User Manual Internet Access for the public key certification service

Version 1.0 / June 2010

WGT2/2010/061-rev

TABLE OF CONTENTS

1 GENERAL INFORMATION

1.1 Introduction

This Manual establishes the procedures followed by the Banca d'Italia as Accredited Certification Authority for the issue and utilization of electronic certificates in the context of the internet access to the TARGET2 system.
The service is provided by Banca d'Italia on behalf of the Eurosystem..
This manual is addressed to:

1. Central Banks participating or connected to TARGET2;
2. Credit Institutions and other entities that are entitled to participate in TARGET2 via the internet as described in the Information Guide (available on the ECB web site)[1];
3. Certificate-holders authorized by the participants.

2 IDENTIFICATION DATA

2.1 The Certification Authority

Name	Banca d'Italia
Registered office	Via Nazionale, 91 – 00184 ROMA
Legal representative	Governor
Website	www.bancaditalia.it

2.2 The User Manual

This document is version 1.0, dated 01 06 2010, of the User Manual for the public key certification service provided by Banca d'Italia. It is available for consultation at the TARGET2 ECB website for banks. (https://target2.ecb.int)

[1] http://www.ecb.europa.eu/pub/pdf/other/target2progressreport5-a1-informationguidetarget2usersen.pdf

3 OBLIGATIONS OF THE CERTIFICATION AUTHORITY, NATIONAL CENTRAL BANKS, PARTICIPANTS, CERTIFICATE-HOLDERS

3.1 Obligations of the Certification Authority

The Certification Authority shall:

1. adopt every organizational and technical measure to avoid injury to third parties;
2. provide complete and clear information on the certification procedure, the requisite technical features for accessing it and the restrictions on use thereof;
3. provide a secure and prompt service for the issuance, suspension and reactivation as well as for the revocation and renewal of electronic certificates and ensure the efficient, timely and secure functioning of the lists of issued, suspended and revoked signature certificates;
4. ensure the precise determination of the date and time of issue, revocation and suspension of electronic certificates;
5. not copy and not conserve the private signature keys of the certificate-holder;
6. prepare all the necessary information, in particular the exact terms and conditions governing the use of certificates, including restrictions on their use and make such information available to all the interested parties in the certification service;
7. use reliable systems for the management of the Register of Certificates, with procedures ensuring that only authorized persons can make additions and changes, that the authenticity of the data can be verified and that the authorized person will become aware of any event that jeopardizes security.
8. in the event of the cessation of its activity, notify holders at least sixty days in advance that all certificates not expired at the time of cessation will be revoked and effectively revoke them in due course;
9. adopt security measures for the treatment of personal data in line with the current Italian legislation (Personal Data Protection Code, legislative Decree n. 196, 30 June 2003).

The Certification Authority is responsible for fulfilling all the obligations established by law and referred to in this Manual.

The Certification Authority will not be liable for:

1. the consequences deriving from failure of the certificate-holder to comply with the operating procedures and methods specified in this Manual;
2. failure to fulfill its obligations for causes beyond its control.

3.2 Obligations of the Central Banks

The Central Bank shall:

1. make available all the relevant documentation provided by the Certification Authority to the participants and to the certified holders;
2. ensure the identity of the person applying for certification;
3. verify the authenticity of the application;
4. promptly transmit to the Certification Authority all the forms and other communications received from the participants following the procedures defined in this Manual.
5. promptly transmit to the participants all the forms and other communications received from the Certification Authority following the procedures defined in this Manual

3.3 Obligations of the TARGET2 Participants

The participants shall:

1. request the issuance of certificates, according to the procedures specified in this Manual,
2. request the suspension and reactivation as well as revocation and renewal of certificates, according to the procedures specified in this Manual, whenever the basis on which a certificate was issued to the holder changes or ceases to exist or in case of the cessation of its own activity (as a result of merger, liquidation, etc.).
3. adopt every precaution and organizational measure serving to ensure utilization of the certificates in conformity with the rules established in this Manual
4. notify the Certification Authority promptly, via the Central Bank providing the account, of every change of the information indicated in the forms at the time of issue of certificates that is relevant for the purposes of its utilization.
5. Ensure the certificate-holder is aware of and abides by their obligations as laid out below.

3.4 Obligations of the certificate-holder

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

The certificate-holder must also:

1. provide all the information requested by the Central Bank providing the account, guaranteeing its reliability under his or her own responsibility;
2. notify the Certification Authority, via the Central Bank providing the account, of any changes to the information provided at the time of registration: personal data, residence, telephone numbers, e-mail address, etc.;
3. conserve the device containing the certificate separately and with the utmost diligence, from the secret codes (PIN and PUK) in order to ensure their integrity and maximum confidentiality ;
4. not use the certificates for functions or purposes other than those for which the certificate was issued;
5. transmit information on and requests for suspension and reactivation as well as revocation and renewal of the certificate following the procedures defined in this Manual;
6. immediately request suspension of the certificates for the keys contained in devices that are defective or no longer in his or her possession;
7. notify the Central Bank providing the account of loss or theft of the security device.

4 USER IDENTIFICATION AND REGISTRATION PROCEDURE

This section describes the procedure for the initial issue of certificates, which includes identification of the applicant and registration.

4.1 Filling of the application form

Persons who apply for the issue of certificates must be identified and designated by the Credit Institution on whose behalf they operate pursuant to an employment or agency relationship; the Home National Central Bank guarantees the correctness of

the applicant identification within the rules agreed at the national level with the participants.

The participant attests that it understands the contents of this Manual and undertakes to comply with its obligations.

The designated person (certificate-holder) draws up and signs the certificate application, which shall:

1. indicate the applicant (certificate-holder's) identification data, including a unique identification number (e.g. tax identification number. identity card number, etc.),;
2. contain a declaration in which the applicant (certificate-holder) attests that the information provided is accurate and undertakes to notify every change therein;
3. contain a declaration attesting that the applicant (certificate-holder) has received the information note on the protection of personal data;
4. be accompanied by a copy of a valid identification document of the applicant (certificate-holder);
5. be countersigned by an authorised approver at the participant

The above-mentioned documentation shall be submitted to the Central Bank providing the account.

4.2 Registration of users

After performing the checks within its competence, the Central Bank providing the account will forward the application for certificates to the SSP Service Desk, which will insert all the necessary data for the issue of the certificates in the registration archive.

When an application form is not accepted, the SSP Service Desk will inform the Central Bank providing the account which in turn will notify the participant.

4.3 Delivery of security devices

The Central Bank providing the account, after receiving the envelopes containing, respectively, the smartcard and the secret codes (PIN, PUK)[2], shall send the envelopes containing the smartcard and secret codes to the requesting participants for further delivery to the applicants (certificate-holder); the NCB will make available to the same applicant (certificate-holder) an electronic version of this User Manual.

The participants will create a record for the delivery to be signed by the person responsible for the delivery to the certificate-holder at the participant and by the certificate-holder.

The participants will inform the Central Bank providing the account that the certificates has been delivered to the certificate-holder ; the Central Bank providing the account has to notify the delivery to the SSP Service Desk in order to trigger the activation of the certificate.

5 CERTIFICATE ISSUANCE PROCEDURE

A certificate associates the public key of a pair of asymmetric keys with a dataset that identifies a person (certificate-holder) who possesses the corresponding private key.

Such association is guaranteed by the signature affixed to the certificate by the Certification Authority with its private certification key.

5.1 Information contained in the certificates

The certificate contains:

1. serial number or other identification code of the certificate;

[2] The PIN must be entered in order to sign and perform other operations connected with the use of auxiliary certificates and must 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.

2. name of the Certification Authority and country in which it is established;
3. holder's identification code at the Certification Authority;
4. holder's given name, family name, unique identification number and date of birth;
5. certificate's term of validity;
6. Certification Authority's digital signature;
7. public key number;
8. utilizable generation and verification algorithms;
9. certificate signature algorithm;
10. type of the pair of keys according to their assigned use.

Identification of the holder will be implemented by means of the Distinguished Name (DN) as provided for in ISO 9594-1 (1997).

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.

The Certification Authority will retain the information concerning the certificate for no less than twenty years from the certificate's expiration or revocation date.

5.2 Periods of validity of the keys and related certificates

The signature certificates issued to holders are valid for up to 3 years.

6 CERTIFICATE SUSPENSION AND REVOCATION PROCEDURES

The Certification Authority suspends or revokes certificates by entering their serial number in the lists of suspended or revoked certificates.[3]

The suspension or revocation of a certificate takes effect from the time of the certificate's entry in the aforesaid lists.

When a certificate is suspended, its validity is interrupted temporarily.

When a certificate is revoked, its validity is terminated in advance.

[3] The two lists are currently presented for consultation as a single list including both suspended and revoked certificates distinguished by different "causes".

6.1 Suspension or revocation of certificates

The certificate-holder or the participant may request that a certificate's validity be suspended or the certificate be revoked for the reasons listed in paragraph 6.2.

When the Certification Authority becomes aware of suspected abuse, falsification or negligence, it may suspend certificates after notifying the certificate-holders via the SSP Service Desk and Central Bank. In emergencies the certificate may be suspended before the Certificate-Holder is notified.

In the event of

- loss,
- theft or
- breach of security of the smartcard,

the holder or the participating bank must contact the Service Desk of the Central Bank providing the account for urgent suspension or revocation of the authorization to access TARGET2 in the Identity and Access Management component (IAM). National Service Desks are normally available from 6:30 to 18:45 on all TARGET2 business days; possible national different opening hours must be checked with the Central Bank providing the account. The Central Bank providing the account shall inform without delay the SSP Service Desk, which in turn will immediately suspend or revoke the relevant user within the IAM.

Afterwards the participant will send the form requesting the suspension or revocation of the certificate to the Central Bank providing the account according to the procedures agreed at local level.

The NCB receiving the form requesting the suspension or revocation of the certificate will - after having verified its authenticity - initiate the procedure by forwarding it to the SSP Service Desk; the latter will record the request in the certified PKI system and notify the NCB about date and time when the revocation or suspension actually takes place.

The Central Bank providing the account will notify the holder and the participant of the suspension or of the revocation of the certificate, specifying the date and time from which the certificate is no longer valid.

6.2 Causes for suspending or revoking certificates

The holder or the participant may request the Central Bank providing the account to suspend or revoke a certificate for the causes listed in the following table. Should the Certification Authority become aware of suspected abuse, falsification or negligence, it may revoke certificates after notifying, via the Central Bank, the certificate-holders

PERSON SUBMITTING THE REQUEST CAUSE	HOLDER (external person or employee)	Participating bank
LOSS OF SMARTCARD	X	X
THEFT OF SMARTCARD	X	X
BREACH OF SECURITY	X	X
DETERIORATION OF SMARTCARD	X	X
CHANGE OF HOLDER'S POSITION[4]	--	X
OTHER[5]	X	X

For requests where the cause is indicated as "other", suitable reasons must be given.

Except in cases of loss or theft, the holder is required to return the smartcard in his/her possession to the participant after rendering it unfit for use by cutting the microcircuit.

6.3 Reactivation of suspended certificates

Should a suspension be requested and the smartcard later recovered, the reactivation of the suspended certificate can be requested; if on the contrary the loss is confirmed, the holder must submit a request for revocation.

The reactivation request must be submitted following the same procedure described above for suspension requests.

The Certification Authority will reactivate the certificate by cancelling it from the Certificate Suspension List.

The Certification Authority will notify, via the Central Bank providing the account, the card's holder and the participant of the reactivation of the certificate, specifying the date and time from which the certificate is newly active.

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

[5] 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..

6.4 Revocation of the certificates for the keys of the Certification Authority

In the following exceptional circumstances the Certification Authority will revoke the certificate for the pair of certification keys stored in internal Databases:

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

The revocation is implemented by inclusion of the certificate in the Certificate Revocation List.

Where the revocation is due to breach of security of the Certification Authority's private key, the Certification Authority, acting on its own authority, will revoke all the certificates signed with that key.

7 PROCEDURE FOR RENEWAL OF CERFICATES

The electronic keys are valid for three years.

When the expiration of certificates approaches, the SSP Service Desk will send a notification to the relevant Central Bank with the list of individuals for each participant whose certificates are about to expire two months in advance. The Central Bank will communicate such information to the participant concerned following local procedures to be defined by each NCB.

Before the expiry date the certificate-holders will be able to renew the certificates through a web page on internet made available by the Certification Authority to generate a new pair of keys. In such a case no other action is necessary. It is therefore strongly recommended to execute the renewal through this procedure before the certificates' expiry date is reached. This will ensure there are no continuity breaks in the certificate validity and capability to operate.

Should the request be submitted only after the expiry date is reached, the participant shall request the NCB to issue a set of certificates identical to the expired ones, by means of the specific form, following local procedures to be defined by each NCB.

The NCB will forward the form to the SSP Service Desk which afterwards will send the NCB the envelopes containing the access codes for the web application through which the new digital certificates will be delivered. For the delivery and receipt of such codes, the rules described under 4.3 concerning the sending and delivery of the security devices to the individuals apply.

8 CARD READER TECHNICAL SPECIFICATIONS

In order to use the smartcard a card reader has to be purchased by the final user.
Recommended card reader:
Desktop PC: "Gemalto PC USB-SL"

Laptop Gemalto “PC Twin” or “PC USB TR”

It is possible to use a different card reader with the following specs:

1. USB interface with type A connector
2. USB power supply
3. Support for smart card ISO 7816 Class A, B e C (5V, 3V e 1,8V)
4. Short circuit protection
5. ISO 7816-2, Dimensions and location of the contacts
6. Electronic signals and transmission protocols ISO 7816/3
7. support for protocol T=0 and T=1
8. driver PC/SC driver for Microsoft
9. compliance with the specifications Microsoft Windows Hardware Quality Labs (WHQL)
10. compatibility with the following operating systems:
    - Windows XP/Vista/7