Certification services for electronic security certificates

(Certification Practice Statement)

Table of Contents

1 Introduction

1.1 Context

This document constitutes Postecom's CPS (*Certification Practice Statement*) for the issue and management of Electronic Security Certificates.

Public Key Infrastructure (PKI) technology enables the implementation of services aimed at meeting the technical requirements of Organisations using electronic certificates as a tool for the protection of digital data transactions. Public certification services support various security mechanisms for the protection of communications and computer assets. Certificates alone, however, do not constitute a mechanism: they are simply an interface tool for such services.

On the basis of standard *Office Automation* applications, of the technical requirements expressed by the Organisation requiring the service, and the CA's internal processes, it will be possible to select the type of Electronic Security Certificates allowing use of the aforementioned security systems.

In this context, Postecom acts as a Certification Authority (CA) for the issue and management of electronic certificates, in compliance with published procedures.

The certificates issued in compliance with this CPS are granted only for Organisations or Communities, in any case after signing a specific agreement. The electronic certificates issued in compliance with this CPS can be both personal (i.e. certificates issued to physical persons in order to, for example, authenticate or sign/cipher e-mails) or functional (for instance, certificates issued for services or functions internal to the same Organisation, in any case connected with security fields).

1.2 Document identification

This document is Postecom's CPS for the issue of electronic certificates for security services and is called:

- *Certification services for electronic security certificates*

The CPS is identified as Version 1.0. The corresponding electronic file is identified as "*CPS_PKIASV01*".

1.3 OID Table

This CPS refers to the following OIDs (Object Identifier Numbers):

CA Certificates			
OID	**CA**	**Personal Certificates**	**Functional Certificates**
1.3.76.11.1.1.6.1	Postecom CS1	✓	✓
1.3.76.11.1.2.1.1	Postecom CA1	✓	
2.5.29.32.0	Postecom CA2	✓	

Electronic Certificates		
OID	**Support Type**	**Certificate Type**
1.3.76.11.1.1.10.1	Hardware	Personal
1.3.76.11.1.1.10.2	Software	Personal
1.3.76.11.1.1.10.10	Software	Functional

"Postecom CA1" and "Postecom CA2" are the CAs accredited for issuing qualified certificates and at the same time is also used to issue personal electronic certificates on the same secure signature device. These electronic certificates are called "auxiliary" and differ from qualified certificates as they have a specific OID (not included in this CPS) and a different valorisation of the **KeyUsage** field: in any case, **NEITHER** electronic certificates, issued in compliance with this CPS, **NOR** auxiliary electronic certificates, will include a **nonRepudiation** attribute (which is reserved only for qualified certificates).

The procedures applied for the issue and life cycle management of auxiliary electronic certificates are the same as those envisaged for qualified certificates. For details of these procedures refer to the specific Operating Manual in force, deposited at the CNIPA and published online at www.poste.it, Postecert Section.

1.4 Definitions

Certificate: digital document in X.509 format, containing information about the Owner, the Owner's public key, signed by the Certification authority with its own private key

Certificate register: register containing certificates issued by the CA and the list of revoked certificates, with telematic access

Certificate revocation: operation whereby the CA revokes validity of the Certificate from a given moment onwards

Certificate revocation list (CRL): a digitally-signed list, containing revoked certificates, stored and updated by the CA

Certification: the result of the IT procedure ensuring one-to-one correspondence between the public key and its Owner, certifying the validity period of the aforementioned key and the expiry date of the relative certificate

Certification Authority (CA): the authority responsible for generating, issuing, publishing, storing and revoking certificates

CPS: a document defining procedures applied by the Certification Authority to perform its activities

Common Name: common name of the certificate Holder. In case of functional certificates, the Holder is the Organisation reported in the certificate

File: software support containing the certificate's private key.

Holder: a person or a entity (service or function) that has been issued with a Certificate pursuant to this CPS. In case of functional certificates, the Holder is the Organisation reported in the certificate

Owner: see Holder.

Key Pair: encrypted asymmetrical pair of correlated keys, one private and one public

Private key: one element of the asymmetrical key pair, which must be known only to the Owner

Public key: element of the asymmetrical key pair which will be made public

Organisation: an organized community of users (for instance companies, businesses, professional and trade associations etc.) who stipulate agreements with the CA for the issue of personal electronic certificates to employees and/or members

Organisation Referent: the person selected by the Organisation to manage relations with the CA, to request the registration of members of the Organisation, as well as forwarding certificate revocation requests

Relaying party: subject receiving an electronic certificate who is not the Owner

Smart card (encrypted): electronic device only programmable at origin, fitted with an encrypted co-processor able to perform private key and public key certificate encryption and storage operations

Subscribers: the subject who requests certification services pursuant to this CPS

User: see relaying party

1.5 Acronyms

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman

2 Subjects involved

2.1 Organisation

The certification service is provided by Postecom S.p.A. for members of Organisations or, in any case, subjects identified by the latter, for digital keys pertaining to secure systems access or information notification, in the context of defined processes.

The Organisation undertakes to appoint, through the conclusion and signature of a special Agreement, the “Organisation Referent” who is delegated to handle the contacts with Postecom.

Whenever contractually agreed, the Organisation may indicate also the “Local Registration Authority Officers” (or LRAOs).

2.2 Organisation Referent

Represents the Organisation to the CA. In order to ensure process efficiency, more than one Organisation Referent may be appointed. The Organisation Referent(s) has (have) the task of providing all the information requested by the CA, assuming responsibility for it as far as authenticity, accuracy and completeness are concerned.

Organisation Referents will be issued with an electronic certificate (usually on a smart card) for communicating with the CA (for instance, when asking for certificate issuing or revocation requests).

2.3 LRA Officer

Whenever contractually agreed, other than the Organisation Referent, the Organisation may indicate also the LRA Officer(s). The LRA Officers, preventively authorized by the Organisation Referent, are qualified to ask, for the certificate Subscribers/Holders of the specific Organisation, the certificate generation/revocation/suspension/unsuspension requests.

The LRAOs will issued with an electronic certificate (usually on a smart card) and, whenever the CA’s procedures will allow, they will be able to use web-based systems for carrying out their activities.

2.4 Holder (or Owner)

Certificate Holders are individuals for whom an electronic certificate has been generated, following a request made by the Organisation Referent(s) -or, whenever foreseen, by the LRAOs-. In case of functional certificates, the Holder is the Organisation reported in the certificate.

Owners may have hardware support (for instance a smart card) or software support (file). The smart card is a device that stores the private key and provides best assurance for certificate security. The information concerning the kind of signature device used is included in the certificate, in the field that contains the relative identifier (OID), as shown in the above OID Table.

2.5 Relying parties

Subjects who are not Owners of any certificates but who receive a certificate and rely on that certificate or on the digital signature it provides.

2.6 Obligations

2.6.1 CA obligations

Postecom undertakes to:

- Protect in security the private key used for issuing the electronic certificates conforming to the present CPS;
- issue the electronic certificate and to make it public if this is requested or required by specific contractual agreements;
- comply with safety measures for data handling, pursuant to Italian Government Decree 196/2003 (that is the Italian law equivalent to the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data);
- use registration data only for managing the certificate life cycle;
- provide timely notification of certificate revocation by publishing the information in the Certificate Revocation List (CRL).

2.6.2 Organisation obligations

The Organisation is obliged to:

- provide true information and documentation during registration;
- appoint from amongst its employees an Organisation Referent(s) to work with Postecom;
- notify the CA immediately of any change in the Organisation Referent(s), requesting revocation of his/her(their) certificate, and of any other variation in the data set out in this CPS and relevant agreements;
- undertake to inform the certificate Owners of the conditions set out in this CPS;
- comply with safety measures for data handling, pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- use registration data only for managing the certificate life cycle;
- adopt suitable Organisational and technical measures for avoiding damage to others.

2.6.3 Organisation Referent obligations

The Organisation Referent, whenever foreseen, must:

- indicate the LRAOs, asking for their electronic certificates issuing;

- adequately inform each new LRAO of their tasks and duties;
- communicate immediately when some LRAOs have to be removed by this activity for any reasons.

Besides, the Organisation Referent and the LRAOs must:

- send certificate registration data compliant with the instructions provided by this CPS and the instruction supplied to the Organisation;
- comply with safety measures for data handling, pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- use registration data only for managing the certificate life cycle;
- ensure, when required, the storage of certificates and secret access credentials in their possession and regulate their delivery to the physical persons for whom they are intended;
- request certificate revocation when the requisites for which the certificate has been issued to the Holder are lacking, in compliance with the instructions provided by this CPS;
- undertake to request certificate revocation when so requested by the Holder, in compliance with the instructions provided by this CPS;
- request certificate revocation in the event of misuse, falsification or use not in conformity with the scope for which the certificate was issued, and for any reason the Organisation Referent/LRAOs deem valid.
- adopt suitable Organisational and technical measures for avoiding damage to others.

2.6.4 Owner obligations

Certificate owners must:

- store their private key safely, adopting all the necessary precautions to avoid damage, tampering or unauthorised key use;
- store the information for enabling use of the private key with utmost diligence, to ensure its integrity and complete confidentiality;
- inform the Organisation Referent (or if foreseen the LRAO) promptly if the information on the issued certificate is no longer valid, requesting revocation of the certificate in compliance with the methods indicated by the CPS;
- inform the Organisation Referent (or if foreseen the LRAO) promptly if there is any doubt that the security of the device on which the private key is installed has been compromised, requesting immediate revocation of the certificate in compliance with the methods indicated by the CPS;
- adopt suitable Organisational and technical measures for avoiding damage to others.

2.6.5 Relying parties obligations

The User who uses a certificate but is not its owner, must:

- be aware of the certificate's scope of use and liability limitations as indicated in the CPS;

- verify the validity of the certificate before using the public key it contains. The certificate's validity is ascertained by verifying that the issuing CA is the one indicated in this CPS, that the OID indicated in the Certificate Policy is referred to in this CPS and corresponds to the desired type of private key support, that the certificate has not expired, been revoked or suspended;
- use data kept in the certificates register (for example, the revocations list) only for verifying certificate validity;
- adopt suitable Organisational and technical measures for avoiding damage to others. The User is the only person liable for use of the issued certificate not in conformity with the indications in this CPS.

2.7 CA Limited liability

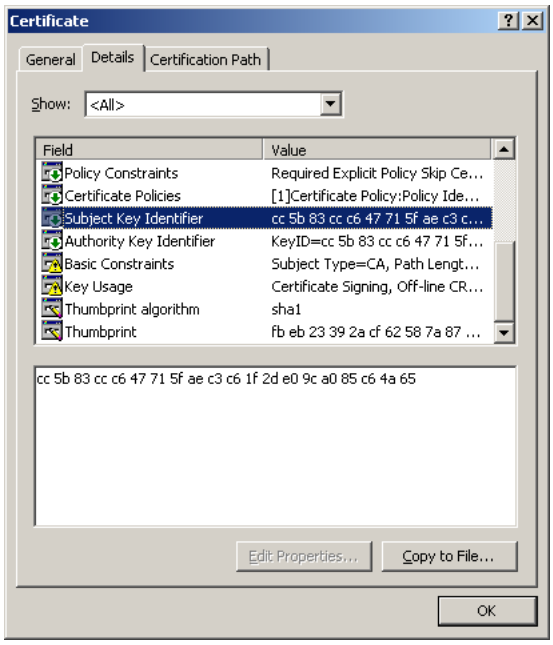
In no case will Postecom be held liable for events not attributable to it, especially damages of any nature (for instance deriving from failure to issue a certificate or for certificate misuse) suffered by the Organisation, the Organisation Referent, the LRAOs, the Owner, Users or any third party, caused directly or indirectly by these subjects' failure to respect the rules included in this CPS, or their failure to apply measures of special diligence for avoiding damages to third parties, as required from a user of certification services, or deriving from illegal activities. The CA is not liable for any default or, in any case, any damaging event caused by fortuitous circumstances or by force majeure.

2.8 Publication and directory

2.8.1 CA information

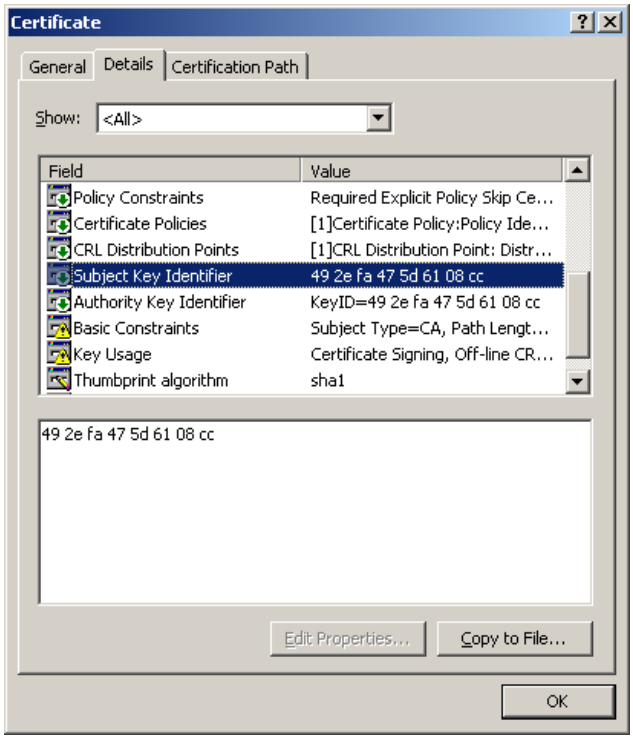
Below there is a table of salient CA certificate data, required for issue of the electronic certificates described in this CPS.

POSTECOM CS1



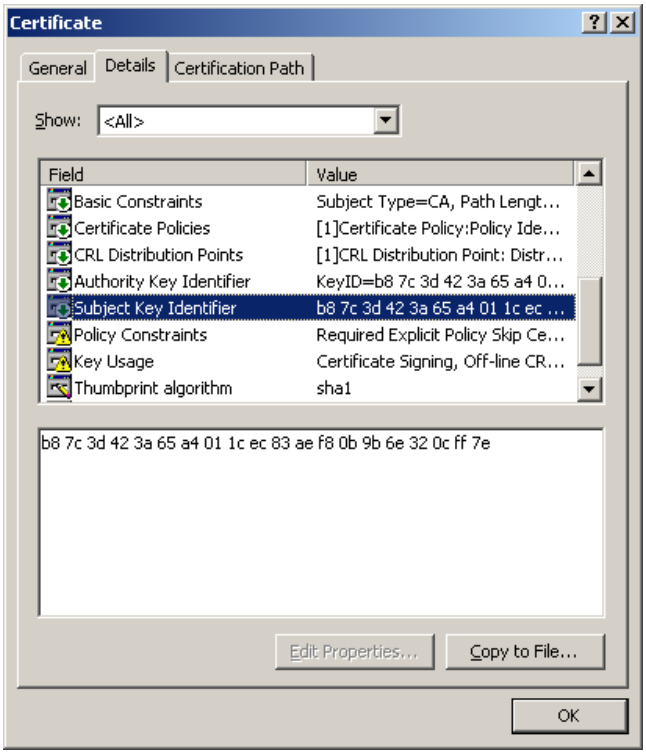
Datum	Value
Subject	**C** = IT, **O** = Postecom s.p.a., **OU** = CA e Sicurezza, **CN** = Postecom CS1
Issuer	**C** = IT, **O** = Postecom s.p.a., **OU** = CA e Sicurezza, **CN** = Postecom CS1
Period of validity	From 03/10/2002 to 30/09/2012
Key length	2048 bit

POSTECOM CA1



Datum	Value
Subject	**C** = IT, **O** = Postecom s.p.a., **OU** = CA e Sicurezza, **CN** = Postecom CA1
Issuer	**C** = IT, **O** = Postecom s.p.a., **OU** = CA e Sicurezza, **CN** = Postecom CA1
Period of validity	From 03/10/2000 to 01/10/2010
Key length	2048 bit

POSTECOM CA2



Datum	**Value**
Subject	**C** = IT, **O** = Postecom s.p.a., **OU** = Certification Authority, **CN** = Postecom CA2
Issuer	**C** = IT, **O** = Postecom s.p.a., **OU** = Certification Authority, **CN** = Postecom CA2
Period of validity	From 10/05/2006 to 10/05/2016
Key length	2048 bit

2.8.2 Certificates and CRL

X.509v3 certificates, if foreseen, are published in a X.500 directory server at:

- Postecom CS1: ldap://digicert.postecert.it
- Postecom CA1: ldap://certificati.postecert.it
- Postecom CA2: ldap://certificati.postecert.it

The directory can be accessed via LDAP protocol v2 and v3.

CRLs are published in the same directory server. The directory can be accessed via LDAP protocol v2 and v3:

- Postecom CS1

  ldap://digicert.postecert.it:389/CN%3dPostecom%20CS1,OU%3dCA%20e%20Sicurezza,O%3d Postecom%20s.p.a.,C%3dIT?CertificateRevocationList;binary

- Postecom CA1

  ldap://certificati.postecert.it:389/CN%3DPostecom%20CA1,OU%3DCA%20e%20Sicurezza,O%3DPostecom%20S.p.A.,C%3DIT?CertificateRevocationList;binary

- Postecom CA2

  ldap://certificati.postecert.it:389/CN%3DPostecom%20CA2,OU%3DCertification%20Authority,O%3DPostecom%20S.p.A.,C%3DIT?CertificateRevocationList;binary

The CRLs are updated when a certificate is revoked and, in any case, at least once a day.

2.9 Confidentiality

Data stored in the database are protected by authorization policies based on user authentication. The mechanisms applied for implementation of the following activities are compliant with minimum security measures for personal data handling, pursuant to Italian Government Decree 196/2003; in particular they allow:

- identification of persons in charge and delegates;
- allocation of identification codes;
- computer protection;
- an appropriate method for appointing data handlers Responsible.

2.10 Applicable law and place of jurisdiction

These General Conditions are subject to Italian law. The only place of jurisdiction for disputes that may arise between the parties in relation to the provisions of this CPS, is the Court of Rome, Italy.

3 Service provision process

The provision of electronic security certificates is offered to Organisations and envisages the prior stipulation of an Agreement, with appointment of an Organisation Referent person who will manage relations between the Organisation and Postecom. This Organisation Referent will be identified and issued centrally with a special electronic certificate (usually on a smart card).

Owners may be issued with electronic certificates in one of two ways:

- centralized
- remote

If required, the issued certificate may be published in the special public register that can be accessed with LDAP protocol.

The delivery of the electronic certificate to the Holder together with, if required, the signature device/secret credential for private key access, is undertaken by the Organisation Referent or by delegated Organisation staff. Postecom does not perform face-to-face identification of the Owner for this type of electronic certificates. The Organisation Referent is authorised to verify Owner data and will do so in the way deemed most appropriate under its responsibility.

Whenever CA procedures allow it and depending on specific policies, the key recovery of he electronic certificate's private key will be possible.

Nevertheless, detailed instructions on the issue of certificates will be provided by Postecom or agreed with the Organisation as part of the specific procedures/Lightweight Certificate Policy, depending on contractual agreements between the Parties.

3.1 Centralized procedure

The centralized procedure includes the forwarding to the CA of a file record with the registration data required for issuing electronic certificates. Postecom must receive registration data sent by the Organisation Referent using the latter's own electronic certificate, in the manner defined by the CA, before proceeding to issue electronic certificates; Postecom will exclusively allow a formal verification of data format compliance, since the Organisation is liable for Owner data conformity. The certificate is issued by Postecom's Centralized Production Structure.

If a smart card (digital secure device) is used as a private key storage device, all the digital secure devices will be sent to the Organisation Referent. The smart cards, with onboard certificate, are given to Owners by the Organisation. The consignment of blind envelopes (that contain the Personal Identification Number -PIN- to access the private key inside the smart card) can be addressed to a different subject, nominated by the Organisation.

3.2 Remote procedure

As an alternative to the centralized certificate procedure, it is also possible to use a remote procedure to generate the certification request.

The remote system must be agreed in advance, on the basis of the Organisation's needs and the CA's internal processes. To be able to request the activation of this type of certificate issue method, a special Agreement must be signed to regulate the Organisation's liability.

Postecom, in any case, reserves the right to assess the Organisation's request with a prior verification of underlying organisational and technological requisites.

Via special systems provided by Postecom, the Organisation or the Subscriber will activate the key pair generation phase. Depending on the Organisation's needs and the CA's technological and Organisational systems, subscriber data may be forwarded in advance to Postecom via a file record, with the Organisation Referent's digital signature (and uploaded by Postecom to its registrations database), or entered by "operators" delegated to perform the remote procedure.

After the key pair has been generated, and authorised operators have sent the certification request, the system will undertake suitability checks and issue the certificate, which is sent to the location of the client workstation who requested it.

3.3 Certificate format and content

The certificate is generated with the information provided by the Organisation Referent or by the delegated subjects. The certificate format is compliant with the X.509 v3 standard.

The certificate profile will be agreed with the Organisation on the basis of the Organisation's requests and Postecom's technological processes. Electronic certificates issued in conformity with this CPS will bear one of the OIDs shown in the OID Table contained in this document.

In any case, the electronic certificates issued by Postecom, **WILL NOT** include a **KeyUsage** with the *nonRepudiation* attribute.

4 Certificate life cycle management

4.1 Certificate revocation

Revocation of a certificate means advance termination of its validity and this will be effective from the time the list containing the serial number is published.

The certificate can be revoked by the:

- Owner
- Organisation Referent
- LRAOs, if contractually foreseen
- CA

The revoked Certificate will be included in the CRL.

Reasons for revocation include:

- if there is an intention to terminate the agreement with Postecom;
- information on the issued certificate is no longer valid;
- it is felt that the security of the device supporting the private key has been compromised.

In the latter case, this should be notified immediately; in any case Postecom will assume no liability for misuse of the private key associated with the certified public key.

The CA may revoke issued certificates at will. If the CA revokes certificates, Postecom may proceed to notify the revocation to the Owner or Organisation Referent.

4.1.1 Owner request for revocation

Owners may forward their requests to the CA via the Organisation Referent, who will undertake to implement it as per the methods he/she has available. Whenever contractually foreseen, Holders could forward their revocation requests also to the LRAOs.

In the event that CA procedures allow it, Owners may access the online certificate revocation service directly, using the web interface made available by Postecom.

4.1.2 Organisation Referent request for revocation

The Organisation Referent is responsible for requesting certificate revocation when the requisites for which the electronic certificate has been issued to the Owner are lacking. The Organisation Referent must request electronic certificate revocation in the event of misuse, falsification or use not in conformity with the scope for which the certificate was issued, and for any reason the Organisation Referent deems valid.

The Organisation Referent may access the online revocation service via his/her own certificate, specifying which electronic certificate it wishes to revoke.

If the Organisation Referent is not authorised to effect an online request, he/she can use special forms (provided by the CA) digitally signed with his/her own electronic certificate.

The Organisation Referent must forward the request to Postecom at least two working days prior to the start date indicated on it.

Whenever contractually foreseen, also LRAOs will be able to ask electronic certificate revocation following the procedures and using the tools supplied by Postecom

Once the CA has received the request and verified its authenticity, it will proceed to revoke the certificate and to include it in the special Certificate Revocation List (CRL), as well as publishing notification in its Certificate Register.

There follows a summary table of the methods for notifying Postecom of a revocation request.

Subject requesting certificate revocation	**How to forward the request**
Owner	Request forwarded to Organisation Referent. When enabled, online method
Organisation Referent (and LRAO, if foreseen)	Online method or (if not enabled) a request digitally-signed with their own certificate

Other methods for accessing the revocation request service may be agreed in advance with the Organisation (and indicated in specific agreements).

4.2 Revocation by CA

The CA has the right to revoke the issued certificates. In these cases, Postecom may proceed to notify the Owner or the Organisation Referent that the certificate has been revoked.

4.3 Service levels

Service	Time
Access to public archive of certificates/CRL (1)	24/24 7/7
Online certificate revocation (if foreseen) (1)	24/24 7/7
Other activities, registration, generation, publication, revocation by digitally-signed forms, renewal (2)	Mon-Fri from 9am to 6pm excluding Italian holidays

(1) The service may not be available in the above times if there are maintenance or force majeure downtimes.

(2) The above times refer only to activities managed directly by the CA. Any registration offices located at the Organisation may have different hours.

5 Security aspects

5.1 Physical protection of premises

The technological systems involved are located in a protected area, with access reserved only for Postecom staff and protected by fingerprint recognition devices, smart card readers, CCTV. The area is located inside the Poste Italiane premises, in Rome, Italy, Viale Europa 175, monitored 24 hours a day, 7 days a week, and includes a permanent Post and Communications Police unit.

5.2 Certification system security

The management platform for certification activities, comprising various modules in the CyberTrust UniCERT software suite, offers the following security functions:

Identification and authentication

- Access to platform applications modules requires user identification. The authentication mechanism is required for starting and/or stopping the service linked to the applications module.

Access control

- Access to platform applications modules requires strong authentication mechanisms. Access to modules is allowed only after correct entry of the passphrase, and user-id and password relative to the database with which the application is interacting.

Traceability

- All applications running the CA's certification system store traces of performed operations on special databases.
- Text format logs are generated and structured in special databases where the start, stop or alarms information is stored for the applications modules services, as well as any information containing traces of configuration modifications made to the services. Log registrations structured in special databases are digitally signed.

Integrity and non-repudiation

- Digital signature for messages. All messages sent by each module in the core suite have digital signatures.
- Verification of messages: All core suite modules verify all messages received, to ensure integrity and authenticity.
- Data storage: all data and audit logs are registered in the database relative to each module. All entries have the digital signature of the DB owner modules belonging to the PKI technology platform. All entries have a unique identification number.

Communications

- Module communications use PKIX protocol.

5.3 Encryption module security

Postecom uses the RSA (Rivest-Shamir-Adleman) algorithm to generate digital signatures.

All certificates issued by Postecom – from CA certificates to Subscriber certificates – are signed using the RSA algorithm. The same RSA algorithm must be used by the subscriber to generate the personal key pair. Owner public keys have a total length of at least 1024 bit; certification keys are 2048 bit.

To date there have been no crypto-analysis systems able to crack keys of that length. Since the probability of cracking 1024 or 2048 bit keys may increase in the future, Postecom reserves the right to adapt key lengths with future technologies.

As far as hash functions are concerned, the function used is that corresponding to function SHA-1.

5.4 Network security

Network infrastructure envisages a first line comprising a firewall system with high reliability configuration, which filters internet traffic towards the DMZ network, where internet-accessible servers reside (like the Directory Server which publishes the CRLs), and a second line which filters traffic between the DMZ network and the Secure LAN, where the certification systems are installed.

The use of this technology allows use of the NAT Network Address Translation to "mask" internal IP addresses going out to the internet, enables interception of attempts to create service interruptions with SYN flood DoS-type attacks, defines anti-spoofing rules, limits access in a time span with granular definition. In order to achieve real-time analysis of packets travelling on the web and to activate suitable protection (IP address block, connection interruption, trap sending) and alarms, where suspect activity is pinpointed, an Intrusion Detection system has been installed, based on a database with continuous vulnerability updates.

There is 24x7x365 coverage, with offices staffed Mon-Fri 8.00am-8pm, and an out-of-hours/holiday callout structure for DMZ services and services used for certification systems. Alarms are notified by SMS and telephone calls from a centralized monitoring system.