Certificate Policy and Certification Practice Statement

Public Key Infrastructure for the Italian Electronic Identity Card “CIE”

OID: 1.3.76.47.2

TABLE OF CONTENTS

1. INTRODUCTION

This document is structured according to RFC 3647 “Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework” [RFC3647].

1.1 Overview

This document describes the Certificate Policy of the Certification Authority that issues X509 digital certificates stored inside the Italian Electronic Identity Card (CIE). These certificates with their private keys are used to access online services using the strong authentication. The document describes the features of the CA as well as binding requirements that have to be fulfilled by service providers and other PKI participants. Moreover (together with the CPSs) it also defines the certification process as well as the cooperation, duties and rights of the PKI participants.

All the sensitive information concerning national security matter are not included in this document.

1.1.1 PKI hierarchy

The architecture of the PKI that has in charge the issuing of the certificates for the Italian Electronic Identity Card CIE 3.0, is shown in Figure 1.

The *National Root CA for the Italian Electronic Identity Card* (the Root CA) issues the CA certificate associated to the *Issuing sub CA for the Italian Electronic Identity Card (*issuing SUBCA*)*. This last one issues the digital certificates that are stored on the chip of the “CIE” ID cards.

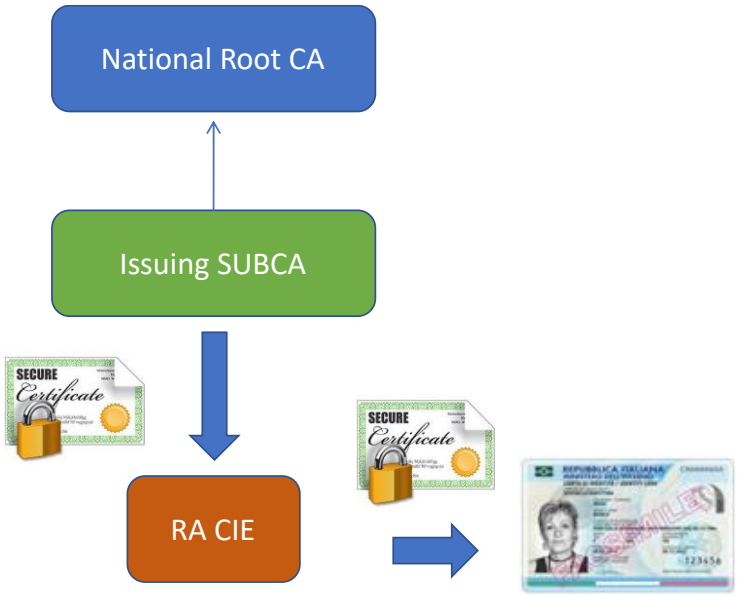

Figure 1 - PKI hierarchy

1.1.2 National Root CA for the Italian Electronic Identity Card (Root CA)

The Root CA issues the X509v3 certificate used by issuing SUBCA and takes care of the management of its lifecycle. The actions performed by this CA are:

- Generating Root CA Key Pairs on an external Hardware Security Module
- Generating its self-signed Certificates
- Generating the digital certificate for the issuing sub CA.
- Revoking CA certificates

The National Root CA is not reachable via network, authorized personnel have to operate using a console that is available inside the trust center where the system is.

1.1.3 Sub CA for the Italian Electronic Identity Card (issuing SUBCA)

The Sub CA for the Italian Electronic Identity Card together with other PKI Participants (such as Registration Authorities) issues, manages or revokes X.509v3 Public Key Certificates.

The services offered include:

- Receiving CSR requests from the registration authority software platform
- Generating Certificates for the end entities
- Revoking End-Entity Certificates (the certificates issued to the holders of the ID Card)
- Maintaining a Revocation List for End-Entity Certificates (“EE-CRL”)
- Publishing the revocation list (https://ldap.cie.interno.gov.it/ciesubca<N>.crl there <N> is the number of renewals of the C, starting from 1.

1.2 Document Name and Identification

This CP is referred to as the ‘Certificate Policy’.

Title: Certificate Policy and Certification Practice Statement - Public Key Infrastructure for the Italian Electronic Identity Card “CIE”

OID: 1.3.76.47.2

Expiration: This version of the document is the most current one until a subsequent release.

1.3 PKI Participants

1.3.1 Certification Authorities

1.3.1.1. Root CA

See chapter 1.1.2 .

1.3.1.2. Issuing SUBCA

See chapter 1.1.3 .

1.3.2 Registration Authorities

The Registration Authority software platform, also called “RA CIE” is responsible for:

- receiving the enrollment requests from the Municipalities issuing the ID cards,
- generating an RSA keypair for each enrollment request
- generating a signed CSR containing the public key
- sending the CSR to the issuing sub CA
- receiving the certificate and preparing the PKCS#12 structure to be used for the issuance of the card

1.3.3 Subscribers

The subscribers are the citizens who request the electronic identity cards to the Municipalities. Each card contains a digital certificate issued by the issuing sub CA.

1.3.4 Relying Parties

Relying parties are service providers that use the certificate issued by the Italian Electronic Identity Card – SUBCA1 to authenticate subscribers named in point 1.3.3 giving them access to their services.

CRL and/or the OCSP responder can be used to check the validity of the certificate.

The CRL is published at:

URL=https://ldap.cie.interno.gov.it/ciesubca<N>.crl

where <N> stands for the number of renewals of the sub CA, starting from 1.

The OCSP responder is available at the address

URL=https://ocsp.cie.interno.gov.it

1.3.5 Other Partecipants

Not applicable

1.4 Certificate usage

1.4.1 Appropriate Certificate Uses

The certificates issued by the issuing sub CA are used only to perform a strong authentication to online services offered by Service Providers.

1.4.2 Prohibited Certificate Uses

Private use of certificates is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This document is published by *Ministry of Interior (www.interno.gov.it), "Direzione Centrale per i servizi Demografici"*:

Ministero dell'Interno

Direzione Centrale per i Servizi Demografici CNSD

P.zza del Viminale, 2 Roma

Website: https://www.interno.gov.it

1.5.2 Contact Person

Att: Dott. Davide Ortenzi

Ministero dell'Interno

Direzione Centrale per i Servizi Demografici CNSD

P.zza del Viminale, 2 Roma

e-mail: davide.ortenzi@interno.it

1.5.3 Person Determining CP and CPS Suitability for the Policy

CP e CPS are always verified and approved by the Ministry of Interior who is supported by the Agency for the Digital Italy.

1.5.4 CPS approval procedures

1.6 Definitions and Acronyms

1.6.1 Definitions

Lists of definitions can be found at the end of this document.

1.6.2 Acronyms

Lists of acronyms can be found at the end of this document.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.2 Publication of Certification Information

The Ministry of Interior publishes the following information:

- Certificate Revocation List of the issuing sub CA
- OCP responder
- CP and CPS

2.3 Time or Frequency of Publication

Publication dates for CRLs and CP and CPS are as follows.

• CRLs: every 12 hours;
• CPs and CPSs: after generation/update.

2.4 Access Controls on Repositories

Read access to the information listed under points 2.2 is not restricted.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

End user certificate profile is described in the document containing the specifications of the microchip of the ID Card. This document is available at the following internet address:

https://www.cartaidentita.interno.gov.it/wp-content/uploads/2016/07/cie_3.0_-_specifiche_chip.pdf

3.1.2 Need for Names to be Meaningful

See section 3.1.1.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymity or pseudonymise in certificate names is prohibited.

3.1.4 Rules for Interpreting Various Name Forms

See section 3.1.1.

3.1.5 Uniqueness of Names

The DN of an end user certificate must be unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The private key associated to the digital certificate of the holder is stored inside the microchip of the ID Card and is protected by a PIN that is supplied to the holder himself by the Ministry of Interior. In details, he receives the first half of the PIN by the enrolling operator at the municipality, while the second half is shipped with the card.

The holder has to insert the PIN to unblock the usage of the private key, when he wants to authenticate himself to a Service Provider.

3.2.2 Authentication of Organization Identity

Not applicable.

3.2.3 Authentication of Individual Identity

The holders request ID card issuance to municipalities. The identity of the citizen requesting the CIE is verified by the enrolling operator during a face-to-face, using one of the following ways:

1. Possession and checking of another identity document (e.g. electronic passport or electronic residence permit in case of non-EU citizen);
2. Acquisition of the details of two adult witnesses who, equipped with a valid identity document and on the basis of concrete facts (kinship, affinity, neighbourhood, etc.) are able to bear witness to the identity of the applicant;
3. Verification of the previous identity card that is withdrawn and is taken by the enrolling operator in order to proceed with the issuing of the new document;
4. Verification by the badge (printed copy of the previous identity card held in duplicate by the Municipality and the competent police headquarters).

Without being identified, it's not possible to request the issuance of an ID Card and the corresponding digital certificate.

3.2.4 Non-Verified Subscriber Information

Only the information required to identify the subscriber according to the paragraph 3.2.3 is used to issue the certificate.

3.2.5 Validation of Authority

Not applicable.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

Re-key requests are not managed.

3.3.1 Identification and Authentication for Routine Re-Key

Not applicable.

3.3.2 Identification and Authentication for Re-Key after Revocation

Re-key requests are not managed.

3.4 Identification and Authentication for Revocation Request

Revocation request are sent after the withdrawal of the document, for one of the following reasons:

1	Loss
2	Theft
3	Tampering
4	Deterioration
5	Judicial measures
6	Administrative acts
10	Renewal for expiring CIE (6 months)
11	Change of personal details
12	Issuance error
13	Return as a result of death
14	Return for other reasons

In cases of loss or theft, the procedures for withdrawal of the CIE are governed in art. 7 of the Decree of the Minister of the Interior of 23 December 2015 laying down the "Technical procedures for issuance of the electronic identity card" [3]: the holder is obliged to file a report with the police force and to send the request for interdiction of the document to the CIE assistance service, according to the procedures reported on the CIE portal at address https://www.cartaidentita.interno.gov.it/contatti/. In the request the citizen must specify name, surname, tax code and details of the report.
The CIE assistance service receives the request, verifies the pertinence of the request on the monitoring systems of the Ministry of the Interior (existence and validity of the card, association with the holder etc.), contacts the issuing Municipality, provides a copy of the report and requests the withdrawal of the document. The Municipality promptly revokes the document on the issuance system.
The citizen can then appear at the Municipality of residence or stay and request a new issue by providing the report to the register official of the issuing Municipality.
In all other cases the citizen directly requests a new issue to his/her Municipality of residence or stay by delivering the old document to the registry official who then withdraws it on the issuance system and destroys it. The official then prepares a report of destruction and sends it to the Ministry of Economy and Finance. A copy of the report shall be preserved in the acts.
The withdrawal of the document implies the revocation of the digital certificate on board and is performed by the issuance system used by the operator at the municipality.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can Submit a Certificate application

The persons that are eligible to apply for certificates issuance are all persons that can apply for the Italian Identity Card according to the Decree of the Ministry of Interior, 23 December 2015.

4.1.2 Enrollment Process and Responsibilities

The enrollment process and the responsibilities are described in the Decree of the Ministry of Interior, 23 December 2015. The decree is published on the Italian Official Gazette, at the URI http://www.gazzettaufficiale.it/eli/id/2015/12/30/15A09809/sg.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The enrollment process and the responsibilities are described in the Decree of the Ministry of Interior, 23 December 2015. The decree is published on the Italian Official Gazette, at the URI http://www.gazzettaufficiale.it/eli/id/2015/12/30/15A09809/sg.

The RA CIE component that request the issuance of each digital certificate is invoked only by the SSCE subsystem of the issuing circuit of ID Card.

4.2.2 Approval or Rejection of Certificate Applications

Not applicable.

4.2.3 Time to Process Certificate Applications

The certificate is issued immediately. No delay is applied.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The RA CIE subsystem receives the various requests for the issuance of the certificates. The subsystem SSCE of the issuance circuit of the Italian ID Card sends these requests to the RA CIE on the behalf of the requests received by the municipalities. The RA CIE validates each request, extracts the data that has to be stored inside the certificate, generates an RSA keypair and a signed CSR containing the public key and sends the request to the issuing SUBCA. The SUBCA verifies the signature of the request, its format and the fields inserted according to the certificate profile. Then it issues the certificate and sends to the RA CIE that creates a PKCS#12 structures and sends it to the SSCE subsystem for the completion of the issuing process.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

No notifications to subscriber are sent when the digital certificate is issued. The subscriber (citizen) receives directly the issued ID Card with the certificate stored inside the microchip.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The certificate is deemed to have been accepted once the ID Card containing it has been delivered to its holder.

4.4.2 Publication of the Certificate by the CA

The certificates issued by the issuing SUBCA are not published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Only the owner is entitled to use the private key and certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are Service Providers which use the certificate only for the purposes stated therein. The relying party also checks the trust of certificate chain, validity period and revocation status of the certificate.

4.6 Certificate Renewal

The certificates cannot be renewed using the existing keypair.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate Re-Key

The certificate Re-key process is not used.

4.7.1 Circumstance for Certificate Re-Key

Not applicable.

4.7.2 Who May Request Certification of a New Public Key

Not applicable.

4.7.3 Processing Certificate Re-Keying Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate modification

The certificate modification is not possible.

4.8.1 Circumstance for Certificate modification

Not applicable.

4.8.2 Who May Request Certificate modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

See chapter 3.4

4.9.2 Who can Request revocation

See chapter 3.4

4.9.3 Procedure for Revocation Request

After the revocation request is sent by the municipality according to what described in chapter 3.4 the subsystem SSCE of the issuing circuit of the ID Card sends a certificate revocation request to the RA CIE component. The RA CIE verifies the request and forwards it to the issuing SUBCA, that revokes the certificate.

4.9.4 Revocation Request Grace Period

Not applicable.

4.9.5 Time Within which CA Must Process the Revocation Request

The Revocation process is immediately processed.

4.9.6 Revocation Checking Requirement for Relying Parties

Not applicable.

4.9.7 CRL Issuance Frequency (if applicable)

The CRL is published every 12 hours. See also chapter 1.3.4

4.9.8 Maximum Latency for CRLs (if applicable)

Not applicable, the CRL is immediately published after it has been generated by the issuing SUBCA.

4.9.9 On-Line Revocation/Status Checking Availability

See chapter 1.3.4

4.9.10 On-Line Revocation Checking Requirements

Not applicable.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Re-Key Compromise

Not applicable.

4.9.13 Circumstances for Suspension

The suspension of the certificates is not permitted.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

See chapter 1.3.4

4.10.1 Operational Characteristics

See chapter 1.3.4

4.10.2 Service Availability

The OCSP responder and the CRL are available 7 days a week, 24 hours per day.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

A subscriber can end the subscription either by requesting revocation of a certificate according to what is described in the chapter 3.4 .

4.12 Key Escrow and Recovery

Key escrow and/or recovery services are not available.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The IT systems of the PKI are hosted in the data center of the Ministry of Interior located in Rome, Piazza del Viminale 1. Physical access to this datacentre is permitted only to authorized personnel.

The root CA is in a restricted area inside the datacentre, is maintained offline and turned on only for the time needed to perform security operations.

In the rooms there is a fire protection system that operates with automatic detection of smoke and heat. The extinguishing system functions with inert gas: each room has its own system consisting of multiple cylinders connected to a common manifold, from which depart the tubes that go into the environment, discharging the gas through nozzles.

5.1.2 Physical Access

Access to the premises where the systems constituting the CIE PKI are hosted occurs by means of an access control system protected by smart card. Staff of the Ministry of the Interior have access to the premises. Staff of the Ministry of the Interior deliver the smart card to the other authorized staff of the IPZS.

5.1.3 Power and Air Conditioning

The power supply meets the required standards.

5.1.4 Water Exposures

The rooms have adequate protection from exposure to water.

5.1.5 Fire Prevention and Protection

Fire prevention and fire alarm regulations are observed.

5.1.6 Media Storage

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

5.1.7 Waste Disposal

To prevent unwanted disclosure of sensitive data waste is disposed of in a secure manner.

5.1.8 Off-Site Backup

There’s a disaster recovery site of the IT systems constituting the PKI CIE, that is located in Bari.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles are established to ensure that individuals are not able to change any of the security-critical components or view, generate or manipulate certificates or private keys without being noticed.

5.2.2 Number of Persons Required per Task

The key ceremony for launching Hardware Security Modules (HSM) is subject to a multiple-pairs-of-eyes principle with at least three persons from different IT units.

5.2.3 Identification and Authentication for Each Role

The trusted roles approach is implemented using a number of technical and organisational measures. Roles are identified and authenticated by using user IDs and passwords.

5.2.4 Roles Requiring Separation of Duties

By separating certain operational and administrative roles and duties, the approach ensures that no one person alone has complete control over the solution.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

In its operations, the responsible unit shall use experienced personnel who have the necessary IT expertise and specific knowledge of CA operations.

5.3.2 Background Check Procedures

The personnel are subjected to an advanced security check in order to guarantee the necessary protection of the systems.

5.3.3 Training Requirements

Personnel operating CAs for the responsible unit receive regular and ad hoc training. They are sensitized to the security relevance of their work.

5.3.4 Retraining Frequency and Requirements

Retraining is provided in particular when new or amended directives, IT systems and/or IT processes are implemented.

5.3.5 Job Rotation Frequency and Sequence

Routinely job rotation does not occur. For new personnel or assignment of new responsibilities the requirements in point 5.3.3 apply.

5.3.6 Sanctions for Unauthorized Actions

Unauthorised actions that endanger the security of the responsible unit or breach data protection requirements are punished/prosecuted by HR.

5.3.7 Independent Contractor Requirements

Independent subcontractors and their personnel are subject to the same background checks as the TSP personnel. SEE 5.3.1.

5.3.8 Documentation Supplied to Personnel

Each party makes available documentation to personnel, during initial training, retraining, or otherwise

5.4 Audit Logging Procedures

Audit logging procedures include systems auditing and are implemented for the purpose of maintaining a secure environment.

In addition, the IT systems of the PKI maintain internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers;
- Outages and major problems;
- Physical access of personnel and other persons to sensitive parts of the site;
- Security intrusions and attempts at intrusion.

The ensures that designated personnel can review log files at regular intervals and detect and report anomalous events.

The log files are protected by an access control mechanism. Log files and audit trails are backed up.

The audit logs management systems currently implemented are SYSLOG and IBM QRADAR. Syslog are gathered through Rsyslog Collector host. Events related to the PKI are traced into its database.

5.4.1 Types of Events Recorded

Each event related to the access to the systems is logged for all the components of the infrastructure.

Generated logs include:

- Database Logon events
- Operating systems Login events

The CA event logging system records events that include but are not limited to:

- Issuance of a certificate;
- Revocation of a certificate;
- Suspension of a certificate;
- (Re)activation of a certificate;
- Automatic revocation;
- Publishing of a CRL (full or incremental).

Audit trail records contain:

- The identification of the operation;
- The date and time of the operation;
- The identification of the certificate involved in the operation;
- The identity of the transaction requestor.

5.4.2 Frequency of Processing Log

Syslog audit logs, stored in a “log collector host”, are archived weekly and processed following an alarm of an anomalous event. Qradar audit logs and CA trace events log are processed following an alarm of an anomalous event.

5.4.3 Retention Period for Audit Log

Syslog audit logs stored in log collector host have unlimited retention. QRadar audit logs retention is 30 days. CA events logs have unlimited retention.

5.4.4 Protection of Audit Log

Only the administrator may access an audit Log.

Measures are taken to ensure:

- Protection against modification of the archive, such as storing the data on a write once medium;
- Protection against deletion of the archive;
- Protection against corruption of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media.

5.4.5 Audit Log Backup Procedures

All the audit logs are backed up daily.

5.4.6 Audit Collection System (Internal vs. External)

The archive collection system is internal.

5.4.7 Notification to Event-Causing Subject

Not applicable.

5.4.8 Vulnerability Assessments

There is an active and generally acceptable policy of vulnerability and patch management in place at Poligrafico which is concerned, according to the decree of the Ministry of the Interior of 23 December 2015, of the management of the main CA and of the SubCA issuer:

- Periodically, the Poligrafico's Cyber Security department produces vulnerability lists to be repaired.
- Critical vulnerabilities are represented to the Ministry of Interior who approves their fix. After the approval, the issues are immediately resolved, planning appropriate updates and patches at the production environment systems;
- Less critical vulnerabilities are addressed using a progressive release roadmap.

5.5 Records Archival

5.5.1 Types of Records Archived

All data that are relevant for the certification process must be archived. See chapter 5.4.1

5.5.2 Retention Period for Archive

See chapter 5.4.3

5.5.3 Protection of Archive

See chapter 5.4.4

5.5.4 Archive Backup Procedures

All the archives are backed up daily.

5.5.5 Requirements for Time-Stamping of Records

Not applicable.

5.5.6 Archive Collection System (Internal or External)

The archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only staff members with a clear hierarchical control and a definite job description may obtain and verify archive information.

5.6 Key Changeover

The CA shall change the key whenever the validity of a user certificate to be issued would exceed the remaining term of the CA.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

When safety incidents occur that may affect the operation of the CIE PKI, these are handled through the incident management procedure in accordance with ISMS. The Ministry of Interior is immediately informed about the security incident.

The information is collected, the risks are assessed, and a resolution procedure is processed and approved by the Ministry of Interior and the security officer (CISO).

The considerations on which the most appropriate procedure is based focus on the consequences of the specific incident.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

If it is established that the CA has faulty or manipulated computing resources, software and/or data that have an impact on the processes conducted by this entity, the system must be stopped immediately. It must be reset using software and data backups, and – after checks in safe mode – it is to be put back into operation. The faulty or modified system must be analyzed. If there is a suspicion of willful action, legal steps may be taken. If certificates have been generated using incorrect data, the subscriber or the person responsible for the IT system and/or the IT process must be informed immediately, and the certificate must be revoked by the certification authority.

5.7.3 Entity Private Key Compromise Procedures

If a CA's private key is compromised:

- the corresponding certificate must be revoked immediately;
- The Ministry of Interior and the Agency for the Digital Italy must be informed;
- a new key pair must be generated, and a new CA must be enrolled;
- the certificate of the new CA is published by the Agency for the Digital Italy into the national Trust Service List.

5.7.4 Business Continuity Capabilities after a Disaster

The capability to recover CA operations within four (4) hours following a disaster with support for all the key functions i.e. certificate issuance, certificate revocation, and publication of CRL information is guaranteed.

5.8 CA or RA Termination

The termination of both the RootCA and the issuing SubCA is not possible. Only in case of the compromission of the private key, the RootCA or the SubCA is revoked and all the issued certificates are revoked.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key material for Root Ca and the issuing SUBCA is generated by the personnel of the Ministry of Interior directly on their dedicated Hardware Security Module that is certified Common Criteria EAL 4+. Then the corresponding public keys are used to build CSR files that are used by the PKI software to complete the enrolment process.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

See chapter 4.3.1 .

6.1.4 CA Public Key Delivery to Relying Parties

Both the RootCA certificate and the issuing SubCA certificate are distributed using trusted lists maintained by the Agency for the Digital Italy.

6.1.5 Key Sizes

The keys of the Root CA and SubCAs are RSA keys and have a size of 4096 bits. Keys associated to the certificated issued to citizens are RSA keys as well and have a size of 2048 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

The following encryption algorithms are to be used.

• RSA with OID 1.2.840.113549.1.1.1

• SHA256 RSA 1.2.840.113549.1.1.11

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

For SubCAs, the key usage purposes are

- signing certificates
- signing CRLs
- Digital signature

For natural persons, the key usage purposes is

- Digital signature

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private keys of Root-CA and SubCAs are created onboard and stored inside HSMs.

Private keys of natural persons are securely stored on the Italian ID cards “CIE” issued.

6.2.1 Cryptographic Module Standards and Controls

The cryptographic modules used must be certified at least to the level of Common Criteria EAL 4+ or FIPS 140-2 Level 3.

6.2.2 Private Key (n out of m) Multi-Person Control

The cryptographic modules used must be certified at least to the level of Common Criteria EAL 4+ or FIPS 140-2 Level 3. For the Root CA a processing of the private key requires a “2 out of 3”multi-person control system.

6.2.3 Private Key Escrow

Not applicable.

6.2.4 Private Key Backup

Backups of private keys for RootCA and/or SubCAs are only permitted within the HSM's security system. Backups of private keys for natural persons are not permitted.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Not applicable.

6.2.7 Private Key Storage on Cryptographic Module

See point 6.2.1 .

6.2.8 Method of Activating Private Key

Private keys belonging to natural persons (citizens) can be used by entering a PIN.

6.2.9 Method of Deactivating Private Key

Smartcards with key materials of natural persons are locked after the following errors has been executed:

- incorrect PIN has been entered three times (in this case the citizen has to use the PUK to unblock the PIN)
- incorrect PUK has been entered ten times (the ID card must be reissued).

6.2.10 Method of Destroying Private Key

Private keys and further key material stored in the HSM leaving the HSM Environment are destroyed by using a factory reset procedure, as dictated by the HSM vendor.

6.2.11 Cryptographic Module Rating

See point 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Not applicable.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificates issued by the PKI have the following validity periods

- Root Ca certificate: 20 years
- SubCA certificate: has a validity of 15 years while its private key is used to issue user certificates only for 4 years; after 4 years it is used only to subscribe CRL and OCSP responses
- User certificates: 11 years for people aged above 18, 6 years for people aged between 3 and 18 years, 4 years for people aged under three years.

It is guaranteed that no user certificate has an expiration date above the expiration date of the certificate of the SubCA.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data for CA private keys (root CA and sub CA) is generated using HSM devices. Activation data are a by-product of the generation of the certificates for natural persons. The subscriber creates his/her own PIN during the issuance process.

6.4.2 Activation Data Protection

For the Root CA, the key custodian's each have a part of the activation key and these tokens are protected by a passphrase. The protection scheme is M of N (2 of 3). The tokens are stored in a security site.

The operational subCA's are protected by a split operational token (2 of 3) and tokens are protected by passphrase. Tokens are stored in a security site of the Ministry of Interior.

The subject's key is protected by a PIN, the PIN is delivered in two halves. The first half is delivered by the municipality. The second half by means of a postal service in a secured envelope containing the ID Card. Activation Data should be memorised, not written down. Activation Data must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g. a Certificate Holder's personal information.

6.4.3 Other Aspects of Activation Data

Not applicable.

6.5 Computer Security Controls

The CA implements appropriate computer security controls including physical and logical access controls, role separation, multi-layered controls, intrusion detection, and multi-factor authentication processes for all personnel who can cause the issuance of a certificate or cause a person to become able to issue a certificate.

6.5.1 Specific Computer Security Technical Requirements

All of the responsible unit's IT systems must be run according to the applicable IT security guidelines and must be competently protected against manipulation and espionage. See point 5.4.8.

6.5.2 Computer Security Rating

Not applicable.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Software development projects are closely monitored and controlled.

6.6.2 Security Management Controls

See chapter 6.5.1

6.6.3 Life Cycle Security Controls

Any IT systems or components that are replaced are disabled in such a way that the functions thereof and data contained therein cannot be misused.

In addition, any changes to IT systems or components must always go through the Poligrafico's IT risk management process and the Ministry of Interior must be informed and he has to approve the changes.

6.7 Network Security Controls

See chapter 6.5.1

6.8 Time-Stamping

It is guaranteed that the time is synchronous on all IT-systems (see point 5.5). Time-stamping is currently not used.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The Certificate profile is described in the document containing the specifications of the microchip of the ID Card. This document is available at the following internet address:

https://www.cartaidentita.interno.gov.it/wp-content/uploads/2016/07/cie_3.0_-_specifiche_chip.pdf

7.1.1 Version Number(s)

See section 7.1.

7.1.2 Certificate Extensions

See section 7.1.

7.1.3 Algorithm Object Identifiers

See section 7.1.

7.1.4 Name Forms

See section 7.1.

7.1.5 Name Constraints

See section 7.1.

7.1.6 Certificate Policy Object Identifier

The Certificate policy OID of the CP Authentication Certificates – Advanced – is 1.3.76.47.2.

7.1.7 Usage of Policy Constraints Extension

See section 7.1.

7.1.8 Policy Qualifiers Syntax and Semantics

See section 7.1.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

7.2 CRL Profile

7.2.1 Version Number(s)

The CRLs issued is in line with the x.509 norm, version 2.

7.2.2 CRL and CRL Entry Extensions

See section 7.1.

7.3 OCSP Profile

OSCPs responder for the check of the status of the certificates issued by the issuing SUBCA is available at the address

https://ocsp.cie.interno.gov.it.

7.3.1 Version Number(s)

OCSP Version 1 is used.

7.3.2 OCSP Extensions

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The working processes of the root CA, the issuing SubCA and other entities involved in certificate issuing are subject to regular and ad hoc inspections.

The technical framework and operational processes of the PKI undergo a regular audit pursuant to the Ministry of Interior that is supported by tthe Agency for Digital Italy. The audit results are not published.

8.1 Frequency or Circumstances of Assessment

As a rule, audits and inspections are conducted at regular intervals. Assessments will take place, among other things, with the following changes:

- change of version,
- installation of new releases or
- replacement of components

If there are no grounds for an earlier assessment, an assessment will take place every three years.

8.2 Identity/Qualifications of Assessor

Audits are conducted by the Agency for the Digital Italy. The inspectors have sufficient knowledge and expertise in the field of public key infrastructure to be able to conduct the audits.

8.3 Assessor's Relationship to Assessed Entity

Assessor’s must not be involved in the responsible unit's production process. Self-assessment is prohibited.

8.4 Topics Covered by Assessment

All topics relevant to the PKI can be inspected. The topics covered in the inspection are at the discretion of the inspector.

8.5 Actions Taken as a Result of Deficiency

If any deficiencies are determined, these must be rectified as quickly as possible by the CA in consultation with the inspector. The inspector must be informed once these deficiencies have been rectified.

8.6 Communication of Results

The results of the assessment will not be published.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

There's no specific fee to pay for the release of the certificate itself. The citizen pays for the issuance of the ID Card that contains the digital certificate issued by the issuing SUBCA. The cost of the ID Card and the way the citizen pays it are described in a decree of the Ministry of Economy and Finances published on the Italian Official Gazette and reachable at the URI http://www.gazzettaufficiale.it/eli/id/2016/06/16/16A04656/sg.

9.1.1 Certificate Issuance or Renewal Fees

Each citizen pays a cost of 16,79 euros for the issuance of the ID card containing the digital certificate, plus an extra fee for the activity that is executed by the enrolling operator at the municipality. The extra fee is typically 5,42 euros but the municipality can ask for the double of this last amount in case of renewal of the document if this last one has been lost or stolen or damaged.

9.1.2 Certificate Access Fees

There's no fee to pay for the certificate access.

9.1.3 Revocation or Status Information Access Fees

There's no fee to pay for the revocation of the certificate or for the status check.

9.1.4 Fees for Other Services

No other fees are charged than the ones described in the chapter 9.1.1

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

No financial responsibility is accepted for certificates issued under this policy.

9.2.1 Insurance Coverage

Not applicable.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information and data about PKI subscribers and participants that are not covered by point 9.3.2 are considered confidential.

9.3.2 Information Not Within the Scope of Confidential Information

All information and data that are contained in published certificates and CRLs, either explicitly (eg. e-mail addresses) or implicitly (eg. data about certification), or that can be derived from them, are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

The responsibility to protect confidential information lies with the PKI.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Personal information is stored and processed according to the EU Regulation number 679 of 2016 (GDPR) and Legislative Decree No. 101 of 2018.

9.4.2 Information Treated as Private

All information about the responsible unit's subscribers and participants is treated as confidential.

9.4.3 Information not Deemed Private

The provisions defined in point 9.3.2 apply.

9.4.4 Responsibility to Protect Private Information

Responsibility for protecting personal information lies with the Ministry of Interior.

9.4.5 Notice and Consent to use Private Information

The subscriber gives the responsible unit consent to use personal information insofar as this is required for it to render its services. In addition, all information that is not deemed confidential may be published.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The Ministry of Interior stores and processes personal information according to the EU Regulation number 679 of 2016 (GDPR) and Legislative Decree No. 101 of 2018.

Such information is disclosed to government entities only if corresponding rulings are presented that are in line with legal provisions.

9.4.7 Other Information Disclosure Circumstances

No other information disclosure circumstances are envisaged.

9.5 Intellectual Property Rights

The Ministry of Interior owns the intellectual property rights to this document. The document can be passed on to third parties as it stands.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The PKI undertakes to follow the provisions of this CP.

9.6.2 RA Representations and Warranties

The PKI and the authorities involved in registration undertake to follow the provisions of this CP.

9.6.3 Subscriber Representations and Warranties

The subscriber’s obligations are defined in point 4.5.1

9.6.4 Relying Party Representations and Warranties

The relying party’s obligations are defined in point 4.5.2. S/he must also follow his/her organisation’s certificate guidelines.

9.6.5 Representations and Warranties of other Participants

Card manufacturer (CM) obligations: according to the decree of the Ministry of Interior of 23 December 2015 (http://www.gazzettaufficiale.it/eli/id/2015/12/30/15A09809/sg) the Card Manufacturer (CM) is the Istituto Poligrafico e Zecca dello Stato S.p.A. who is responsible for the initialisation, the personalisation and the distribution of the electronic identity card containing the citizen's certificate.

The CM receives from the Ministry of Interior the data of the citizens requesting the ID Card, produces the card and ships it in a secure envelope containing a carrier and the second half of the PIN and PUK codes used to unblock the usage of the certificate and of the private key.

9.7 Disclaimers of Warranties

The Ministry of Interior makes no representation and gives no warranty, condition or undertaking in relation to the PKI for the ID Card and its operation.

9.8 Limitations of Liability

Not applicable.

9.9 Indemnities

The Ministry of Interior declines any payment of indemnities for damages arising from the use or rejection of certificates it issues.

9.10 Term and Termination

9.10.1 Term

This CP comes into force on the day it is published.

9.10.2 Termination

This document is valid until it is replaced by a new version or until the PKI operations are terminated.

9.10.3 Effect of Termination and Survival

The responsibility to protect confidential and personal information remains unaffected by the consequences of terminating this CP.

9.11 Individual Notices and Communications with Participants

No rules in this respect have been made in this CP/CPS.

9.12 Amendments

9.12.1 Procedure for Amendment

The procedures for the amendments to the CP involve the Ministry of Interior that has to approve them and publish the new version of the document.

9.12.2 Notification Mechanism and Period

After a new version of the CPS has been approved it's published beside the former version on the repository website http://www.cartaidentita.interno.gov.it/policy/cittadini_cps.pdf.

9.12.3 Circumstances Under Which OID Must be Changed

The OID will not be amended before the end of the CA's period of validity.

9.13 Dispute Resolution Provisions

All disputes associated with this CPS will be resolved according to Italian law.

9.14 Governing Law

The PKI provides its services under the provisions of the Italian law and according to what is described in the decree of the Ministry of Interior of 23 December 2015, available at the address http://www.gazzettaufficiale.it/eli/id/2015/12/30/15A09809/sg.

9.15 Compliance with Applicable Law

This CP/CPS is governed by Italian law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

All provisions of this CP/CPS are valid between the Ministry of Interior and the subscribers. If a new version is issued, this replaces all previous versions. There are no verbal or subsidiary agreements.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

If individual provisions of this CP/CPS are or become invalid, this shall not affect the remaining provisions of this CP/CPS. Likewise, if a provision is missing, this shall not affect the validity of the CP/CPS. In place of the ineffective provision, an effective provision shall be deemed to be agreed that comes closest to the original intention or that would have been determined in line with the meaning and purpose of the CP/CPS had this point been covered therein.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Not applicable.

9.16.5 Force Majeure

The Ministry of Interior accepts no liability for the violation of an obligation, for default or for non-fulfilment under this CP if this results from an underlying event that is beyond its control (eg. force majeure, war, network outage, fire, earthquake or other catastrophes).

9.17 Other Provisions

Not applicable.

APPENDIX A

Definitions & acronyms

CA	Certification Authority
Certificate	Secure assignment of public keys to a subscriber
CN	Common name (part of the Distinguished Name)
CP	Certificate Policy of a PKI
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished name
HSM	Hardware Security Module
O	Organisation (part of the Distinguished Name)
OCSP	Online Certificate Status Protocol
OID	Object identifier
OU	Organisational unit (part of the Distinguished Name)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comment, documents for global standardisation
RFC3647	This RFC describes documents that outline PKI operations
Root CA	Highest CA of a PKI
x.509v3	Certification standard
CIE	Italian Electronic Identity Card
CISO	Chief Information Security Officer