certificates on signature devices are described in paragraph 4.3.
At the end of the issue operations, an entry concerning the certificate issued is made in the Register of certificates; date and time of issue are logged.
The state of the certificates is available as described in this document (cfr. Chapter 7).

The CA root certificate is in the ISO 9594-8 format.

The holder's keys, the related certificate and CA certificates are stored in an electronic device (smartcard or USB token) that has a microchip with cryptographic functionalities.

[1.3.76.38.1.1.1.2 REMOTE], [1.3.76.38.1.1.1.3 SYSTEM OPERATED]

To implement a remote and system operated signature system, the Bank of Italy has a specific infrastructure based on a high-security certificate system which shields holders' private keys and certificates and has defined a process their generation and release to end-users. The certificate and private keys for remote and system operated signature are recorded in HSM, stored in CA protected premises.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The Bank of Italy has implemented a combination of physical, logical and procedural controls in order to ensure the security of private keys.

The Bank of Italy does not act as a depositary of data for the creation of the holder's signature nor copies or maintains the private keys of the holder.
The certificate-holder is required to ensure the safekeeping of the security device and to adopt every organizational and technical measure to avoid the loss, dissemination, modification or non-authorized use of the private key.
The certificate-holder must conserve the device containing the private key and secret codes (PIN, PUK and pass-phrase) or authentication tools received from the Bank of Italy separately and with the utmost diligence, in order to ensure their integrity and maximum confidentiality.

System to issue certificates

The software product to manage certificates is implemented using a cryptographic toolkit certified FIPS 140-2 L3.

Cryptographic devices for CA keys

The device HSM which contains the CA private key meets the Common Criteria EAL 4+ certification .
The device management operations are performed by applications installed on the system for issuing the certificate or using functionalities directly on board of the HSM. The administrative tasks are authorized by trusted persons through the use of hardware keys.
The Bank of Italy adopts technical and procedural mechanisms that require the participation of a number of people authorized to perform cryptographic operations sensitive for the CA.
These copies can be used in circumstances in which, due to malfunctioning or impossibility to use the original key, the continuity of the service cannot be guaranteed using the production plants and systems.
In the event of disposal or replacement as a result of failure of the HSM, data on the device are safely and permanently deleted, in accordance with the procedures issued by the manufacturer.
At the end of their life cycle, the CA key pair and the device that contained them are safely destroyed. Operations are conducted on the principle of "four-eyes" and a record is made.

Cryptographic devices for holder's key

The qualified electronic signature creation devices used by the holders are certified Common Criteria EAL4 + (protection Profile CWA14169) and meets the requirements of Annex II of the eIDAS Regulation (Requirements for qualified electronic signature creation devices).
The following qualified electronic signature creation devices are used: smartcards (for the Bank of Italy employees smartcards are integrated with personal badges); USB tokens for certain categories of external users. The certificate-holder's access to the private key is protected by a PIN code.

The following operations take place during the security module personalization:

- acquisition of the certificate-holder's identification and matching him/her to the device;
- registration, in the security module, of the identification data held by the Bank of Italy;
- registration of the holder's qualified certificate-holder in the security module.

The responsibility of private key protection and his/her security device is in charge to the holder .
The certificate-holder’s private key cannot be drawn, at the current technological level, from the hardware security modules in which they are lodged.
The Bank of Italy does not duplicate private keys nor the hardware security modules that host them.

[1.3.76.38.1.1.1.2 REMOTE]

The remote mode signature and the set of authentication tools used to issue the remote signature are carried out using technical and organizational measures approved, for their respective responsibilities, by AgID and OCSI (art. 35 of the CAD with regard to safety of HSM and process), in order to guarantee the exclusive control of the private key by the holder.
The HSM used for remote signature is certified Common Criteria EAL4 and all the security operations take place using a system protected by hardware and software anti-tamper measures.
The process of issue and delivery of remote signing keys and the related certificates takes place in accordance with art. 12 and 13 of DPCM 22/02/2013, using a process articulated in different phases and based on secure communication channels (see section 6.7 Network Security Controls).
The remote signature architecture is characterized by fault tolerance and load balancing mechanisms along the entire processing chain; each component (hardware and software) is redundant in order to exclude a single point of failure. The same redundancy also applies to Hardware Security Module (HSM) devices on which the digital signature certificates are managed.

[1.3.76.38.1.1.1.3 SYSTEM OPERATED]

The architecture for the system operated signature has been implemented and optimized to provide signature solutions in an automatic mode; it uses the same HSM used for the remote signature, but with specific software components. The signature software interfaces are similar to the remote one in order to promote flexibility and integration of systems. The process of issue and delivery of system operated signing keys and the related certificates takes place in accordance with art. 12 and 13 of DPCM 22/02/2013, using a process articulated in different phases and based on secure communication channels (see section 6.7 Network Security Controls).

Private keys backup

Bank of Italy creates backup copies of CA private key for the purpose of routine and disaster recovery. During the certifying key generation process, the private keys are cloned on recovery modules with the same authorization features as the original ones and are stored in safe premises. When a backup of the CA key pair is created on another hardware cryptographic module, the key pairs are transported from one module to another one in encrypted form.

Back-up and key escrow (see section 4) are not allowed for holder’s private keys.

Private keys archival

CA private key is stored in hardware cryptographic modules in encrypted form.
When the CA key pair has reached the end of the validity period, it will be archived for a period of at least five years. The archived CA key pair will be stored in a secure environment using hardware cryptographic modules that meet the requirements of this CPS/CPs.

Holders' private keys are not archived.

Private keys destroy

If needed, the Bank of Italy destroys the CA private keys in order to ensure that there are no residues that could lead to reconstruct of them.
At the end of their lifecycle, the CA signing keys are securely destroyed and the containing hardware is securely disposed in accordance with the procedures issued by the manufacturer. The operations are carried out accordingly to the "four-eyes" principle and a report of such operations is made.

Subscriber private keys stored on a smartcard are destructed when the secure device (smartcard) is retired. The smartcard is permanently made unusable by cutting the microcircuit.

6.3 Other aspects of key pairs management

All issues connected with the management of key pairs have been dealt with in the previous sections.

6.4 Activation data

The CA private key is always active.

The certificate-holders activate the private key with the PIN entry after the insertion of the smartcard in the reader device.
Holders remove the smart card from the reader after each operation.

[1.3.76.38.1.1.1.2 REMOTE]

The remote mode requires the holder to carry out a two factor authentication at each signature.

To authenticate the holder on the remote signature infrastructure the HSM verifies authentication data: controls the holder's username/PIN and contacts the OTP server for a check on the OTP code that was generated on a mobile device owned by the holder . If all controls are successful, the holder's private key is activated.,

[1.3.76.38.1.1.1.3 SYSTEM OPERATED]

The certificate-holder enters a PIN and enables, through a web interface over HTTPS, a computer procedure to sign on its behalf. Following this authorization, the procedure activates the holder's private key using a secure communication channel (see section 6.7 Network Security Controls) toward the PKI.

6.5 Computer security controls

The infrastructure has been classified according to security, confidentiality and availability profiles and the relevant risk analysis and countermeasure selection have been carried out. In accordance with eIDAS the Bank of Italy uses trustworthy systems and products that are protected against modification and ensures the technical security and reliability of the processes they support. The security level of the assets, specifically the operational systems, has been hardened in accordance with DPCM 22.02.2013 art. 32, clause 1:all environments are subjected to a centralized management of the configuration and all services not necessary for the operation of the infrastructure PKI are disabled.

The Bank of Italy ensures that systems that hosts CA software and relating files are trusted systems secured against unauthorized access with strong authentication and limits access to production servers.

Users' privileges are profiled according to the principles of need-to-know and least privilege. High-privilege passwords are stored in a safe.

Access policy to certification systems are differentiated for core components (Certification Authority and directory master) and for support services (audit log system, components involved in the registration process, operational copy of the certificate registry).

Core components management activities are carried out on premises in a restricted area, or remotely, after authentication, via internal network protected by firewalls. Support services are carried out by authorized workstations on the internal network of the Bank of Italy.

The Directory Master of Certificate Registry is located in a secure area and accessible only by the CA system to register certificates issued and lists of revoked and suspended certificates.

The Bank of Italy uses reliable systems to manage the Register of certificates and only authorized persons can make entries and changes, authenticity of the information is verifiable and the operator is aware of any event that compromises the safety requirements. Upon request, the relevant information about certificates can be made accessible to third-parties relying on them.

Event logging is configured to monitor system events to make diagnostics and monitor the execution of specific commands.

All PKI workstations and servers are protected with antivirus software.

6.6 Life Cycle Security Controls

The security controls of the Bank of Italy guarantee, through the following support processes, the protection of computing resources, in terms of confidentiality, integrity, availability, verifiability and accountability along the entire life cycle of software and hardware infrastructure.

- IT risk analysis, aimed at the identification and risk assessment connected with the use of IT resources and security countermeasures suitable for ensuring the required security levels. The IT risk analysis process is completed through the conduction of a pre-production security assessment, prior to the release into operation. The risk analysis process steps are repeated on the occasion of major changes to the computer systems or upon the occurrence of significant incidents and, in any case, periodically, in order evaluate the technological environment evolution, as well as of threats and vulnerabilities.

- Security incidents management[28], the set of activities put in place in order to minimize the impact of the security incidents and to ensure the reactivation of services. The process is based on a formal procedure previously defined and periodically updated that has, among other things, the objective to collect and preserve all the information useful for the reconstruction of the events. The activity is completed with a follow-up phase in order to identify vulnerabilities that have made the incident possible in order to prevent further similar occurrences.
- Business continuity management of applications and information systems, aimed at limiting, within a predetermined level considered acceptable, the impact on the organization caused by incidents or disasters which, directly or indirectly, affect the proper conduction of critical processes and facilitate recovery in a short time of normal operating conditions.
- Change management for any changes to be made to operational systems is subject to a formal process, in order to ensure the maintenance of the security levels on the affected systems. Changes must be documented and submitted to a preliminary analysis to assess the possible impact on the operation, reputation and assets of the Bank of Italy. For most significant changes, the risk analysis is updated.
- IT security monitoring, several activities whose methods and frequency are established in the risk analysis. These activities include:
    - verification of compliance of the security configuration;
    - monitoring of significant security events in order to detect and report any potential threat;
    - identification of potential vulnerabilities in the configurations of the systems.
- Vulnerability and Patch Management process with the aim to identify and eliminate new vulnerabilities and thus potential risk situations, in order to preserve the confidentiality, integrity and availability of information, services and applications of the Bank of Italy.

6.7 Network Security Controls

The PKI infrastructure uses a layered defense approach, by placing servers and appliances on different network levels, separated by means of safety devices (firewall) which allow only authorized communication flows. The aggregation criteria of the servers and of the appliances in the various levels respond, in addition to a functional logic, to the possession of homogeneous security requirements.

The procedures to configure network components ensure the management of changes, the restriction of access to the components, prevention of unauthorized accesses/improper changes to the configurations.
The configuration procedures of network components ensure:

- the management of configurations changes;
- restricting access to components using a least privilege principle;

[28] A security incident is a breach or the imminent threat of a breach of rules and business practices of information security or of existing legal rules and the national and supranational level.

- prevention of improper or unauthorized accesses or changes.

The certification service uses a network-based security infrastructure firewalling mechanisms and TLS (Transport Layer Security) in order to realize a secure channel between all parties authorized to have access to CA. All network flows (protocols, source, destination) moving between different security domains are identified, classified and authorized. The system is also supported by specific security products (network intrusion detection, network intrusion protection, virus protection) and from all the relevant management procedures.
Periodically or after every significant change a penetration testing of the infrastructure is carried out.

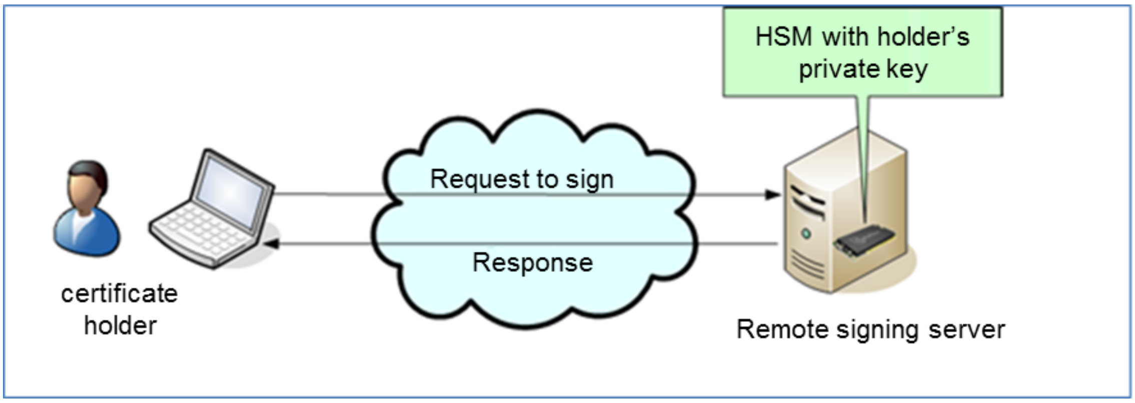
Access to the directory master is only possible from the CA. Access to operational copy of the certificate registry is done in different ways depending if the request is coming from external networks or from the internal network of the Bank of Italy:

- access from the public network (Internet) is filtered by the proxy server that, after analyzing and filtering requests, forwards them to the operational copy of the certificate registry;
- access from the internal network takes place directly on the operational copy of the certificate registry.

[1.3.76.38.1.1.1.2 REMOTE]

The Bank of Italy has its own on-premise remote signature service. In the signature in remote mode, the private key resides in a remote device (a HSM - Hardware Security Module), not in a secure device consigned to holders (eg. smartcard).
The infrastructure consists of an HSM, inside which the keys and digital certificates are generated and stored; a software component that manages communication flows towards HSM and the two factor authentication system for the correct activation of the remote digital signature service; web services to invoke a remote signature operation.

Data are exchanged with HSM through a secure network as sketched in the following figure.



The signature client could be a desktop application or a third application that invokes the signing server by software interfaces.

[1.3.76.38.1.1.1.3 SYSTEM OPERATED]

The same architecture for remote signature is used for the qualified signature by a system operated on behalf of a natural person. This mode, through the invocation of specific signing web services, allows IT procedures to sign documents on behalf of a natural person without requiring the intervention of the certificate-holder.
The certificate-holder delegates IT procedures to sign on his/her behalf using a specific web application ("gestione delle deleghe" portal).

6.8 Time-stamping

The certificates, the suspension and revocation list and other items stored on the database related to the revocation and suspension must specify time and date.

The time references derive from a system fed from an external source (ETS, External Time Source) supplied with satellite GPS synchronization. Such references correspond to the UTC(IEN) time scale.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The digital certificates issued by the Bank of Italy are signed with its CA 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 AgID provisions and with standard ETSI EN 319 412. As the same classification for 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).

Certificates are generated at the competent Head Office of the Bank of Italy with a dedicated system housed in appropriately protected premises. Only authorized operators may access the certificate generation system, and only for their assigned functions.
After a certificate is generated, it will be entered in the Certificate Registry; the date and time of issue will be memorized in the audit log journal.

The holder's certificate, in accordance with requirements laid down in Annex I of the eIDAS Regulation and with AgID provisions where applicable, contains:

- the indication that the certificate is qualified;
- the serial number or other identification code of the certificate;
- the name 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 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 key pair according to its 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 list of revoke certificates 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 qualified electronic signature certificates issued to holders have a maximum validity of 5 years.

Without prejudice to the foregoing, identification of the holder will be implemented by means of the Distinguished Name (DN) as provided for in ISO 9594-1.
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 Bank of Italy holds the information about the certificate for 20 years from the date of issue of the certificate.

If a certificate is intended for a pair of certification keys, the use of such keys for certification will be indicated.

CA certificate profile

Field	Value	Critical
Version	V3	
Serial Number	<random bytes>	
Signing Algorithm	SHA256WithRSAEncryption	

Subject DN	CN=Banca d'Italia
	OU=Servizi di certificazione
	O=Banca d'Italia/00950501007
	C=IT	

SubjectPublicKeyInfo	<RSA 4096 bit PublicKey>	

Issuer DN	CN=Banca d'Italia
	OU=Servizi di certificazione
	O=Banca d'Italia/00950501007
	C=IT	

Signed By	Self Signed	
Validity (*y *mo *d) or end date of the certificate	20y (24/11/2014 – 24/11/2034)	
Extensions		
Basic Constraints	IsCA: true - Path length: 1	X
SubjectKeyIdentifier (SKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	
KeyUsage	Certificate Signing, CRL Signing , Off-line CRL Signing	X
CertificatePolicies	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale	

Default CRL Dist. Point	URL=ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList
	URL=http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
	CRL
	Nome punto distribuzione:
	Nome completo:
	Indirizzo directory:
	CN=CRLXXX
	CN=Banca d'Italia
	OU=Servizi di certificazione
	O=Banca d'Italia/00950501007
	C=IT	

End-entity signature certificate profiles

Employees			
Field	**Value for qualified signature** based on a qualified signature creation device hold by the signatory	**Value for remote signature**	**Value for signature** through a system operated on behalf of a natural person
Version	V3	V3	V3
Serial Number	<random bytes>	<random bytes>	<random bytes>
Signature	SHA256WithRSAEncryption	SHA256WithRSAEncryption	SHA256WithRSAEncryption

Issuer	CN = Banca d'Italia
	OU = Servizi di certificazione
	O = Banca d'Italia/00950501007
	C = IT
		CN = Banca d'Italia
		OU = Servizi di certificazione
		O = Banca d'Italia/00950501007
		C = IT
			CN = Banca d'Italia
			OU = Servizi di certificazione
			O = Banca d'Italia/00950501007
			C = IT

Validity	<5 y>	<5 anni>	<5 y>

Subject	SERIALNUMBER = TIN<Country Code>-<Codice fiscale>
	CN = <Last Name Name>
	G = <Name>
	SN = < Last Name>
	dnQualifier = <IUT>
	O = Banca d'Italia/00950501007
	C = IT
		SERIALNUMBER = TIN<Country Code>-<Codice fiscale>
		CN = <Last Name Name>
		G = <Name>
		SN = << Last Name >
		dnQualifier = <IUT>
		O = Banca d'Italia/00950501007
		C = IT
			SERIALNUMBER = TIN<Country Code>-<Codice fiscale>
			CN = <Last Name Name >
			G = <Name>
			SN = < Last Name>
			dnQualifier = <IUT>
			O = Banca d'Italia/00950501007
			C = IT

SubjectPublicKeyInfo	<RSA 2048 bit PublicKey>	<RSA 2048 bit PublicKey>	< RSA 2048 bit PublicKey >
Extensions			
AuthoritykeyIdentifier (AKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>

SubjectKeyIdentifier (SKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>
KeyUsage	Non repudiation	Non repudiation	Non repudiation
CertificatePolicies	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [1,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso=I titolari fanno uso del certificato solo per le finalita' di lavoro per le quali esso e' rilasciato. The holder must use the certificate only for the purposes for which it is issued. [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1.1 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= Il presente certificato è valido solo per le firme apposte con l'utilizzo di un dispositivo crittografico qualificato sicuro custodito dal titolare. / This certificate may only be used with a qualified signature creation	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale/footer [1,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso=I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso e' rilasciato. The holder must use the certificate only for the purposes for which it is issued. [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1.2 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso=Il presente certificato è valido per la firma apposta in modalità	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [1,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The holder must use the certificate only for the purposes for which it is issued. [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1.3 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= Il presente certificato è valido solo per firme apposte con procedura automatica. / This certificate may only be used through a system that will operate on behalf of a natural person.

	device hold by the signatory. [3]Criterio certificato: Identificatore criterio=1.3.76.16.6	remota. / This certificate may only be used in remote mode. [3]Criterio certificato: Identificatore criterio=1.3.76.16.6	[3]Criterio certificato: Identificatore criterio=1.3.76.16.6
AuthorityInformationAccess (AIA)	URL=http://ocsp.firmadigitale.bancaditalia.it/ocsp	URL=http://ocsp.firmadigitale.bancaditalia.it/ocsp	URL=http://ocsp.firmadigitale.bancaditalia.it/ocsp
QcStatement	id-etsi-qcs-QcCompliance id-etsi-qcs.3 id-etsi-qcs.4	id-etsi-qcs-QcCompliance id-etsi-qcs.3 id-etsi-qcs.4	id-etsi-qcs-QcCompliance id-etsi-qcs.3 id-etsi-qcs.4

CRLDistributionPoints
(CDP)
	URL=ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList
	URL=http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
	CRL
	Nome punto distribuzione:
	Nome completo:
	Indirizzo directory:
	CN=CRLXXX
	CN=Banca d'Italia
	OU=Servizi di certificazione
	O=Banca d'Italia/00950501007
	C=IT
		URL=ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList
		URL=http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
		CRL
		Nome punto distribuzione:
		Nome completo:
		Indirizzo directory:
		CN=CRLXXX
		CN=Banca d'Italia
		OU=Servizi di certificazione
		O=Banca d'Italia/00950501007
		C=IT
			URL=ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList
			URL=http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
			CRL
			Nome punto distribuzione:
			Nome completo:
			Indirizzo directory:
			CN=CRLXXX
			CN=Banca d'Italia
			OU=Servizi di certificazione
			O=Banca d'Italia/00950501007
			C=IT

Default OCSP Service	ocsp;uniformResourceIdentifier: http://ocsp.firmadigitale.bancaditalia.it/ocsp	ocsp;uniformResourceIdentifier: http://ocsp.firmadigitale.bancaditalia.it/ocsp	ocsp;uniformResourceIdentifier: http://ocsp.firmadigitale.bancaditalia.it/ocsp

Locator			

Externals			
Field	**Value for qualified signature** based on a qualified signature creation device hold by the signatory	**Value for remote signature**	**Value for signature** through a system operated on behalf of a natural person
Version	V3	V3	V3
Serial Number	<random bytes>	<random bytes>	<random bytes>
Signature	SHA256WithRSAEncryption	SHA256WithRSAEncryption	SHA256WithRSAEncryption

Issuer	CN = Banca d'Italia
	OU = Servizi di certificazione
	O = Banca d'Italia/00950501007
	C = IT
		CN = Banca d'Italia
		OU = Servizi di certificazione
		O = Banca d'Italia/00950501007
		C = IT
			CN = Banca d'Italia
			OU = Servizi di certificazione
			O = Banca d'Italia/00950501007
			C = IT

Validity	<5 y>	<5 y>	<5 y>

Subject	SERIALNUMBER = <Country Code>:<Tax identification number>
	CN = <Last Name Name>
	G = <Name>
	SN = < Last Name>
	dnQualifier = <IUT>
		SERIALNUMBER = <Country Code>:<Tax identification number>
		CN = <Last Name Name>
		G = <Name>
		SN = < Last Name>
		dnQualifier = <IUT>
			SERIALNUMBER = <Country Code>:<Tax identification number>
			CN = <Last Name Name>
			G = <Name>
			SN = < Last Name>
			dnQualifier = <IUT>

SubjectPublicKeyInfo	< RSA da 2048 bit Public Key>	< RSA da 2048 bit Public Key>	< RSA da 2048 bit Public Key>
Extensions			
AuthoritykeyIdentifier (AKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>

SubjectKeyIdentifier (SKI)	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>	<KeyIdentifier according to first method of RFC5280 section 4.2.1.2>
KeyUsage	Non repudiation	Non repudiation	Non repudiation
CertificatePolicies	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [1,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= L'utilizzo del certificato e' limitato ai rapporti con la Banca d'Italia. The certificate may be used only for relations with the Bank of Italy. [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1.1 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= Il presente certificato è valido solo per le firme apposte con l'utilizzo di un dispositivo crittografico qualificato sicuro custodito dal titolare. / This certificate may only be used with a qualified signature creation	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale/footer [1,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= L'utilizzo del certificato e' limitato ai rapporti con la Banca d'Italia. The certificate may be used only for relations with the Bank of Italy. [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1.2 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso=Il presente certificato è valido per la firma apposta in modalità remota. / This certificate may only be used in remote mode.	[1]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://www.bancaditalia.it/firmadigitale [1,2]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= L'utilizzo del certificato e' limitato ai rapporti con la Banca d'Italia. The certificate may be used only for relations with the Bank of Italy. [2]Criterio certificato: Identificatore criterio=1.3.76.38.1.1.1.3 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=Notifica utente Definizione: Testo avviso= Il presente certificato è valido solo per firme apposte con procedura automatica. / This certificate may only be used through a system that will operate on behalf of a natural person. [3]Criterio certificato:

	device hold by the signatory. [3]Criterio certificato: Identificatore criterio=1.3.76.16.6	[3]Criterio certificato: Identificatore criterio=1.3.76.16.6	Identificatore criterio=1.3.76.16.6
AuthorityInformationAccess (AIA)	URL=http://ocsp.firmadigitale.bancaditalia.it/ocsp	URL=http://ocsp.firmadigitale.bancaditalia.it/ocsp	URL=http://ocsp.firmadigitale.bancaditalia.it/ocsp
QcStatement	id-etsi-qcs-QcCompliance id-etsi-qcs.3 id-etsi-qcs.4	id-etsi-qcs-QcCompliance id-etsi-qcs.3 id-etsi-qcs.4	id-etsi-qcs-QcCompliance id-etsi-qcs.3 id-etsi-qcs.4

CRLDistributionPoints
(CDP)
	URL=ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList
	URL=http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
	CRL
	Nome punto distribuzione:
	Nome completo:
	Indirizzo directory:
	CN=CRLXXX
	CN=Banca d'Italia
	OU=Servizi di certificazione
	O=Banca d'Italia/00950501007
	C=IT
		URL=ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList
		URL=http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
		CRL
		Nome punto distribuzione:
		Nome completo:
		Indirizzo directory:
		CN=CRLXXX
		CN=Banca d'Italia
		OU=Servizi di certificazione
		O=Banca d'Italia/00950501007
		C=IT
			URL=ldap://ldap.firmadigitale.bancaditalia.it/cn=WinCombined1,cn=Banca%20d'Italia,ou=Servizi%20di%20certificazione,o=Banca%20d'Italia/00950501007,c=IT?certificateRevocationList
			URL=http://www.firmadigitale.bancaditalia.it/crl/crl1.crl
			CRL
			Nome punto distribuzione:
			Nome completo:
			Indirizzo directory:
			CN=CRLXXX
			CN=Banca d'Italia
			OU=Servizi di certificazione
			O=Banca d'Italia/00950501007
			C=IT

7.2 CRL profile

The Certificate Registry contains all the certificates issued by the Bank of Italy and the suspension and revocation list.
Revocation, suspension and subsequent reactivation of the certificates are registered in the audit log journal indicating the date and time of execution.
One or more copies (directory shadows) are made of the Certificate Registry (directory master). The directory master is updated every time a certificate is issued, suspended or revoked. The directory shadows are copies of the contents of the directory master. All the operations that modify the contents of the directory master are registered in the audit log journal. The shadows are updated each time the directory master is updated..
The Certificate Registry (directory master), impossible to access from the outside, is located on a safe system on Bank of Italy's network accessible only from the CA system that generates the certificates and registers on the registry the issued certificates and the list of suspended and revoked certificates. The operational copy is also accessed from Internet.

The CRL is published at least every 24 hours. The revocation of a certificate is promptly published.

The CRL conforms to the international standard ISO / IEC 9594-8 X.509 and public standard RFC 5280.

In addition to the mandatory fields, the CRL contains:

- the field nextUpdate (scheduled date for the next issue of the CRL);
- the extension CRLNumber (sequential number of CRL).

Furthermore, for every CRL item, the reasonCode is indicated to motivate the certification suspension or revocation.

The CRL is signed with sha256WithRSAEncryption algorithm.

The CRL can be consulted on one of the following Internet addresses without authentication:

- 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[29].

7.3 OCSP[30] Profile

The Bank of Italy OCSP conforms to RFC 6960, 2560 and 5019.

[29] Access to operational copy is carried out, via LDAP in accordance with RFC 1777, via URL in accordance with RFC 2255.

[30] OCSP (Online Certificate Status Protocol) is a protocol to obtain timely information on the status of a particular certificate revocation.

Private keys to sign OCSP response are stored in a HSM partition dedicated and separated from the partition containing root CA keys.

The OCSP service is available at http://ocsp.firmadigitale.bancaditalia.it/ocsp.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The Bank of Italy, in compliance with eIDAS Regulation, shall be audited at its own expense at least every 24 months by an external conformity assessment body recognized by Accredia (Regulation (EC) n. 765/2008 'art. 2 clause 13). The Bank of Italy submits the resulting conformity assessment report to the national supervision authority of trust service providers (AgID).

AgID carries out inspection in accordance with its supervision role foreseen by eIDAS and CAD (art. 14 bis) then it can carry out assessment or gives mandate to a conformity assessment body at expense of Bank of Italy.

8.2 Identity/qualifications of assessor

Compliance assessments are carried out by assessment bodies independent of the Bank of Italy.

8.3 Assessor's relationship to assessed entity

There is no pre-existing corporate or professional relationship between the Bank of Italy and external assessors that could in any way affect the outcome of the audits.

8.4 Topics covered by assessment

The assessment carried out by the external auditors is aimed at verifying the compliance of the provider and the provided services to accreditation schemas.

8.5 Actions taken as a result of deficiency

As a result of deficiency, the CA shall take the necessary corrective measures, on pain of suspension or revocation of accreditation.

8.6 Communication of results

The compliance assessment is sent to AgID by the Structure of the Bank of Italy responsible for the certification service.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fees are charged.

9.2 Financial responsibility

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

9.3 Confidentiality of business information

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 the information about the certificate-holders that are not publicly available through the certificate or through revocation and suspension list online are treated as confidential. In particular:

- holders' data and issue requests;
- holders' private keys and information needed to recover such private keys;
- transactional data (full records or trace audits log on operations);
- emergency plans and disaster recovery plans;
- security measures of the hardware and software operations relating to the certification services.

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

The Bank of Italy employees are committed to maintaining professional secrecy. Contracted personnel that take part in any PKI activities or operations are subject to the duty of professional secrecy within the framework of their contractual obligations with Bank of Italy.

9.4 Privacy of personal information

The Certifier must adopt safety measures for the treatment of personal data in compliance with the minimum safety measures for handling of personal data provided by eIDAS and European and national legislation on personal data protection and subsequent amendments and additions.

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

9.5 Intellectual property rights

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 the

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 at the national competent body for the release of these codes (UNINFO). No OID assigned to Bank of Italy may be used, partially or fully, except for the specific uses included in the certificate.

9.6 Representations and warranties

For obligations and responsibilities of different roles involved in the certification service or that use certificates, see section 1.3.

9.7 Disclaimers of warranties

See section 9.8.

9.8 Limitations 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 this CPS/CPs;
- 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 the sole responsible for fulfilling all the obligations established by law and referred to in this document.

The Bank of Italy will also be 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.

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.

9.9 Indemnities

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

9.10 Term and termination

The CPS/CPs are the reference document for holders that have a valid certificate issued by Bank of Italy and shall come into force from the moment it is published on the Bank of Italy website and shall remain valid until it is expressly terminated due to the issue of a new version of the CPS/CPs or because the termination of the certification service.

9.11 Individual notices and communications with participants

All notifications and any other type of communication shall be carried out by Bank of Italy via(e-mail or registered delivery service - PEC).

Holders communicate with Bank of Italy as described in chapters 3 and 4.

The Bank of Italy contacts are indicated in section 1.5.

9.12 Amendments

Updates of this document are performed updating this entire document or by addendum and are notified to national supervision Authority and conformity assessment entity.

New versions are indicated with an integer followed by a decimal that is zero. Minor changes are indicated through one decimal number greater than zero.

New versions are available for users on the Bank of Italy web site.

9.13 Dispute resolution provisions

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

9.14 Governing law

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. In addition, the Bank of Italy 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 European and national legislation on personal data protection.

9.15 Compliance with applicable law

The Bank of Italy certification service is compliant with the applicable legislation stated under the previous section.

The Bank of Italy shall be audited at their own expense at least every 24 months by a conformity assessment body (see section 8.1) and submit the resulting conformity assessment report to the national supervisory body (AgID).

9.16 Miscellaneous provisions

Operational procedure for the generation of digital signatures

Digitally signing a document implies the following operations:

- calculation of the fingerprint of the document using the mathematical function called hash;
- ciphering of the fingerprint thus obtained using an asymmetric algorithm RSA that uses the private key of the certificate-holder lodged in the smart card.

The certificate-holder carries out these operations using the signing software and the smart card given by the Bank of Italy.
The software allows to select the document which needs to be signed and allows the certificate-holder to see a preview of it before signing it; when the certificate-holder decides to sign the document, the software asks for a confirmation of the intention to sign the previewed electronic document.
In case of an affirmative answer, it is necessary to insert the card in the reader, type the PIN code in and thus produce the signed digital document.

Document format

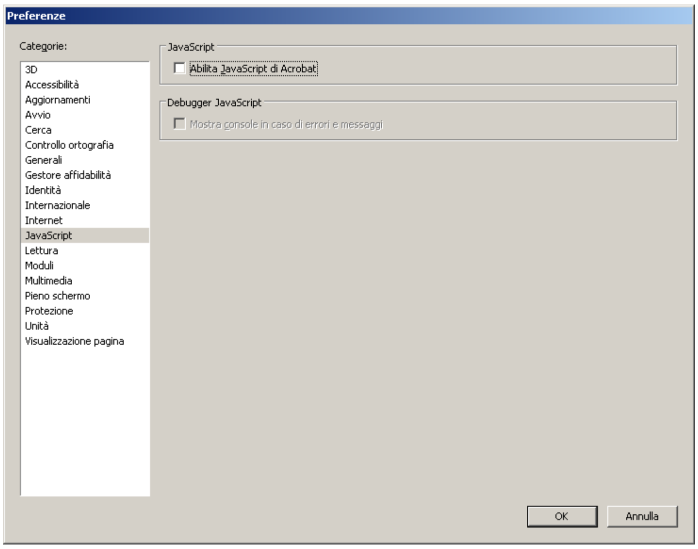
Office automation has introduced the use of document formats that enrich the “contents” of the document with macros o executable codes that are aimed, for example, at increasing the reuse of the document (es. forms, data fields, page numbering, text format) or performing mathematical calculations..
The code elements interpreted by the software package could alter the original contents of the document, thus altering “acts, facts or the data contained in the document” (DPCM 22.2.2013, art. 4, paragraph 3) when signing.

It is thus advisable to use static formats, such as:

- text – “.txt”;
- Portable Document Format – “.pdf” (if without form fields or javascript).

When it is necessary to use formats like .doc, .dot, .rtf, .xls, before signing the document it is necessary to identify any dynamic field such as the following ones.

- Macros. A macro is a procedure, written in a specific programming language, which allows the automatic running of a sequence of operations when using Microsoft Office® products..
- Field codes. Field codes are objects which allow dynamic values such as page numbers, indexes, cross-references, etc., to be inserted in the document.
- Objects. To test for the presence of external references in a MS Word® document, like, for example, an MS Excel® sheet, choose Structure from the menu View.
- Formulas.
- Javascript. PDF documents can contain Javascript code that adds dynamic functions to validate forms, access local databases and control multimedia objects. Javascript code in Adobe® Reader is enabled by default; to disable it choose Preferences from the Modify menu; select Javascript from the column on the left and deselect the option Enable Acrobat Javascript (the following picture refers to Adobe® Reader version 7).



Preferenze

JavaScript

☐ Abilita JavaScript di Acrobat

Debugger JavaScript

☐ Mostra console in caso di errori e messaggi

9.17 Other provisions

There are no further provisions other than the ones indicated in the previous sections.