BANCA D'ITALIA
EUROSISTEMA

# PUBLIC-KEY CERTIFICATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES

## PUBLIC KEY INFRASTRUCTURE (PKI)

## DISCLOSURE STATEMENT

Version 1.3 - 01/02/2022

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

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

The service is carried out in compliance with:

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

Certificates are issued to[2]:

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

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

---

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

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

## 1. TSP contact info

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

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

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

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

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

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

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

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

The Bank of Italy is responsible for the qualified certification service; the relevant tasks are allocated to the 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 | 06/47921 |
| Help Desk for urgent suspension requests | +39 06 47929361 |

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

**Person responsible for the Certification Practice Statement**

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

## 2. Certificate type, validation procedures and usage

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

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

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

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

- the holder's identification code at the Certifying Entity;
- the holder's given name, family name, tax identification number and date of birth;
- the certificate's terms of validity;
- the Certifying Entity's digital signature;
- the public key number;
- the usable generation and verification algorithms;
- the certificate signature algorithm;
- the type of the pair of keys according to their assigned use;
- the holder's e-mail address (optional);
- the location where the CA certificate is available free of charge;
- the internet address where the 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 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.

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

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

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

Issue

The applicant fills in and subscribes an application – using a specific application form (available on www.bancaditalia.it/firmadigitale) - 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.

When signing the application, the applicant declares to:

- be informed of the conditions of use of the certificates identified in CPS/CP 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 Certification Practice Statement/Certificate Policies and undertakes to fulfill the obligations established for them herein;
- have attached the certificate application form, drawn up and signed by the designated person.

The above-mentioned documentation must be sent[3] to the competent RA.

The RA controls the documentation and, after a validation phase via a Registration Web Application[4], forwards issue requests to the CA.

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

Data and documentation provided are handled through automated procedures strictly for the purposes described above and with the use of security measures to ensure the confidentiality of personal data and to prevent illegal access to data pursuant to European and national legislation on personal data protection.

Suspension or revocation

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

[3] 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.

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

**Suspension**

| APPLICANT / CAUSE | HOLDER (external person or employee) | INTERESTED THIRD PARTY (for external people) | BANK OF ITALY (for employees) |
|---|---|---|---|
| LOSS OF SMARTCARD | X | -- | -- |
| THEFT OF SMARTCARD | X | -- | -- |
| BREACH OF SECURITY | X | -- | -- |
| PROLONGED ABSENCE OF THE HOLDER | -- | -- | X |
| OTHER[5] | X | X | X |

**Revocation**

| APPLICANT / CAUSE | HOLDER (external person or employee) | INTERESTED THIRD PARTY (for external people) | BANK OF ITALY (for employees) |
|---|---|---|---|
| LOSS OF SMARTCARD (after suspension) | X | - | - |
| THEFT OF SMARTCARD (after suspension) | X | - | - |
| BREACH OF SECURITY[6] (after suspension) | X | - | - |
| DETERIORATION OF SMARTCARD | X | X | X |
| CHANGE OF HOLDER'S POSITION[7] | - | X | X |

The Bank of Italy assures a suspension service:

- for urgent requests, due to theft, loss or breach of security, by telephone with a Help Desk[8] (+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).

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

[6] 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).

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

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

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

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

For external users, the revocation request must be submitted to the competent RA by the holder or third party[9]; in this case the request must be signed by the entity's legal representative or other duly appointed person.

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

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

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

Revoked certificates must not be reactivated.

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

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

---

[9] 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.

Certificates may be suspended or revoked by the Bank of Italy in case of circumstances provided for article 36 of d.lgs. 82/2005[10].

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

Issue

Application for remote and system operated certificates are sent to the IT Development Directorate via an e-mail electronically signed by subscribers, normally Bank of Italy's employees, that have qualified certificates issued by the Bank of Italy (see section 1). After the application, certificate holders receive – in an encrypted mode - secret codes (PIN, activation code to initialize an OTP generator – One Time Password[11]) to activate his/her private key stored in a Hardware Security Module hosted by the CA in secure premises.

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

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

Revocation

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

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

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

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

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

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

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

## 3. Reliance limits

The Bank of Italy will retain records and information concerning qualified certificates, including all events connected to their life-cycle, for twenty years from the time of their issue, also in case of CA termination, inter alia in order to provide proof of the certification in judicial proceedings[12].

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

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

## 4. Obligations of subscribers

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

The certificate-holder is required to ensure the safekeeping of the signature device, 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 CPS/CPs, must also:

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

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

### 4.1. Obligations of the interested third party

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

## 5. Certificate status checking obligations of relying parties

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

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

Applicants for signature verification must verify:

1. the 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 - see section 2.1);
3. the existence of and compliance with any restrictions on the use of the certificate used by the certificate-holder.

## 6. Limited warranty and disclaimer/limitation of liability

The Bank of Italy will not be liable for:

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

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

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

- the exactness and completeness of the data needed to verify the signature contained in the certificate at the date of issue and on their completeness with respect to the requirements established for qualified certificates;
- the guarantee that at the time of issue of the certificate the signatory possessed signature-creation data corresponding to the signature verification data contained or identified in the certificate

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

### 6.1. Obligations of the Qualified Trust Service Provider

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

1. adopt every organizational and technical measure to avoid injury to third parties;

2. identify with certainty the person applying for certification;
3. verify the authenticity of the application;
4. issue, render public and manage the qualified certificate in the manner prescribed by the technical rules referred to DPCM 22.02.2013 as amended and in compliance with European and national legislation on personal data protection as amended;
5. specify in the qualified certificate, at the request of the applicant and with the consent of the interested third party, the powers of representation or other professional attributes or titles of the certificate-holder, subject to verification of the documentation submitted by the applicant attesting to the existence thereof;
6. give applicants complete and clear information on the certification procedure, the requisite technical features for accessing it, the characteristics of the signatures issued on the basis of the certification service and the restrictions on the use thereof;
7. not act as depositary of data for the creation of the holder's qualified signature;
8. promptly publish the revocation or suspension of a qualified certificate in case of a request by the holder or the interested third party, or where the signature device or authentication tools are no longer in the possession of the certificate-holder or their integrity hava 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[13];
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

[13] 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.

service providers) uses for signing the Public List of qualified trust service providers and publish it in its own Register of Certificates;

17. provide or indicate at least one system that permits signature verification and ensures its interoperability (in accordance with eIDAS and as referred to in Article 14 of the Decree of 22 February 2013 as amended)[14];
18. publish on the website a link to the public list, subscribed by the national supervision authority of trust service providers AgID, of trust service providers (Trusted List) qualified in accordance with the eIDAS Regulation, containing their certificates and CAs key;
19. 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 termination, well in advance, the national supervision authority of trust service providers (AgID) and holders of the termination and to assure a revocation status information service.

## 7. Applicable agreements, CPS, CP

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

- the CA certificate;
- the CA certificate fingerprint;
- the CPS/CPs;
- this document PKI Disclosure Statement;
- the instructions to use the signature software.

[14] The digital signature verification system, to be used with an active Internet connection, makes it possible to:

- verify the validity of the signatory's certificate and the issuer's qualification as qualified trust service provider;
- ascertain the integrity of the signed document;
- verify the validity of the signature in the same period validity of the corresponding certificate.

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

## 8. Privacy policy

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

The following information is considered public information:

- the CPS/CPs;
- the list of certificates suspended or revoked.

The Bank of Italy must adopt data safety measures for the treatment of personal data in compliance with the 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 if, in good faith, considers that:

- the disclosure is necessary in response to subpoenas and search warrants;
- the disclosure is necessary in response to judicial or administrative processes.

The following roles are responsible for processing the data in accordance with European and national legislation on 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.

## 9. Refund policy

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

## 10. Applicable law, complaints and dispute resolution

The Bank of Italy, as a Qualified Trust Service Provider, adheres to the Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and

related European standards, and the relevant provisions of the Legislative Decree no. 82/2005 and subsequent amendments. The Bank of Italy is compliant with the technical rules DPCM 22/02/2013.

The Bank of Italy adopts the security measures for the processing of personal data pursuant to European and national legislation.

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

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

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

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

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

## Glossary

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

[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.

| | |
|---|---|
| | system with an asymmetric matching pair of keys (public and private) which allows both the card holder (using the private key) and the recipient (using the public key) to prove the source and integrity of the electronic document/group of documents. |
| Electronic signature | Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. |
| Electronic signature creation device | Configured software or hardware used to create an electronic signature. |
| Electronic time stamp | Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. |
| Fingerprint of a sequence of binary symbols (bits) | The sequence of binary symbols (bits) of predefined length generated by the application of a suitable hash function to the sequence. |
| Hash function | A mathematical function that uses a generic sequence of binary symbols to convert data into a fingerprint from which it is impossible to trace the sequence of binary symbols that generated it. The probability of defining two sequences of binary symbols for which the hash function yields the same fingerprint is computationally infeasible. |
| Holder | The natural person (see signatory) that:<br>- is assigned the electronic signature;<br>- has access to the devices for the creation of the electronic signature;<br>- 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 which can be made public. If the public key is part of a signature pair or an authentication pair it can be used to verify the signature given by the matching private key. |
| PUK | PIN unlock key. |
| Qualified certificate for electronic signature | A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS regulation. |
| Qualified electronic signature | An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. |
| Qualified electronic signature creation device | An electronic signature creation device that meets the requirements laid down in Annex II of eIDAS and of DPCM 22.02.2013. |
| Qualified trust service | A trust service that meets the applicable requirements laid down in eIDAS. |
| Qualified trust service provider' | A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body. |
| Registration | Collection, authentication and storage of the personal data regarding the applicants for certificates. The registration is a necessary step before accepting the application for certification. |
| 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 registre all the certificates issued by the Trust Service Provider. |
| Remote signature | A particular type of qualified electronic signature or digital signature process generated on HSM which ensures exclusive control of private keys by the holder. |
| Signatory | A natural person who creates an electronic signature. |
| Subscriber | Legal or natural person bound by agreement with a trust service provider to any subscriber obligations. |
| Smartcard | Security device with an embedded circuit used for storing the key pair (private and public) and the certificate of the certificate-holder. |
| System operated signature on behalf of a natural person | Particular automatic system for qualified electronic signature or digital signature performed prior consent of the subscriber that maintains exclusive control of their signing keys, in the absence of timely and continuous supervision by this. |

| | |
|---|---|
| Third party | An institutional interlocutor (body or legal person) which request the issue of a certificate for another subjects, on whose behalf they operate pursuant to an employment or agency relationship. |
| Time reference | Specific time and date stamp connected to one or more documents. |
| Time validation | Result of the computer procedure with which one or more digital documents are time stamped as to be enforceable against third parties. |
| USB token | Security device with an embedded circuit used for storing the key pair (private and public) and the certificate of the certificate-holder. |
| Trust service | An electronic service normally provided for remuneration which consists of:<br>(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<br>(b) the creation, verification and validation of certificates for website authentication; or<br>(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<br>"Devolvement to the Government of the conferment of functions and assignments to regions and other local government bodies, for the reform of the public administration and administrative simplification" published in the S.O. 56/L of the *Gazzetta Ufficiale* n.63 of the 17 march 1997. |
| Law 229/2003 art. 10 | Law of 29 July 2003, n. 229<br>"Measures regarding regulatory, legislative and codification quality – simplification law 2001", published in the Gazzetta Ufficiale n.196 of 25 August 2003 |
| D.Lgs. 196/2003 | Personal Data Protection Code - Legislative Decree no.196 of 30 June 2003 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<br>"Codice dell'Amministrazione Digitale"<br>(Digital Administration Code - CAD) | Legislative decree 7 March 2005, n. 82<br>"Digital administration code" published in the S.O. N. 93/L of the Gazzetta Ufficiale n.112 of 16 May 2005[2]. |
| DETERMINAZIONE<br>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<br>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 |

[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.

| | |
|---|---|
| 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.”<br><br>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<br>on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.<br>Published in the EU Official Journal of 28 August 2014 L 257 |
| Regulation 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 |