Certification Authority
Certification Practice Statement

Notartel S.p.A – S.B.

Version: 2.0

Date: 18/07/2024

SUMMARY

HISTORY

VERSION	DESCRIPTION	DATE
1.0	First edition	1 march 2022
2.0	Update: release one-shot certificate	18 july 2024

SCOPE

This document is the Certification Practice Statement – CPS – describing the practices implemented by the Notartel CA in issuing Qualified Certificates to be used to generate Qualified Signatures in compliance with the EU Regulation 910/2014 and Italian law, as mentioned in section I.
This CPS implements the provisions specified in the QCP ETSI TS 319 411 – 1 [25].

I. References to the european and italian rules of law

Law 89/1913 – Notary law	Law N. 89 of 16 February 1913 - (published on the Gazzetta Ufficiale della Repubblica Italiana No 55 of 7 March 1913) – Arrangement of Subjects and of Notary Archives
Dlgs 82/2005	Legislative Decree n. 82 of 7 March 2005 (published in the Gazzetta Ufficiale della Repubblica Italiana n. 112 of 16 May 2005), as amended by Legislative Decree n. 159 of 4 April 2006 (published on the Gazzetta Ufficiale della Repubblica Italiana n. 99 of 29 April 2006): "Code of the digital administration"
DPR 68/2005	Decree by the President of the Republic No 68 of 11 February 2005 – Rules bearing provisions for the utilisation of the Registered E-Mail, as per art. 27 of law No 3 of 16 January 2003 – (published on the Gazzetta Ufficiale della Repubblica Italiana n. 97 of 28 April 2005)
DPCM of 22/01/2013	Decree by the President of the Counsel of Ministers of February 22nd 2013 – "Technical Rules for the creation, transmission, storage, duplication, reproduction and validation, also related to timing validation, of electronic documents", published on the Gazzetta Ufficiale Serie Generale n.117 del 21-5-2013
DPCM 12 October 2007	Decree by the President of the Counsel of Ministers of 13 January 2004 – "Deferment of the time that authorizes the self-declaration regarding the compliance with the security requirements laid down in article 13(4) of the DPCM 30 October 2003."
AGID/DET/ 147/2019	Agid Determination 147/2019 - Guidelines containing the Technical Rules and Recommendations concerning the generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic timestamps
AGID/DET/185/2017	AGID Determination 185/2017 - Issue of the regulation containing the modalities with which the subjects they intend to initiate the provision of qualified trust services submit an application to AgID qualification pursuant to art. 29 of the legislative decree 7 March 2005, n. 82
CNIPA Del 11/2004	CNIPA Deliberation No 11 of 19 February 2004 – "Technical rules for reproduction and conservation of documents on optical media suitable to guarantee their conformity documents to the original – Ref. to Art. 6 (1) and (2) of the Decree by the President of the Republic No 445 of 28 December 2000 - published on the Gazzetta Ufficiale della Repubblica Italiana No 57 of 9 March 2004.
EU Regulation 2014/910	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for

	electronic transactions in the internal market and repealing Directive 1999/93/EC.
EU Regulation 2016/679	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

II. Reference to standards and law required documents

Some sections of this document make reference to provisions of the following documents that, therefore, become provisions of this document.

[1] ISO/IEC 9594-2:2005 - INTERNATIONAL STANDARD ISO/IEC 9594-2:2005 - Information technology — Open Systems Interconnection — The Directory: Models

[2] ISO/IEC 9594-8:2005 - INTERNATIONAL STANDARD ISO/IEC 9594-8:2005 – Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

[3] ISO/IEC 13335 - Information technology — Guidelines for the management of IT Security

[4] ISO/IEC 27001 - Information technology — Security techniques — Information security management systems — Requirements

[5] ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security management

[6] Manuale Operativo – published at https://ca.notartel.it

[7] Piano della Sicurezza – Security Plan - internal use document

[8] RFC 1777 – Lightweight Directory Access Protocol, 1995

[9] RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels

[10] RFC 2251 - Lightweight Directory Access Protocol (v3) – 1997

[11] RFC 4510 - Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map - 2006

[12] RFC 2314 - PKCS #10: Certification Request Syntax Version 1.5, March 1998

[13] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[14] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – 2003

[15] RFC 2828 – Internet Security Glossary - 2000

[16] RFC 3739 - Internet X.509 Public Key Infrastructure Qualified Certificates Profile, March 2004.

[17] ETSI TS 101 456 – Policy requirements for certification authorities issuing qualified certificates

[18] ETSI EN 319 412-2 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[19] ETSI TS 102 023 – Policy requirements for time-stamping authorities

[20] ETSI TS 102 280 – X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

[21] CEN/ISSS CWA 14171:2003 - General Guidelines for Electronic Signature Verification

[22] RFC 4510 - Lightweight Directory Access Protocol (LDAP): The Protocol

[23] RFC 6960 - X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP

[24] ETSI EN 319 411 – 1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[25] ETSI EN 319 411 – 2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

DEFINITIONS AND ABBREVIATIONS

Definitions

Term	Meaning	Reference
TSP	Trust Service Provider, a Service Provider, as per Regulation EU 910/2014, wins accreditation at the Agid, as qualified service provider.	
Blind envelope	Envelope inside which a text (e.g. a Personal Identification Number – PIN) is printed in a way that it cannot be read from outside. This envelope also has a tamper-evident sealing.	
Certificate	See "public-key certificate" – "PKC"	
Certificate Policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.	ISO 9594-8 [2] RFC 3647 [14]
Certificate Revocation List	A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.	ISO 9594-8 [2]
Certification Authority	An authority trusted by one or more users to create and assign public key certificates.	Certification Authority
Certification Practice Statement	A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.	RFC 3647 [14]
Trust Service Provider	Entity which provides one or more trust services	Regulation EU no. 910/2014
Certifier	The entity that provides electronic signatures services or other services related to them.	Dlgs 82/2005
Common Criteria	A security evaluation criteria that permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.	ISO/IEC 15408
Consiglio Nazionale Notarile	Italian National Notary Council.	
Consiglio Notarile Distrettuale	District Notary Council: the subject District, the jurisdiction of which most often coincides with that of a Civil Court, governing the Subjects of that area. It is Chaired by a President who, as regards Notartel CA, fulfills all the related subjects registration obligations.	
Control log	The control log is made of all records automatically taken by the	DPCM 13/1/2004

	devices installed at the Certifier's facilities, whenever the relevant conditions in the present decree for such recording occur. Records may be taken separately on various supports even of different type.	Art. 31
District Notary Council	See "Consiglio Notarile Distrettuale"	
Digital signature	A peculiar qualified signature type built on a system based on a correlated cryptographic keys pair, one public and one private, that allows the owner by means of the private key and the recipient by means of the public key, respectively, to make known and to verify the origin and integrity of one electronic document, or of one electronic documents set.	Dlsg 82/2005 as modified by Dlgs 159/2006
Distinguished Name	The distinguished name of a given object is defined as that name which consists of the sequence of the RDNs of the entry which represents the object and those of all of its superior entries (in descending order).	ISO 9594-2 [1] – section 9.7
Firewall	An internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall.	RFC 2828 [15]
Grace period	Minimum time period an initial verifier has to wait to allow any authorized entity to request a certificate revocation and the relevant revocation status provider to publish revocation status.	CWA 14171 [2]
Information Technology Security Evaluation Criteria	ITSEC is a structured set of criteria for evaluating computer security within products and systems.	
Local Registration Authority	An entity that performs on behalf of the Registration Authority the operations related to the RA responsibility.	
Long term signature	Signatures that are expected to be verified beyond the signers' certificate expiration date and, possibly, even after the expiration date of the certificate of the signers' certificate-issuing CA.	CWA 14171
Manuale Operativo	Operating Manual – The operating manual lays down the procedures to be adopted by the Certifier in carrying out his own duties.	DPCM 13/1/2004 Art. 38
One-shot certificate	Qualified certificate for a qualified electronic signature for remote procedure as defined by this Certificate Practice Statement whose keys, once generated, are available only in the context of an IT domain and exclusively for the signature transaction for which it was issued. Immediately after its use the private key is destroyed.	
Piano della Sicurezza - Security Plan	Security Plan – The Security Plan specifies the security measures set in place by the Qualified Certifier to securely perform its task as such.	DPCM 13/1/2004 Art. 30
Posta Elettronica	Any electronic mail system that provides the sender evidences of	DPR 68/2005

Certificata	shipment and of delivery of electronic documents.	
Public Key Certificate	The public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it.	ISO 9594–8 [2]
Public Key Infrastructure (PKI)	The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.	ISO 9594–8 [2]
Public List of TSP (TSL)	Trusted List of Trust Services Providers accredited at AGID, that for each CA contains the basic identification data and the self-signed certificates.	DPCM 13/1/2004 Art. 41
Qualified CA (or "Qualified Certifier")	Certifier that issues qualified certificates.	Dlgs 82/2005 Art. 27
Qualified Certificate	Certificate which meets the requirements laid down in annex I (of the Regulation UE 910/2014) and is provided by a trust-service-provider who fulfils the requirements laid down in the regulation.	Regulation UE 910/2014
Qualified signature	An electronic signature, generated with an electronic procedure ensuring that it is uniquely linked to the signatory, is created using means that the signatory can maintain under his sole control, is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable, which is based on a qualified certificate and is created by a secure-signature-creation device.	Dlgs 82/2005 as modified by Dlgs 159/2006
Registered E-Mail	See: "Posta Elettronica Certificata"	
Registration Authority	An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. Note: in this CPS the term "subscriber" is to be meant as "subject", consistently with ETSI EN 319 411 – 1 [24].	RFC 3647 [14]
Related CP	ETSI EN 319 411 – 1 [24]	
Relative distinguished name	A set of one or more attribute type and value pairs, each of which matches a distinct distinguished attribute value of the entry	ISO 9594-2 – [1]
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.	RFC 3647 [14]
Risk Analysis	the systematic process of estimating the magnitude of risks	ISO/IEC 13335 [3]
Risk Assessment	the process of combining risk identification, risk analysis and risk evaluation	ISO/IEC 13335 [3]
Qualified Signature Creation Device	Signature-creation device which meets the requirements laid down in Annex II of Regulation EU 910/2014 or Annex III of	

	Directive 1999/93/EC	
Security Policy	A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources	RFC 2828 [15]
Short term signatures	Signatures that are to be verified for a period of time that does not go beyond the signers' certificate expiration date.	CWA 14171 [21]
Subject	Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.	ETSI EN 319 411 – 1
Subscriber	Entity subscribing with a Certification Authority on behalf of one or more subjects Note: in the IETF RFC 3647 the term subscriber is used with the meaning of "subject" in ETSI EN 319 411 – 1	ETSI EN 319 411 – 1
Third party	The party which specifies any power of representation or other title relating to the subject's profession or office held. This is often referred to, in this document, as "Client Organization", when the subject belongs to this Organization, like in the case of relationship between employer and employee.	Dlgs 82/2005 Art. 28 (3)
Time-Stamping Authority	Authority that issues Time Stamp Tokens.	

Abbreviations

Abbreviation	Meaning	Reference
AgID (ex CNIPA)	Agenzia per l'Italia Digitale, national agency for digital development in Italy. Previously known as: Centro nazionale per l'Informatica nella Pubblica Amministrazione (National Center for IT in the Public Administration)	
CA	Certification Authority	
CND	Consiglio Notarile Distrettuale	
CNN	Consiglio Nazionale del Notariato National Notary Council	
CP	Certificate Policy	RFC 3647 [14]
CPS	Certification Practice Statement	RFC 3647 [14]
CRL	Certificate Revocation List	ISO 9594-8 – 2005
CRN	Secret code, known only to a certificate owner (i.e. the related Notary), to be used by this person to authenticate him/her-self when requesting in emergency on the phone the revocation/suspension of this certificate.	
CRP	Secret code, known only to the President of a LRA, to be used by this person to authenticate him/her-self when requesting in emergency on the phone the revocation/suspension of a certificate issued to one Notary belonging to the same LRA. Each certificate corresponds to one CRP.	
DN	Distinguished Name	
DPCM	Decree by the President of the Council of Ministers	
ICT	Information and Communication Technology	
IDS	Intrusion Detection System	
IETF	Internet Engineering Task Force	www.ietf.org
ITSEC	Information Technology Security Evaluation Criteria	
LRA	Local Registration Authority	
OID	Object Identifier	
PEC	Posta Elettronica Certificata	DPR 68/2005
PIN	Personal Identification Number	
PKC	Public Key Certificate	
PKCS	Public Key Cryptography Standard	RSA Laboratories

PKI	Public Key Infrastructure	
PP	Protection profile	ISO 15408
QC	Qualified Certificate	
QCP	Qualified Certificate Policy	ETSI EN 319 411 – 2 [25]
RA	Registration Authority	
Related CP	Certificate Policy ETSI EN 319 411 – 1 [24], the OID of which is specified in subsection 7.1.6	
SP	Security Policy	
QSCD	Qualified electronic Signature/Seal Creation Device	Directive 1999/93/EC Regulation (EU) 910/2014
TSA	Time Stamping Authority	
TSP	Trusted Service Provider	Regulation (EU) 910/2014
URL	Uniform Resource Locator	

1 INTRODUCTION

Notartel S.p.A. – S.B., hereinafter referred to also as NTL, is a Qualified Trusted Service Provider and acts as Certification Authority (CA) of which is accredited by Agenzia per l'Italia Digitale (AgID) and as per Regulation (EU) No 910/2014.
As per the Italian rules of law, Notartel issues qualified certificates to italian Subjects.
Notartel documents relevant for this CA are listed below:

1. PKI Standards based documents:
   a) Certificate Policy (CP) for qualified subscription certificates, also known as Manuale Operativo;
   b) Certification Practice Statement (CPS) for qualified subscription certificates (this document).
2. Law required documents:
   a) Manuale Operativo (Operating Manual)[6] required by DPCM 22/2/2013 art. 38;
   b) Piano per la Sicurezza (Security Plan) [7] required by DPCM 22/2/2013 art. 30.
3. Security standards based documents:
   a) Security Policy;
   b) Disclosure statement.

Note: Security plan and Security Policy are confidential documents and are not available to the public.

1.1 Overview

This Certification Practice Statement, hereinafter referenced to also as CPS:

- describes how NOTARTEL implements the technical, security and organizational requirements stipulated in the Qualified Certificate Policy ETSI TS 319 411 – 1 [24], relative to signature private key kept in an QSCD, the OID of which is specified in subsection 7.1.6;
- does not disclose confidential security related topics;
- is compliant with the Italian rules of law in force; more in detail: Dlgs 82/2005, DPCM 22/02/2013, AGID/DET/185/2017;
- is compliant with the Manuale Operativo [6] (Operating Manual) and the Piano della Sicurezza (Security Plan) [7] of Notartel as deposited at AGID;
- is compliant with RFC 3647 [14].

The CA is compliant to the current version of the document Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published on http://www.cabforum.org In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
In this Certification Practice Statement, keywords are used with the same meaning as in RFC 2119 [9] to Indicate Requirement Levels. In particular this RFC assigns to the following terms the meaning specified below.

1. MUST – This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT – This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. SHOULD – This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT – This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY – This word, or the adjective "OPTIONAL", mean that an item is truly optional.

This Certification Practice Statement applies to the following certificates issued by Notartel CA in abidance by the Italian rules of law:

- self-signed certificates of Notartel CA that issues qualified subscription certificates;
- Subjects' qualified subscription certificates;
- Cross-certificates issued to other CAs.

The Manuale Operativo [6] (in Italian), the ETSI CP ETSI EN 319 411 – 1 [24], this CPS and other relevant ETSI ESI and CEN documents can be retrieved from the CA web site at the address specified in Subsection 1.2.
The Piano della Sicurezza (Security plan) for security reasons is confidential and is not publicly available.

1.2 Identification

The present document is the Certification Practice Statement of the following Qualified CA.

QTSP Name:	Notartel S.p.A. – S.B.
QTSP Address:	Via Giovanni Vincenzo Gravina 4, 00196 Roma
Legal Representative:	Gian Mario Braido
Telephone: +39-0636769300	Fax: +39-0632650077
Operating sites: via Flaminia 160, 00196 Roma via Giovanni Vincenzo Gravina 4, 00196 Roma Via Flaminia 133-135, 00196 Roma	E-mail address: notartel.amministrazione@postacertificata.notariato.it esercizio@postacertificata.notariato.it
Internet address: https://ca.notartel.it https://www.notartel.it	Customer Care: customercare@notartel.it

Certification Practice Statement identifier: 0.4.0.1456.1.3

1.3 PKI Participants

This CPS applies to the PKI participants specified in the following subsections and it addresses PKI personnel, subscribers and relying parties as well as other involved entities, equipment (HW and SW), physical infrastructures, in whatever site these participants operate to perform services and activities related to the provision of subscription certificates in conformance with the above mentioned European rules of law and with the ETSI EN 319 411 - 1[24].

1.3.1 Certification Authorities

This CPS applies to the Trusted Service Provider NOTARTEL that issues to subscribers that ask for qualified certificates in compliance with the Italian rules of law and, therefore, with the Regulation EU no 910/2014.
As required by the Italian rules of law, Notartel acts as a Root CA issuing self signed certificates for its public keys. No subordinate CA certificate is issued by the root CA.

1.3.2 Registration Authorities

This CPS also applies to the Subjects, supported by RA Operators, that act as Notartel LRAs.
It also applies to RA operators when they act as master operator.

1.3.3 Subcribers

This CPS applies to subscribers.
All subscribers are presumed to use software products, supplied by the CA, in compliance with the related CP and this CPS.

1.3.4 Relying Parties

In compliance with the ETSI EN 319 411 – 1 [24] Notartel CA will uphold, on the basis of this CPS, any verification of short and long term signatures performed by relying parties based on its root certificate with valid CRLs or, where applicable, OCSP Responses demonstrating that at the time of receipt the involved certificates were neither revoked nor suspended.
It is up to the Relying Party's due diligence to provide documents with reliable time reference suitable to be used in case of dispute. Example of these time references are: Time Stamp Tokens issued by a Time Stamping Authority accredited as per the European or Italian rules of law, transmission by means of the Italian Registered Email, Italian Public Administration electronic logbooks, document storage held by a Public Officer (with the meaning per the Italian rules of law).

1.3.5 Other Participants

This CPS applies also to any external Company providing services related to Notartel CA.

1.4 Certificate Usage

Certificates issued by Notartel Qualified CA are in compliance with this CPS and its related CP [24], and can only be used:

1. by subscribers to support qualified electronic signatures they issue with the corresponding private keys in the execution of their duty,
2. by Relying Parties to verify the same qualified electronic signatures in compliance with the Italian law.

Usage of these Certificates outside this set of rules will not be upheld by Notartel Qualified CA.

1.4.1 Appropriate Certificate Uses

Certificate issued in compliance with this CPS and its related CP [24] can only be used by the physical persons to which they are issued.
In compliance with Art. 32(1) of Dlgs 82/2005, certificate owners are bound to make personal use of their signing device.
Where the signing key is declared to be used in a specific automated signing procedure, as per DPCM 22/02/2013 art. 4 (2) and (3), that key pair and the related certificate SHALL be used exclusively for that purpose.

1.4.2 Prohibited Certificate Uses

Certificates issued in compliance with this CPS and its related CP [24] SHALL NOT be used by physical persons other than those to which they have been issued, nor they can be used for encrypting, authenticating, and for any other usage than issuing qualified electronic signature, consistently with the KeyUsage extension specified therein and in compliance with the subject office.
Where the signing key is not declared (refer to item 0 of section 3.2.3) to be used in a specific automated signing procedure, as per DPCM 22/02/2013 art. 4 (2) and (3), that key pair and the related certificate SHALL NOT be used for that purpose.
Where the signing key is declared (refer to item 0 of section 3.2.3) to be used in a specific automated signing procedure, as per DPCM 22/02/2013 art. 4(2) and (3), that key pair and the related certificate SHALL NOT be used for other purposes.

1.5 Policy Administration

1.5.1 Organization administering the document

This Certification Practice Statement is issued under the responsibility of NOTARTEL the data of which are specified in section 1.2.

1.5.2 Contacts

The person in charge of this Certification Practice Statement is:

Notartel S.p.A. – S.B. General Manager
Via Giovanni Vincenzo Gravina, 4

00196 Roma (ITALY)
Telephone: +39-0636209311
Fax No: +39-0632650077

1.5.3 Person Determining CPS Suitability for the Policy

The Manager in charge of this Certification Practice Statement has the responsibility to determine its suitability for the related Qualified Certificate Policy, ETSI EN 319 411 – 1 [24].

1.5.4 CPS Approval Procedures

This CPS is approved by the Manager in charge, upon formal endorsement by the other managers involved in the various PKI related activities.

Compliance with related CP is paramount for the approval.

1.6 Definitions and acronyms

Please refer to sections “Definitions and abbreviations”.

1.7 Additional Obligations related to the Italian law

This section, additional to the RFC 3647 [14] structure, is meant to address specific obligations related to the requirements set by the Italian rules of law as in section “I”.

1.7.1 CA Obligations

In addition the obligations specified in the related CP and throughout this document, Notartel, as a Qualified CA, complies with the requirements set by the Italian rules of law. In particular it shall:

1. identify with certainty through its LRAs the certificate requester;
2. ensure the reliability of time and date specified in the issued qualified certificates and CRLs;
3. before entering the contractual relationship with a subscriber to be issued a certificate to support his/her electronic signature, Notartel SHALL inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence and scope of the AGID managed accreditation scheme and of procedures for complaints and dispute settlement; such information are publicly available via the Operating Manual [6], published on Notartel website, and the subject law;
4. deal with personal data in abidance by the GDPR; this implies that the persons’ data are collected directly from the involved person or else only upon explicit consensus received by the person such data refer to;
5. manage a reliable, timely and efficient certificate revocation and suspension service;
6. archive for at least 20 (twenty) years the information related to the certificate and for at least 30 (thirty) years the information related to its owner; this term is longer than required by the Dlgs 82/2005 that is of 20 (twenty) years;
7. issue qualified certificates for the public keys correspondent to the private ones used by the AGID to sign the Public List of Certifiers;

8. securely forward to the AGID Notartel self-signed certificates. The AGID:
   - adds them to the TSL trusted service list,
   - signs the updated List and
   - delivers the updated List to all listed certifiers.
9. timely publish in its repositories the latest Public List of Certifiers as soon as this is received from the AGID, and the certificates issued to the latest AGID public keys.

1.7.2 Client Organizations Obligations - LRA

The only Client Organizations suitable to have agreements in place for delivery of certificates to their members are the LRAs, the responsible of the LRA is in charge of abide by the obligations related to managing the subscribers as certificate owners on behalf of Notartel.

As such, every LRA by means of its responsible, in addition to the obligations specified throughout this CPS, is required to:

1. request for a certificate revocation whenever the requisite for issuing it to its owner is no more valid, due, for example, to:
   a. modification of the certificate data;
   b. cessation of the LRA relationship with the certificate owner, i.e. the involved Notary moves to another LRA;
2. inform the certificate owners at issue of all the security related topics regarding the digital signature.

2 PUBLICATION AND REPOSITORY RESPONSABILITIES

2.1 Repositories

Notartel CA manages itself the repositories where its following information is published:

1. the root certificates;
2. the Certificate Policy this CPS refers to (related CP [24]);
3. this Certification Practice Statement;
4. the "Manuale Operativo" [6], the certificate policy as deposited at the AGID.

ETSI and CEN/ISSS documents are available at their respective web sites.

2.2 Publication of Certification Information

2.2.1 Certificate repository

The certificates repository master copy, inaccessible from outside, is securely managed in systems installed on a network protected by suitable measures, such as firewalls, IDS, etc., located in safe rooms. Operational copies of the Directory are accessible through the Internet on a DMZ protected by a firewall.

The data of the publicly accessible repository copy is backed up and mirrored in different locations, among which the Disaster Recovery site, to ensure its continuous availability to the public.

In the repository are published: Notartel self-signed certificates, the CRLs and (where applicable) cross-certificates.

2.2.2 ETSI related documents publications

This CPS is published at Notartel URL: http://ca.notartel.it.

The "Manuale Operativo" [6], deposited at the AgID, is published at the AgID site (https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia) and at Notartel URL: http://ca.notartel.it.

The "§Trusted Service List" (Public List of Trusted Service Provider) is published at the AgID site (https://eidas.agid.gov.it/TL/TSL-IT.xml).

2.3 Frequency of Publication

Updated versions of the following documents SHALL be published as below specified:

1. "Manuale Operativo" [6]: after it has been published at the AGID web site;
2. Certificates for which publication is required: as soon as they are issued;
3. CRL: as detailed in section 4.9.7;
4. this CPS: soon after completion of their approval processes (see section 9.12).

2.4 Access control

The publicly accessible certificate repository URL is specified at section 1.5.1 and is accessible via the http protocols.

The repository Master copy can be accessed and maintained only by the Database Administrators and by the CA certificates and CRL managing functions.

With the exception of the present CPS that is available only at Notartel CA site, the public information mentioned in this Chapter 2 can also be respectively accessed, in addition to Notartel CA web site, at the AGID site and ETSI site. Updating this information requires write privileges which are granted only to authorized NOTARTEL, AGID and ETSI officers respectively.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The certificate owner's and issuer's names are registered in the certificates subject and issuer fields as Distinguished Names, which are structured in compliance with AGID Deliberation N.4/2005, as specified in the following subsections.

Alternative name can be used in subject certificate to specify the subject's e-mail address, as specified in section 7.1.2.

3.1.1.1 CA Name

CA's name is registered both in the subject and in the issuer field of its self-signed certificates that contain the following attributes:

CA for electronic signature

a. *commonName* (OID: 2.5.4.3), having value = "Notartel Qualified Electronic Signature CA 2021"
b. *organizationalUnitName* (OID: 2.5.4.11), having value = "Qualified Trust Service Provider"
c. *organizationIdentifier* (OID: 2.5.4.97), having value = "VATIT-05364151000"
d. *organizationName* (OID: 2.5.4.10), having value = "Notartel S.p.A."
e. *countryName* (OID: 2.5.4.6), having value = "IT"

CA for timestamping

a. *commonName* (OID: 2.5.4.3), having value = "Notartel Qualified TimeStamp CA 2021"
b. *organizationalUnitName* (OID: 2.5.4.11), having value = "Qualified Time Stamping Authority"
c. *organizationIdentifier* (OID: 2.5.4.97), having value = "VATIT-05364151000"
d. *organizationName* (OID: 2.5.4.10), having value = "Notartel S.p.A."
e. *countryName* (OID: 2.5.4.6), having value = "IT"

3.1.1.2 Subject Name

The **issuer** field value is as specified in the subsection 3.1.1.1.
The **subject** Distinguished Name depends on subject types, as hereafter specified.

a) *dnQualifier* (OID: 2.5.4.46), indicating the id of the subscriber for the RA
b) *serialNumber* (OID: 2.5.4.5), indicating the Italian Fiscal Code, or any other identification number required by EIDAS
c) *surname* (OID: 2.5.4.4)

d) *givenName* (OID: 2.5.4.42)

e) *commonName* (OID: 2.5.4.3), indicating the Given Name and the Surname in this order

f) *countryName* (OID: 2.5.4.6), having value = "IT"

Other X.501 distinguished names components are usable, as specified Agid determinations.

3.1.2 Need for Names to be meaningful

The need for names to be meaningful, as per the ETSI EN 319 411 – 1, ETSI EN 319 412-2, and the corresponding Italian rules of law currently in force, is achieved by adopting the law compliant Certificate profile specified in section 7.1.

3.1.3 Anonymity or Pseudonymity of Subscribers

Not applicable.

3.1.4 Rules for interpreting various Name Forms

Agid decision rules apply.

The e-mail address reports the address declared by the subject at registration time, or in subsequent communications, to receive e-mails.

3.1.5 Recognition, Authentication and Role of Trademarks

No stipulation.

3.2 Initial Identity validation

3.2.1 Proof of Possession of Private Key

This proof of possession is achieved as per the following subsections.

3.2.1.1 Subject registration and certification

The LRA responsible register subjects as specified in section 3.2.3.

Notartel CA associates to each request:

1. a Personal ID and a ERC code to be used by the RAO to request for his/her certificate revocation or suspension in emergency;
2. the PIN and PUK related to the private key;
3. An OTP to sign with strong auth.

The subject after authentication to a specific application with the received codes as in item 1, activates the generation of the remote signing key pair and of the correspondent signing certificate requests as per PKCS#10 rel. 1.5 (RFC 2314 [12]). Being this request signed with the corresponding private key the proof of possession is ensured. Where necessary, help can be provided by the LRA Operator in the registration process, or by Notartel RA Operator in the registration or authorization processes.

Notartel CA generates the private key and thr subscription certificate, as indicated in subsection 4.3, the private key is subsequently written into the HSM.

3.2.1.2 Additional Provision – Subject's key Management

Notartel detailed internal procedures provide for a reliable management of the subjects' keys preserved on HSM.
The management of their distribution and inventory is under the responsibility of a specific Manager, appointed by a NOTARTEL suitably high level management.

3.2.2 Authentication of Organization Identity

No stipulation.

3.2.3 Authentication of Individual Identity

For each request, Notartel collect the following information:

1. Name and Surname;
2. Date of birth;
3. City of birth;
4. Personal identification number (es. Fiscal code, etc);
5. Identification document data;
6. Personal contacts (mobile, phone number, etc);
7. e-mail address.

If the subject signing key will be used in an automated signing procedure, he/she SHALL subscribe a binding statement that, as per DPCM 22/02/2013 art. 4 (2) and (3), such key pair and the related certificate will be used exclusively for that purpose.

These data are stored by Notartel in a specific registration database.
Notartel use six methods to identify an individual identity (phisical person).
Method 1: Identification in person;
Method 2: identification via videoconferencing system;
Method 3: identification via digital signature;
Method 4: identification via CIE, Electronic Passport, SPID (at least level 2);
Method 5: identification via a previous one-shot certificate (OneShot only);
Method 6: identification via Notary Intermediary (OneShot only).

3.2.3.1 Identification in person

The applicant SHALL be properly identified by LRA via at least one of the following official Italian identification documents:

- Citizens residing in Italy:
  - Identity card;

- Electronic identity card (CIE);
- Passport;
- Driving licence.

- Citizens residing in an EU member state:
  - Electronic identity card (CIE);
  - Passport.
- Citizens residing in a non-EU state:
  - Passport.

3.2.3.2 Identification via VDC

Identification is carried out by CA operators duly trained through a video call with the applicant remotely.

The operator performing the identification verifies the identity of the holder by checking a valid and non-expired document, in accordance with Article 35, Presidential Decree of 28 December 2000, no. 445, which is presented through the video call. The recording of the exhibition process by the holder guarantees the recognition of the holder. This main process is supported by other security processes as established by AGID regulations on the issuance of qualified digital certificates remotely.

3.2.3.3 Identification via digital signature

The certifier relies on recognition already carried out by another certifier. The holder already has a signature device with an associated qualified certificate still valid. The holder submits to the CA the duly completed and digitally signed request for the issuance of the OneShot Certificate, if in person, through the Registration Office or, if remotely, through the specific application provided by Notartel.

Registration data is stored exclusively in electronic format in this case.

3.2.3.4 Identification via electronic document or SPID

The certifier relies on recognition already carried out by an SPID Issuing Body or by the Municipality that issued the CIE. The holder, already in possession of a secure device with a CIE certificate or valid SPID identity, authenticates to the certifier's portal and submits the request for the issuance of the one-shot certificate.

Registration data is stored exclusively in electronic format in this case.

3.2.3.5 Identification via previous OneShot signature

Method valid only for issuing a OneShot signature.

If an applicant has already obtained a previous one-shot signature certificate from the Notartel certifier within a year of the last request, (a situation highlighted by the application which, holding the registry of certificates already issued, verifies their presence starting from the TIN code), the request will be signed using the recognition already carried out.

Registration data is also stored exclusively in electronic format in this case.

3.2.3.6 Identification via notary intermediation

Method valid only for issuing a OneShot signature.

This method is only provided for in-person issuance, when the applicant does not have any technological system for identification. In this case, the notary, as described in the introduction, forwards the certificate request for the applicant authenticated by him in the capacity of intermediary (public official) using the functionalities provided by the Notartel certifier in PNI.

The digital request is stored by the certifier, like the previous methods, and a printed copy signed by the requesting party remains with the notary for record-keeping purposes.

3.2.4 Non-verified Subject or Subscriber information

3.2.4.1 Professional qualifications

No stipulations.

3.2.4.2 Association with a Legal Person

No stipulations.

3.2.4.3 Subject belonging to a Client Organization

No stipulations.

3.2.5 Validation of Authority

No stipulations.

3.2.6 Criteria for Interoperation

Requirement to ensure interoperability among Italian accredited Qualified Certificate issuers are specified in the current Agid decision and by EIDAS. Additionally, issuers several requirements must be met, that are stipulated in the set of Italian rules of law relevant to electronic signatures. All these requirements, amongst others, will be subject to inspections by the AGID, as per Art. 31 of Dlgs 82/2005.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The subject whose certificate expiration date is approaching, at least ninety days before the certificate expiration date (i.e. the value in the “notAfter” certificate field) should report to the LRA, asking for a new private key to be issued.

3.3.2 Identification and Authentication for Re-Key After Revocation

A complete new private key issuance procedure is to be performed as per section 3.2.1.1.

3.3.3 Identification and Authentication for Revocation Request

The following methods can be used:

1. revocation or suspension request subscribed with a handwritten signature;
    a) where the subject is requesting revocation of his/her own certificate, he/she SHALL report to the LRA who testifies for his/her identity;
    b) where the LRA is requesting revocation of a certificate the LRA's request is forwarded directly to Notartel;
2. revocation or suspension request subscribed with a qualified signature; the qualified signature vouches indisputably for the request authenticity of origin and rightfulness;

Further details are specified in section 4.9.

The subject will be notified of any revocation/suspension.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A qualified certificate application can be submitted only by the subject him/her-self, candidate certificate owner, following the procedure described in section 3.2.1.1.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 Subject registration

The LRA, duly assisted by the LRA Operator, collects the information specified in section 3.2.3 that are uploaded via secured web channel into Notartel subjects' database, and authorizes the initiation of the certification process that is implemented as specified in section 3.2.1.1.

4.1.2.2 LRA registration

When a newly appointed LRA is taking office, his/her registration is performed via secured web channel or through a digital signature of the LRA (ex. notary and his office).

These requests are approved by a Central RA Operator.

4.2 Certificate Application processing

4.2.1 Performing Identification and Authentication Functions

The certificate requester's identity is reliably verified during the enrollment process as specified in section 4.1.2.

As specified in sections 3.2.1.1, the certificate request complies with the RFC 2314 [12] (i.e. PKCS#10) provisions, therefore its formal correctness along with the reliability of the enrollment process ensure the correspondence between private and public key as well as the owner's identity and data correctness.

4.2.2 Approval or Rejection of Applications

Based on the controls specified in 4.2.1 and 4.3.1 sections the certification request is approved or rejected.

If it is approved the corresponding certificate is generated and forwarded to the certificate subject to be written in the HSM and systems of Notartel CA.

If it is rejected this may depend on one of these two cases:

1. CA Software malfunction; in which case, once fixed, the certificate generation procedure is newly executed;
2. malfunction of the certificate request creation application; in which case, once fixed, the certificate generation procedure is newly executed.

4.2.3 Time to Process Certificate Applications

If the certificate request is approved the corresponding certificate is immediately generated and forwarded to the certificate subject to be written in the HSM.

The time to complete the overall process from registration to certificate delivery, as specified at subsection 3.2.1.1, depends on the time needed to perform these phases:

1. registration and authorization by the LRA;
2. forward to NOTARTEL LRA of the request for remote signature;
3. delivery of PIN and passwords to the subject to activate the private key.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The CA performs the verifications specified at subsection 4.2.1, namely:

1. existence of the certificate requester's information in the CA registration database;
2. correspondence between the information in the certificate request and in the registration database;
3. correspondence between private and public key, as per RFC 2314 [12] (i.e. PKCS#10) provisions.

If the certificate request is approved the corresponding certificate is immediately generated and forwarded to the certificate subject to be written in the HSM.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The subject receives at the email address he/she previously specified the related secret codes with which the certification process is activated by the subject.

The subject is informed online and by email of the certification process completion by the related application program, once the generated certificate has been generated.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The certificate requester SHALL verify immediately upon delivery the correctness of the certificate data and, if they should be incorrect, SHALL immediately request for the certificate revocation as per section 4.9.3.

4.4.2 Publication of the Certificate by the CA

The CA SHALL publish only its own self-signed certificates and, where applicable, cross-certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subjects shall use their NOTARTEL certified key pairs only to issue digital signatures, as defined in section 1(1), letter s) of Dlgs 82/2005.

Where they have signed a declaration that the said key pair will be used with a specific automated procedure, they SHALL only use it with such a procedure.

In the case of OneShot certificate shall only be used in a specific context or for a specific purpose. It is not intended for general use or for multiple purposes.

No other usage of the subscription key pair is allowed.

4.5.1.1 Signature Issuance Application and Document formats

The certificate owner SHOULD make use of a signature issuance application provided by Notartel CA.

Otherwise, if documents to be signed are in dynamic formats, that intrinsically can host malware suitable to modify the presentation of document, the certificate owner SHALL transform those documents into static ones before signing them, to avoid the above mentioned malware.

4.5.1.2 Signature Issuance devices

The signature issuance application SHOULD be installed and used only on suitably secured devices, that SHOULD be under the subject direct or indirect control, equipped with SW and/or HW tools suitable to prevent attacks enacted with malware such as virus, Trojan horse, spyware, capable to modify the data to be signed or to stealthily acquire the signature activation code.

4.5.2 Relying Party Public Key and Certificate Usage

4.5.2.1 Third Parties acting as Relying Party in relation with NOTARTEL CA issued certificates

Relying Parties who are not subscribers of NOTARTEL issued certificates, in order to verify signatures based on NOTARTEL issued certificates SHALL verify the certificates validity as specified in section 4.9.6.

4.5.2.2 Cautions when referring to CRLs

A relying party that verifies a digital signature supported by certificates issued by Notartel CA, SHOULD take also into account the time necessary:

1. to who requests a revocation/suspension to submit such request to the CA;
2. to the CA to execute the organizational and computing procedures that process the request and publish the related output.

In order to assess a signature validity the status of the related certificate SHALL be checked at time of receipt of the signed document, and, if necessary, a trusted time reference SHOULD be associated to the signed document to reliably mark the actual date of receipt (e.g. a Time Stamp Token issued by a TSA belonging to a CA listed in the Public List of Certifiers, or the time included in a Posta Elettronica Certificata – PEC – message with which the signed document was delivered).

In addition to this time reference the signature verifier SHALL take into account that the CA publishes a new CRL at every revocation event or at least every 8 hours.

Note: “force majeure” events may occur that might delay the CRL publication. To prevent their negative effects, Notartel CA issues CRLs some minutes before the expected time (i.e. the value in the current CRL “nextUpdate” field). However in exceptional cases a CRL might be issued beyond the value in this“nextUpdate” field, therefore relying parties may happen to access an expired CRL, i.e. where the value in the CRL “nextUpdate” field is in the past. In such exceptional events, relying parties SHALL abstain from assessing as valid digital signatures associated to a trusted time reference that is subsequent to such past “nextUpdate” value.

4.5.3 Use restrictions and value limits

OneShot certificates are limited only to the use in the domain specified by the contract, for the subscription of digital documents made available to the Subject by the CA or the Subscriber. In this case, the digital documents may be related to relationships between the Subscriber and the Subject. The use of the certificate is technically limited to the signature of the underlying documents.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal[1]

No Certificate renewal is provided by NOTARTEL.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

[1] RFC 3647 section 4.4.6: "Certificate renewal means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate."

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

4.7.1.1 End User Certificate Re-Key

No stipulation.

4.7.2 Processing Certificate Re-Keying Requests

No stipulation.

4.7.3 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.4 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.5 Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.6 Notification of Certificate Issuance by the CA to Other Entities

The same provision as in section 4.4.3 apply.

4.8 Certificate Modification

No Certificate modification is implemented: any change in the certificate data will cause a new certificate to be issued, with a new generated key pair.

4.8.1 Circumstances for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

Suspension is a revocation with a specific "reasonCode", therefore in the following subsections only the term "revocation" is used. Where provisions are applicable only to revocation or suspension this is clearly specified. Further details for suspension are indicated in sections 4.9.13 and beyond. Revoked certificates are kept into CRL also after their expiration.

4.9.1 Circumstances for Revocation

When an anticipated cessation of validity is planned for a certificate, Notartel CA revokes at it at the requested time, for example in the case when the certificate owner is planned to cease from the task for which his/her certificate was issued, or in case of planned absence of the certificate owner from his/her duty, in which case a "suspension" is carried out.
When Notartel CA cannot timely ascertain one revocation request authenticity, the certificate at issue is suspended for the period of time necessary to ascertain such authentication. If and when the request proves as authentic, the certificate is outright revoked.
The certificate revocation or suspension is always communicated by Notartel CA to the subject, also indicating the time and date the certificate at issue was revoked/suspended.

4.9.1.1 Request for revocation submitted by the subject

A subject SHALL ask for his/her own certificate revocation at least in the following cases:

1. loss of exclusive control of the private key, this may depend on one or more of the following reasons:
   a) theft or outright loss of the private key;
   b) reasonable doubt that the confidentiality of the private key activation codes has been compromised;
   c) reasonable doubt that the confidentiality of the private key has been compromised;
2. private key malfunction.

In previous case 1a) the subject SHALL also report the loss or theft to the competent authority.
In any moment a subject can request for his/her certificate revocation in writing, also specifying the date of effectiveness.

4.9.1.2 Request for revocation submitted by the LRA/RAO

The LRA SHALL ask for a subject revocation at least in the following cases:

1. when the subject loses his/her office, regardless of the reason:
   a) the subject quits or is dismissed from his office;
   b) the subject moves to another District;
   c) any other reason for ceasing from his/her office;
2. upon authority orders implying cessation from the subject office.

RAO SHALL ask for a LRA's certificate revocation whenever events analogue to those above specified occur to that LRA.

4.9.1.3 Request for revocation enacted autonomously by Notartel

Notartel timely revokes a certificate when Notartel becomes aware of one or more of the following circumstances:

1. case 1 of section 4.9.1.1;
2. the certificate owner's capabilities have been or are subject to limitation, that the signing device has been illegally used or that signature forgeries have occurred;
3. any variation of substantial certificate data, such as the subject's fiscal code etc;

upon completion of the signing operations for which the OneShot certificate was issued.

Notartel CA before revoking a qualified certificate notifies the related notary in advance, unless good reasons prevent Notartel from doing this.

4.9.1.4 Used Revocation Reason Codes

Notartel adopts at least the following reason codes among those provided for by the ISO/IEC 9594-8:2005:

- Unspecified;
- KeyCompromise;
- CACompromise.

4.9.2 Who Can Request Revocation

A certificate can be revoked or suspended:

1. upon request by the certificate owner,
2. upon request by the relevant LRA,
3. upon request by RAO upon solicitation by the involved LRA,
4. upon Notartel CA initiative,
5. upon authorities' order.

4.9.3 Procedure for Revocation or Suspension Request

4.9.3.1 Basic Stipulations for Revocation Requests

The certificate owner and, where applicable, the President of the LRA the subject belongs to, or RAO, upon solicitation by LRA, can ask for a subject certificate revocation by using one of the three following mechanisms:

- Submit a request subscribed with handwritten signature;
- Submit a request subscribed with digital signature;
- Report by telephone to the Customer care / RAO (only for urgent suspension).

Notartel CA processes the request giving way to its revocation, or suspension, and to its publication in the CRL that is then published.

Both the subject and the LRA are notified of the certificate revocation or suspension.

Once a certificate is revoked / suspended as per the required timing and manners, the certificate owner is notified of the event by e-mail.

4.9.3.2 Revocation Request subscribed with handwritten signature

a) The subject, where applicable, SHALL submit his/her request, signed with a handwritten signature, to the LRA.
b) The LRA SHALL submit the revocation request, be it signed by him/her-self or by the subject, to Notartel CA.
c) The revocation or suspension request SHALL specify what follows:
    1. certificate owner's name and surname,
    2. site and LRA where he/she belongs to,
    3. certificate serial number, if available,
    4. revocation or suspension reason,
    5. any other information suitable to help identify the cases where a greater urgency of even emergency applies.
d) Revocation/suspension requests are submitted to Notartel CA.

4.9.3.3 Revocation Request subscribed with digital signature

The requester, be the subject or the LRA, SHALL forward the digitally signed request in telematic way to Notartel CA, also through the web portal of the RA.

The same stipulations as in section 4.9.3.2 item c) apply.

4.9.3.4 Revocation Request through Customer Care / RAO

a) The requester sends to the Customer Care / RAO and is authenticated by means of his/her digital signature or hadwritten signature
b) The following information SHALL be provided to the Customer Care:
    1. LRA identifier, where this is the revocation requester;
    2. certificate owner's name and surname;
    3. LRA the subject belongs to;
    4. reason and time of effect of the revocation or suspension;
    5. all information useful to define the urgency (or emergency) of the case.
c) Notartel CA revokes the certificate at issue, adds its identifier in the CRL that is afterwards published in the Directory.

4.9.3.5 Revocation and suspension service availability

Different services availability apply depending on the request submission type of revocation and suspension.

1. Telematic submission of digitally signed requests via RA application: 24*7 service.
2. Digitally signed or handwritten signature requests via Customer Care: Monday to Friday – 9:00 a.m. through 6:00 p.m.

4.9.4 Revocation Request Grace Period

Note: in this CPS, that complies with TS 101 456, the meaning of the term “Grace Period” is slightly different from its meaning in the RFC 3647, since it also encompasses the period necessary to the CA to perform the entire revocation process, including the revocation publication.

A Relying Party SHALL take into account, in order to assess a signature validity, the current CRL or, preferably, one CRL issued at latest 1 hour after the receipt of the signed document or after a trusted time associated to the signed document, e.g. a Time Stamp Token or the time specified in a PEC e-mail.

This procedure also suites the case when the revocation request is received by Notartel CA so close to the next CRL issue time that it is impossible for the CA to process it and publish it in such CRL. As a consequence the revoked/suspended certificate will be referred to in the second next CRL.

4.9.5 Time Within Which CA Must Process the Revocation Request

Notartel CA systems process the revocation requests queue at intervals of few minutes, at latest 1 hour after the event. Unless abnormal conditions occur, as hinted to in the previous subsection, revocations will be reported in the next CRL. A new CRL is issued at least every 8 hours.

4.9.6 Revocation Checking Requirements for Relying Parties

Unless Relying Parties make use of the verification application provided for by Notartel CA, they SHALL take into account what follows when assessing a signature supported by a NOTARTEL CA issued.

1. The TSL published by Agid.
2. The self-signed certificate of the CA that issued the certificate associated to the signature under verification MUST be listed in the TSL.
3. A suitable CRL, i.e. that is accessed taking into account the Grace Period as per subsection 4.9.4, SHALL be downloaded from the address indicated in the signer’s certificate’s CRL Distribution Point.
4. The signature of the CRL SHALL be verified with the above CA certificate (see item 3).
5. The value in the “thisUpdate” field in the retrieved CRL MUST be subsequent to the time of receipt or, where applicable, to the time specified in the associated Trusted Time plus the Grace Period (see 4.9.4) and the value in the “nextUpdate” field MUST be beyond the moment the verification is carried out.

If the values in the “thisUpdate” field or in the “nextUpdate” field do not meet the above specified requirements, the Relying Party SHALL retrieve subsequent CRLs until fetching one that meets them.

6. The fetched CRL, meeting the above requirements, SHALL NOT refer to the certificate supporting the signature being verified.
7. The signature MUST be cryptographically correct.
8. The Relying Party SHALL make use of verification applications capable at least to give a warning if the signed document presentation has changed since signing time, without affecting the signature cryptographic validity.

Note: no claim raised against Notartel CA will be accepted if the Relying Parties cannot demonstrate they have complied with all of the above requirements.

4.9.7 CRL Issuance Frequency

CRLs are issued at every revocation event or at least every 24 hours.

4.9.8 Maximum Latency for CRLs

Once a CRL is issued it is published over the internet and in its shadow copies with the minimum possible delay, depending on the network and systems conditions.

4.9.9 On-Line Revocation/Status Checking Availability

An OCSP system, RFC 6960 [23] compliant, is indicated by Notartel in the AIA extension.

4.9.10 On-Line Revocation Checking Requirements

The certificates revocation status verification by means of Notartel CA OCSP, when applicable, is to be performed according to the RFC 6960 [23].

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re-Key Compromise

Any authorized entity (see section 4.9.1.4) SHALL immediately request for a certificate revocation with reason code “keyCompromise” whenever they become aware of one of the events described in item 1 of section 4.9.1.1.

What specified in the second and third paragraph of 4.9.1 applies.

4.9.13 Circumstances for Suspension

A certificate can be suspended for a limited time in the following cases:

1. when its certificate owner will be absent on leave; this can be requested by both the subject or the LRA;
2. upon competent authority’s proceedings implying temporary cessation of the subject from his/her signature capabilities.

4.9.14 Who Can Request Suspension

Suspension can be requested by the same persons as in section 4.9.14.

4.9.15 Procedure for Suspension Request

In addition to stipulations in section 4.9.3, a certificate SHALL be suspended whenever Notartel CA cannot authenticate a revocation request before publishing its outcome in the CRL. The certificate at issue SHALL remain suspended up to the end of the authentication process, and will be either outright revoked or reactivated depending on the authentication outcome.

4.9.16 Limits on Suspension Period

Section 4.9.13 specifies the different cases for which a certificate can be suspended. The related duration depends on the specific case identified in that section.

4.9.17 Certificate Reactivation after Suspension – Additional section

A suspended certificate is reactivated:

1. automatically at the end of its *planned* suspension period;
2. upon request by the LRA, submitted in writing (i.e. subscribed with a handwritten or digital signature) in the same way as per its revocation/suspension (see section 4.9.3).

Whenever a certificate is reactivated, it reference is removed from the CRL and both the owner and the LRA are notified with a digitally signed document or via Registered Letter.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status information is provided through Certificate Revocation Lists published over internet and OCSP service, also openly accessible by the public and situated in different sites to ensure information provision even in case of disaster.

In each issued certificate the related CRL Distribution Point address is specified, pointing to a CRL or OCSP service.

4.10.2 Service Availability

The CRL and OCSP availability is ensured 24*7, also due to the directory replication mechanism.

4.10.3 Operational Features

No stipulations.

4.11 End of Subscription

Given the CA peculiarity (it serves Subjects whose duty is to ensure reliable service and documents retrievability in the centuries to come) end of subscription is not an issue. A subject can quit the CA services only when he/she is dismissed, or quits office.

In this case the related certificate is revoked as detailed in section 4.9.3.

4.12 Key Escrow and Recovery

Only CA private keys are backed up and restored, when required2.

No subscription private key is escrowed. This is consistent with QCP ETSI EN 319 411 – 1 [24] section 6.3.12 that states: “

a) The security of any duplicated subject's private keys shall be at the same level as for the original subject's private keys.

b) The number of any duplicated subject's private keys shall not exceed the minimum needed to ensure continuity of the service.”

This is also consistent with DPCM 22/02/2013 at art. 8(1): “

Except as provided for in paragraphs 2, 3 and 4, duplication of the private key and devices containing it is forbidden”

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

[2] For specific security reasons it is allowed that certification private keys are exported, provided that this is performed with procedures suitable not to reduce the security level.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

All PKI related buildings are compliant with the Italian rules of law regarding safety and security measures.

The buildings are under human and/or advanced electronic surveillance and monitoring.

5.1.2 Physical Access

Central PKI systems are installed inside dedicated premises the access to which is controlled and protected via both electronic or human control and surveillance systems.

These systems are located inside a dedicated network, protected from attacks by means of firewalls, IDS, etc.

Physical access is reserved to authorized people. Sensitive PKI tasks are required to be performed under at least dual control. Occasional visitors (including unauthorized people with a need to access, e.g.: service and maintenance personnel, and even managers) may access these areas only under prior authorization and are continuously escorted by regularly authorized personnel, who are directly accountable for these escorted persons. All access is logged and physical access audit trails are kept.

Active and passive anti intrusion systems are in operation.

5.1.3 Power and Air Conditioning

A UPS ensures seamless processing even in case of power interruption. It is also complemented by a long lasting emergency power generator, the duration of which depends only on the fuel stock and regular supply.

PKI areas air conditioning is sized to meet the devices suppliers' specifications.

5.1.4 Water Exposures

The CA site is located in a place at the level of a nearby river, but the entire geographic area is duly monitored and managed to prevent floods that have never occurred since 1926, when the Tiber river embankments were completed, apart from a really minor one in 1937.

The Disaster Recovery site is far from any water stream.

5.1.5 Fire Prevention and Protection

Fire prevention and protection measures comply with the current Italian rules of law. The fire detector and extinguishing system is inspected every 6 months.

5.1.6 Media Storage

Media are stocked in safe and secure places. Procedures in force aim to protect them from tampering, in order to keep them free from malicious codes since their arrival up to their sanitized disposal, and to prevent that media are stolen.
NOTARTEL Security Policies detail PKI related cryptographic devices secure storage and handling.

5.1.7 Waste Disposal

In addition to the stipulation specified in the related CP [24], the following apply.
Dangerous and toxic waste is disposed of according to the rules of law in force.
Disposition of paper documents and of electronic media bearing sensitive information is performed in a secure way. Paper documents are shredded and electronic media are degaussed if of magnetic type, otherwise are outright destroyed: optical media are cut or pierced several times, device bearing chips like smart cards are either cut in parts or pierced, paying attention that the chip is actually divided in at least two parts or that is smashed in an unrecoverable way.

5.1.8 Off-Site Backup

All information that is required for service continuity is backed up in local systems and in a remote site. Back-up copies are generated at regular intervals, databases are implemented by means of their mirroring functions over MAN (Metropolitan Area Network) between primary site and disaster recovery site.

5.2 Procedural Controls

The Italian applicable rules of law require that specific managing roles are clearly separated. ISO/IEC 27001 [4] Annex A, section A.10.1.3 and ISO/IEC 27002 [5] section 10.1.33 similarly requires separation of duties when sensitive procedures are involved.
Notartel CA strictly enforces the segregation of roles both in compliance of the Italian rules of law and of the ISO/IEC 27002.

5.2.1 Trusted Roles

Employees are appointed to trusted roles by a suitably high level management of Notartel in agreement with Notartel management, depending on the involved role. For security reasons, details are not specified hereinafter for these roles, with the sole exception of the Certificate Issuance Manager who has also operational responsibilities.
Also trusted operating roles are separated and are assigned by Notartel high level management with agreement with NOTARTEL management, depending on the involved role.
Access to restricted areas is governed by specific procedures, that also require that, when people authorized to access these areas quit, resign or are moved to a different operation area, their PKI related privileges SHALL be timely revoked and they SHALL return any PKI relevant identity badge or credential that grants access to restricted areas, as well as all confidential documentation. Where applicable they are also reminded their obligation not to disclose confidential information even after the termination of their employment relationship.

5.2.2 Number of Persons Required per Task

No key trusted task is assigned to only one officer, in order to prevent service interruptions.
On the other hand, all sensitive activities are performed under at least dual control, achieved at least with organizational procedures and, where possible, also by technical means.

5.2.3 Identification and Authentication for Each Role

All officers are assigned their PKI related duties upon identification face to face.
They authenticate themselves to the related procedures either with physical credentials (e.g. smart cards, etc.) or logical (e.g. password).
When passwords are used, their composition rules complexity is directly related to the accessed function sensitiveness, additionally they are to be changed with a frequency that is inversely dependent on their robustness, e.g. long passwords made of uppercase, lowercase, numbers and special characters require a less frequent change than short and purely numerical passwords.

[3] Control: "Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets."

5.2.4 Roles Requiring Separation of Duties

One person is not allowed to perform tasks that might be in conflicting situations, in particular he/she cannot be in charge of multiple jobs such that:

1. one job authorizes another jobs operation;
2. one job controls another job outcomes correctness;
3. one job execution and security depends on, or is affected by, the completion and / or correct execution of another job.

Persons can be in charge also of non PKI-related roles, if they do not conflict with their PKI-related ones.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The following provisions apply, in addition to provisions laid down in the related CP [24].
As required by the rules of law in force, officers appointed with the managing roles mentioned in Section 5.2.1 MUST have a minimum of 5 years background in information systems analysis, development, planning or managing.

5.3.2 Background Check Procedures

A screening on the background of personnel about to be hired is performed to the extent that this is allowed by the rules of law in force, in particular related to privacy (i.e. GDPR and implementation juridical instruments). Their CV is verified at the previous employers.
Where this information is already in possession of Notartel or of its CA service provider Notartel, this verification is performed up to where this is legally possible. No person that has been subject to discipline measure due to serious security violation is employed in sensitive PKI roles.
Finally, PKI related functions SHALL be assigned only to personnel who has previously demonstrated, in addition to the specific technical skill, also a specific carefulness in complying with security and confidentiality related tasks.

5.3.3 Training Requirements

All PKI related employees are timely trained on PKI technology, on Notartel CA organization security policies and procedures, prior to being assigned to PKI related tasks.
In particular, in addition to training the personnel on the day by day operations, a special attention is given in training them on incident reporting and on dealing with disaster situations.

5.3.4 Retraining Frequency and Requirements

All employees appointed to PKI tasks are duly trained whenever the PKI technology undergoes updates and security policies, procedures, and organization change.
Yearly all PKI officers all delivered classes on the main procedures they are related to, in particular on the emergency related ones, to ensure that they are capable to run even the little used procedures, should exceptional cases occur.

5.3.5 Job Rotation Frequency and Sequence

Job rotation MAY be performed both to ensure a seamless smooth process execution even in case of emergency that reduce the staffing, and to avoid that a “collusion feeling” is established among operators that frequently and jointly operate.
Generally speaking, no “a priory” general rule exists, except the following one: positions MUST not be overturned, i.e. one person who previously was verifying the correctness of another person’s task outcomes cannot swap tasks with that very person, to avoid the above mentioned collusion.

5.3.6 Sanctions for Unauthorized Actions

The Italian rules of law are enforced in case of violation of security measures. All interested employees are informed of the sanctions that can be applied as per the collective working contract. Should civil or criminal offences be perpetrated, NOTARTEL SHALL be free to take legal steps.

5.3.7 Independent Contractor Requirements

Contractors of PKI related services are required by contract to enact to their personnel security measures similar to the ones applicable to Notartel / Notartel personnel.
Notartel and its CA services provider Notartel by contract can perform inspections on contractors' sites and can ask to be exhibited the results of internal inspections performed on the contractors by they themselves or by external auditing companies they appoint.

5.3.8 Documentation Supplied to Personnel

All PKI personnel is endowed with operating manuals related to their tasks where such tasks are documented for each involved procedure. Namely:

1. this CPS,
2. the Italian "Manuale Operativo" that summarizes the CP with additional law abiding stipulations,
3. the "Security Plan" ("Piano per la Sicurezza"), limited to a restricted audience, that provides an overall information of all the security related measures,
4. the Security Policies related to the procedures the single employee operates with the distribution of which is based on a "need to know" criteria,
5. specific operational procedures.

In particular a suitable number of copies of the emergency procedures, both on paper and retrievable by electronic means, is distributed among the various PKI related sites.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

All events relevant to the PKI processes systems/applications described in this CPS and in the related CP [24] are logged. Event severity is recorded in the log records that are tagged accordingly, from events related to normal operation up to alarm raising ones.
Additionally, as per DPCM 22/02/2013, the following events, that are automatically recorded by the related systems, make the "Control Log".
When such recording mechanisms are exceptionally not operational, these very events are manually logged for the duration of the exceptional event and subsequently electronically transcribed on the Control Log.

1. Access to the CA secured premises
2. Certificates generation sessions start and end time
3. Information related to certificate generation, suspension and revocation, and to the certificate status publication.

The related time reference SHALL be specified in every "Control Log" recording, and has legal value.

5.4.2 Frequency of Processing Log

Daily log files, in particular the "Control log", are backed up. At least once a month the "Control Log" integrity is verified.

5.4.3 Retention Period for Audit Log

Records in the "Control log" are kept for at least 20 years, as per Notartel internal rules: this time period is longer than the 20 years that are required by the DLgs 82/2005. The Control Log refers to the information specified at section 5.4.1 item 3.
Application procedures necessary to visualize the Control Log records are also kept for 20 years.

5.4.4 Protection of Audit Log

The Control Log can only be modified by the applications that create its records. Where applicable, the intrinsic structure of these records ensures that no change or deletion can be applied after each record is written.
The Control Log and its copies are securely kept in a secure environment and can only be accessed in read mode.
At least once a month the Control Log is inspected for integrity by auditors.

5.4.5 Audit Log Backup Procedures

Reports on the back up procedure completion are inspected to verify if they were successfully executed. In case of unsuccessful execution the subsequent back up session, that will occur after removal of the malfunction, will include also the previously wrongly backed up data.
Also successful back up copies are kept in at least one back up site.

A Control Log is also managed at the Disaster Recovery site by DR service provider, and it is related to its infrastructure.

5.4.6 Audit Collection System (Internal vs. External)

Audit data are originally collected internally to the related systems, to later merge in the Control Log. Where applicable, Control log agents parse logs of the PKI applications and send these records to Control Log system.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

An overall CA Risk Assessment is performed regularly, as required by the QCP [24] and by the European and Italian rules of law, that addresses also the Control Log recording and storage.

5.5 Records Archival

5.5.1 Types of Records Archived

All documentation (either on electronic or paper media) and events are archived, related to:

a. Subject's, LRA's, RAO's registration and certification requests,

b. certificate generation,

c. certificate revocation, suspension and reactivation,

d. access and task activation/deactivation,

e. Control Log.

Are also archived:

f. abnormal events on PKI systems (CA, Directory), such as attempts to illegal access or modification of these systems data, system malfunctions, etc.;

g. back up copies of the publicly accessible Directory.

Are also kept:

- the minutes of the CA key generation/update ceremony,
- the PKI systems configuration history.

Paper documentation may be digitally scanned, in which case the output file may be digitally signed by the officer who performed the scanning, and is made easily available to authorized personnel.
PKI systems approved configuration is kept by the specific Manager.
Should Notartel terminate its operation as a CA, stipulation as in section 5.8 will take effect.

5.5.2 Retention Period for Archive

All certificates related information is kept for at least 20 years, as per Notartel internal rules, that is longer than the law abiding period of 20 years.
No stipulation exists for other archives, apart what is specified in section 5.4.3 for Control Log.

5.5.3 Protection of Archive

5.5.3.1 Who can view the archive

Only authorized personnel can access the CA related archives and solely in read only mode.

5.5.3.2 Integrity protection of the archive – modification

Archives, once downloaded from their systems of origin, are kept on media that, either intrinsically or with procedural measures, cannot be modified or deleted.
The integrity of the CA Archives are verified:

1. soon after the backup copies are performed;
2. at least monthly as far as the Control Log is concerned;
3. as per the programmed Security Audit inspections;

4. at any other time whenever a security audit is required.

5.5.3.3 Integrity protection of the archive - modification

No further stipulation.

5.5.3.4 Protection against archive deterioration

The person in charge of the data security ensures the copies readability by periodically inspecting their status. Should any problem be identified, new copies are created starting from other instances of the data stored in the defective media.

5.5.3.5 Protection against obsolescence

Where applicable, multiple copies of the programs required to read the stored data are kept and are subject to measures similar to those in the previous section 5.5.3.4 suitable to ensure their readability.

5.5.4 Archive Backup Procedures

On a daily basis backup copies are produced of new data, applications, Control Log and of every new file necessary to completely restore the CA management critical systems.
For these systems the backup copies generation is remotely managed and controlled by means of a central system in order to:

- Minimize the need for human intervention and access to system rooms;
- Simplify the backup procedures scheduling and their auditing;
- Enhance the backup operations reliability.

The archived data will be available at the main CA site and their copies at the off site storage backup location, in secured closets.

5.5.4.1 Electronic Information Archive

Data are saved daily. These data are periodically consolidated and saved.
Archives are stored in a safe way at the CA main site. Data related to the Disaster Recovery site are saved and archived also at the Disaster Recovery site by the Disaster Recovery service provider.

5.5.4.2 Paper Information Archive

Paper information is securely stored at the CA site.
After an initial period, depending on the relevant procedures, it may be securely and safely kept at a back up site.

5.5.5 Requirements for Time-Stamping of Records

All audit log and archive records include an indication of time and day that is reliably acquired when they are recorded, based on the trusted source of time the CA makes use of.

This source of time is based on a GPS signal and, as a backup, on a ntp signal received from the Italian Istituto Elettrotecnico Nazionale (IEN) "Galileo Ferraris", the official time provider for Italy. The time receiver is certified by the IEN, the acquired time is then securely broadcast to Notartel systems thus ensuring that all these systems benefit from the same reliable, and therefore common, time.
Where necessary, a Time Stamp Token is issued to the above records/logs.

5.5.6 Archive Collection System (Internal or External).

Archived data are only handled within the related system, until they are copied for back up reasons.

5.5.7 Procedures to Obtain and Verify Archive Information

Confidential documentation is handled as per QCP [24].
Any person may request in writing to access his/her own relevant personal data. Upon positive validation of the request the requester is granted secure access to the relevant data.
Records related to CA systems with restricted access may be only inspected by operators in charge of the specific system and by specifically appointed Auditors.

5.6 CA Key Changeover

When the CA self-signed certificate is approaching its validity end date, in particular when the current CA certificate "notAfter" value is at least just beyond the highest "notAfter" value among the issued subscription certificates4, an additional new instance of the CA is generated and a new key ceremony is carried out with the generation at least of a new key pair and of a new self-signed certificate. The latter certificate is sent to the AGID along a secure channel agreed with the AGID for inclusion in the Public List of Certifiers.
This new CA instance will thenceforth issue and manage the new subscription certificates, while the previous CA instance will only issue CRLs until all certificates issued with that key pair are expired. Once the last certificate has expired this CA instance is withdrawn from operation.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

NOTARTEL has in operation an incident managing plan, which includes also a Disaster Recovery plan, to deal with incidents and disasters including:

1. CA system unrecoverable malfunctions;
2. Unrecoverable malfunctions of Notartel main site network connection to the internet;
3. CA key compromise;
4. Disaster affecting the central and/or backup site CA systems and facilities.

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

If the data and/or the media they are stored on at Notartel main site become unreadable, they SHALL be restored from their security copies previously created:

1. periodically, with an RPO5 and consistently with an RTO6 suitable to prevent data loss;
2. with a mirroring function.

If systems are unusable, they will be hot-swapped with other systems in the same cluster. Where necessary the Disaster Recovery site will be activated.
Notartel has in place agreements with different providers of service communication to the Internet, therefore, even in case of malfunction of one network, the redundant connection system will ensure a continuous service.

[4] Since the subscription certificates duration is three years, this occurs when the current date is just before the "notAfter" value in the self-signed CA certificate minus three years.

[5] **Recovery point objective** (RPO): a point in time to which data must be restored in order to be acceptable to the processes supported by that data.

[6] **Recovery time objective** (RTO): the time within which a business process must be recovered to avoid unacceptable break in continuity.

5.7.3 Entity (NOTARTEL) Private Key Compromise Procedures

5.7.3.1 NOTARTEL CA Certificates Signing Key Device Failure

If the subscription certificates signing device of Notartel CA fails, duly appointed officers, at least in dual control under the supervision of the Certificate Issuance Manager, will reestablish from its security copy and activate the private key that was originally kept inside the defective signing device. Depending on whether the original HSM is still operational this key re-instating will be performed on such HSM or on a new one that Notartel has in stock.

5.7.3.2 NOTARTEL CA Certificates Signing Key Compromise

Should the CA signing key used to issue the Subjects' subscription certificates be compromised, its revocation as per DPCM in force will be performed. A new NOTARTEL CA key pair creation will be performed.

Notartel SHALL inform all Subjects of this compromise, indicating that certificates and revocation status information signed with this CA key may no longer be absolutely trusted, even if their indicated issuance date is before the CA key compromise time. Therefore a signature can be trusted only if recipients have additional methods, like a TST or a PEC message, to prove that the time of this digital signature issuance was prior than the known CA key compromise time.

5.7.4 Disaster Recovery Capabilities After a Disaster

Notartel has in force a Disaster Recovery Plan that provides for activating a Disaster Recovery site, when necessary, and that provides for the following management phases.

1. Emergency – the last issued CRL is kept accessible to relying parties; new CRLs and certificates issuance may be issued with soma delay, if events require operations to be started up at the back up site, but this will be given a high priority.

   The above may not apply in cases of extreme severity and width catastrophes, affecting all Notartel sites (main site, backup site, disaster recovery site), in which case specific Operational Procedure become effective.
2. Transition period management – functions will run normally at the main or in a back up site; in the latter case activities to bring the main site back to operation are initiated;
3. Resume – normal operations are resumed in the original site, or in an alternative but definitive one.

In order to implement such plan, a Disaster Recovery site is fully equipped with mirror machinery, information, data and software.

5.8 CA Termination

In addition to stipulations as of the QCP [24], provisions in Dlgs 82/2005 will be implemented that require to:

1. notify the AGID at least 60 days in advance;
2. notify without any delay all CA certificate owners;
3. communicate, along with the above notifications, whether the documentation required by the law to be kept is taken over by another CA, in which case this CA will be specified, or if it will be annulled, in which latter case all issued certificates will be revoked at operations cessation time.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 NOTARTEL CAs Key Pair Generation

Notartel CAs key pair generation is performed at least in dual control by authorized officers under the Certificate Issuance Manager's supervision.

Each HSM is initialized and its key pair generation function is activated by the authorized operators as per the HSM procedures assessed as compliant with the required certifcation.

A self signed ISO 9594-8 [2] compliant certificate is issued for the newly generated key pair, that is both published in the certificate repository and sent to the AGID on an agreed secure channel. Notartel CA SHALL then issue certificates for the AGID public keys, and publish them in its Directory. The AGID in turn creates an updated Public List of Certifiers and securely delivers it to Notartel CA that SHALL publish it on its CA web site.

6.1.1.2 Subjects

The subject triggers his/her own secret codes into creating the subjects' key pairs. Please refer to section 3.2.1 and related subsections.

6.1.1.3 Cross certified CAs

Not applicable

6.1.2 Private Key Delivery to Subscriber

Not applicable (please refer to section 3.2.1.1).

6.1.3 Public Key Delivery to Certificate Issuer

Please refer to section 3.2.1 and related subsections.

6.1.4 CA Public Key Delivery to Relying Parties

Section 4.9.6 exhaustively explains the signature verification process that also addresses how to securely retrieve the CA self signed certificate containing the CA Public key.
In addition to fetching the AGID Public List of Certifiers, if the Relying Party's CA is listed in it, this Public List can be accessed from the Relying Party's CA web site, although with a slightly lower reliability given the possibility of various types of attacks.

6.1.5 Key Sizes

The RSA keys generated in abidance by Notartel CA comply with the Italian rules of law in force.
At the moment this CPS is drafted:

1. Subjects' subscription keys length is at least 2048 bit.

2. CA keys length is at least 4096 bit.

6.1.6 Public Key Parameters Generation and Quality Checking

The public key parameters quality is ensured by the certification FIPS140-2 level 3 or ISO/IEC 15408 EAL4 of the adopted QSCD and HSM.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

6.1.7.1 NOTARTEL CAs keys usage

The sole keyUsage field bits in the self-issued ISO/IEC 9594-8 [2] CA certificates set to "on" are: **keyCertSign + cRLSign**.

6.1.7.2 Subjects keys usage

The sole keyUsage field bit in the issued ISO/IEC 9594-8 [2] subscription certificates set "on" is **nonRepudiation7**.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

CA and subjects key pairs are generated and securely kept inside the cryptographic devices (QSCD or HSM) that will use them to create signatures. Physical and organizational controls are implemented, consistently with the device type, to prevent the private key from being disclosed. Signing can only be performed inside the device.
Subjects are responsible to securely keep their own cryptographic devices and the relevant activation codes.
If Notartel CA cryptographic devices are disconnected, they require specific activation data and devices to be operated in order to newly become operational.

6.2.1 Cryptographic Module Standards and Controls

CA HSMs and subjects QSCDs are attested as complying with FIPS 140-2 Level 3 security criteria, or with ISO/IEC 15408 at least EAL 4. Security criteria internationally acknowledged as equivalent can also be used, provided they are accepted by the OCSI (the Italian Information Security Certification Organism).

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

The Storage Master keys that wrap the CA private key can be exported from the HSM in multiple parts, according to a Secret sharing scheme that requires the usage of "n out of m" parts, each one under control by a specifically appointed officer, to rebuild the private key.

[7] With ISO/IEC 9594-8:2005 edition (incorporating Draft Technical Corrigendum 6 to 2001 edition) the keyword "nonRepudiation" has been substituted with "contentCommitment" with the following note: "*Note that it is not incorrect to refer to this keyUsage bit using the identifier nonRepudiation. However, the use of this identifier has been deprecated*".

6.2.3 Private Key Escrow

Not applicable. Refer to section 4.12.

6.2.4 Private Key Backup

Only the CA private keys are backed up, under secure procedures consistently with what is specified in section 6.2.2.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Subjects' subscription keys are not transferred into their QSCD, since they are generated directly inside them.
CA private keys are backed up from the HSM and restored back under secure procedures consistently with what is specified in section 6.2.2.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

Subjects activate their private keys by means of the delivered PIN, as specified in sections 3.2.1.1. After the first activation subjects have to change the initial PIN with a new secret one.
When an excessive number of erroneous activation data insertion occurs, the access to the key automatically deactivates. It can only be reactivated by using the PUK delivered to the subject along with the PIN.

6.2.9 Method of Deactivating Private Key

QSCD private keys are deactivated by logging-off the signature application or by removing the device from the reader. If the private key has been in an idle log-in status for more than a fixed time or more than a fixed number of issued signatures, whichever comes first, it deactivates automatically, except when the private key is used in automated signing procedure, where specific application deactivation criteria are used.
NOTARTEL CA HSM private keys are deactivated by stopping HSM services directly on the console of the HSM by the Crypto Hardware Operator with the Security Officer Keys.

6.2.10 Method of Destroying Private Key

Private keys cannot be zeroised without the PIN, therefore the only way to destroy them is to physically destroy the SSCD itself or to access to private keys by the PIN and deleting them. At certificate expiration the subject may either destroy personally his/her QSCDor turn it back to the LRA that will destroy it at the subject's presence.

HSM private keys can be zeroised following a specific, manufacturer provided, procedure.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All public keys are archived, since all certificates (CAs', subjects', cross certified CAs') requests are kept by Notartel CA and backed up in the Disaster Recovery site.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The subjects' private and public keys life span is of 36 months.
Notartel CA certificate signing key pair life span is of 20 years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data characteristics are defined in the Security Policy document.

6.4.2 Activation Data Protection

No additional stipulation as to what is specified in the related CP [24] regarding Notartel CA.
Subjects are securely delivered the private key activation codes (PIN and PUK) as specified in sections
Subjects SHALL change their PIN after its first usage and whenever they want and SHALL keep it securely, separated from the private key (DPCM 22/02/2013 art.8(5) letter b).

6.4.3 Other Aspects of Activation Data

In case of more than 3 erroneous PIN input the private key private key is deactivated.

Notartel provided PUK is required to unlock the private key.

6.5 Computer Security Controls

A copy of all PKI related systems approved configurations is kept by the relevant Manager as an audit trail, that is periodically matched against the ones actually in use.

6.5.1 Specific Computer Security Technical Requirements

The following technical controls are implemented:

- Physical access controls to CA services are described in section 5.1.2;
- Passwords are enforced for all CA roles and PKI client applications, in compliance with the related Security Policies;
- Security related events are audited;
- On all PKI relevant systems and workstations, suitable anti-malware applications are installed and kept updated with due frequency.

6.5.2 Computer Security Rating

As required by ETSI EN 319 411 – 1 and Commission Implementing Decision (Eu) 2016/650, Notartel PKI devices are conformant at least with security criteria equivalent to the following FIPS or ISO/IEC 15408 levels. Security criteria internationally acknowledged as equivalent can also be accepted.

1. HSM for CA Signature creation devices (certified per FIPS 140-2 Level 3 – ISO 15408 EAL4 or declared as conformant by Notartel CA in compliance with OCSI)
2. HSM for subject signature (certified per ISO 15408 EAL4)

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

Security audit is implemented also using tools that are kept secure to prevent tampering.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Notartel PKI networks are dedicated subnets inside Notartel general network. They are protected with dedicated firewalls.
Notartel PKI systems are installed on computers, hardened to enable only the strictly necessary functions.
Communications are implemented along secured channels between:

- Notartel PKI site and Notartel backup site;
- the LRA computers and the subjects' systems on the one side and the RA on the other side; these secure channels are implemented by adoption of SSL.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Subscription and CA certificates, and CRLs comply with ISO/IEC 9594-8 [2].
Subscription certificate profiles comply with RFC 5280 [13], RFC 3739 [16], ETSI EN 319 412-2 [18] and Italian rules of law.
Certificate fields are populated as per the base certificate structure (ISO 9594-8 [2]).
Note: provisions specified in this chapter abide by the currently in force Italian rules of law. They will be adapted to new Italian rules of law when they come in force.

7.1.1 Certificate Profile for root CA

Certificate:

Data:
Version: 3
Serial Number: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX (20 bytes)

Signature Algorithm: sha256WithRSAEncryption

Issuer:
C = IT
O = Notartel S.p.A.
organizationIdentifier = VATIT-05364151000
OU = Qualified Trust Service Provider
CN = Notartel Qualified Electronic Signature CA 2021

Subject:
C = IT
O = Notartel S.p.A.
organizationIdentifier = VATIT-05364151000
OU = Qualified Trust Service Provider
CN = Notartel Qualified Electronic Signature CA 2021

Validity
Not Before: Date key cerimony
Not After : Date key cerimony + 20 Anni

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)

X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0

X509v3 Certificate Policies:
cps (1.3.6.1.5.5.7.2.1) [
IA5_STRING - https://ca.notartel.it/documentazione/cps_ca_notartel.pdf
]

X509v3 Key Usage: critical
Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:
XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX (20 bytes)

7.1.2 Certificate Profile for root TSA

Certificate:

Data:
Version: 3
Serial Number: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX (20 bytes)

Signature Algorithm: sha256WithRSAEncryption

Issuer:
C = IT
O = Notartel S.p.A.
organizationIdentifier = VATIT-05364151000
OU = Qualified Time Stamping Authority
CN = Notartel Qualified TimeStamp CA 2021

Subject:
C = IT
O = Notartel S.p.A.
organizationIdentifier = VATIT-05364151000
OU = Qualified Time Stamping Authority
CN = Notartel Qualified TimeStamp CA 2021

Validity
Not Before: Date key cerimony
Not After : Date key cerimony + 20 Anni

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)

X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0

X509v3 Certificate Policies:
cps (1.3.6.1.5.5.7.2.1) [
IA5_STRING - https://ca.notartel.it/documentazione/cps_tsa_notartel.pdf
]

X509v3 Key Usage: critical
Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:
XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX (20 bytes)

7.1.3 Certificate Profile for remote signature after AGID Determination 147/2019 (May 2020)

Certificate:
Data:
Version: 3
Serial Number: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX (20 bytes)

Signature Algorithm: sha256WithRSAEncryption

Issuer:
C = IT
O = Notartel S.p.A.
organizationIdentifier = VATIT-05364151000
OU = Qualified Trust Service Provider
CN = Notartel Qualified Electronic Signature CA 2021

Subject:
C = IT
SN = {cognome}
GN = {nome}
serialNumber = {tipodocumento}{nazionedocumento}-{numerodocumento} (For all persons in possession of a Tax Code, it will be TINIT-{codicefiscale})
CN = {nome} {cognome}
dnQualifier = PFR{pk-cms} (Composition of the acronym PFR "persona fisica remota" + identificativo univoco della richiesta all'interno del CMS zeropadded a 8 cifre es. PFR00000154)
#Solo per certificati di ruolo
T = {titolo} (Opzionale, qualifica aziendale)
organizationIdentifier = VAT{nazioneazienda}-{partitaiva} (For all Italian companies in possession of a VAT number, it will be VATIT-{partitaiva})
O = {nomeazienda} (Es. "Bit4id S.r.l.")

Validity
Not Before: Date of first issue
Not After : Date of first issue + 3 years

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)

X509v3 extensions:
Authority Information Access:
CA Issuers - URI:http://ca.notartel.it/pki/certificates/ca_notartel_2021.cer
OCSP - URI:https://ocsp.notartel.it

X509v3 Subject Key Identifier:
XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

X509v3 Authority Key Identifier:
keyid:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

X509v3 Basic Constraints: critical
CA:FALSE

X509v3 Certificate Policies:
agIDcert (1.3.76.16.6)
qcp-natural-qscd (0.4.0.194112.1.2)
cps (1.3.6.1.5.5.7.2.1) [
IA5_STRING - https://ca.notartel.it/documentazione/cps_ca_notartel.pdf
]
notartel-pfr (1.3.6.1.4.1.41870.10.2) (definire OID Notartel)

X509v3 CRL Distribution Points:
Full Name:
URI:http://crl.notartel.it/pki/crls/ca_notartel_2021.crl

X509v3 Key Usage: critical
Non Repudiation

qcStatements:
QcCompliance (0.4.0.1862.1.1)
QcRetentionPeriod (0.4.0.1862.1.3) [
INTEGER - 20
]
QcSSCD (0.4.0.1862.1.4)
QcEuPDS (0.4.0.1862.1.5) [
SEQUENCE[
IA5_STRING - https://ca.notartel.it/documentazione/pds_notartel_pfr_it.pdf
PRINTABLE_STRING - it
]
SEQUENCE[
IA5_STRING - https://ca.notartel.it/pki/documentazione/pds_notartel_pfr_en.pdf

PRINTABLE_STRING - en
]
]

7.1.4 Certificate Profile for One Shot remote signature.

Certificate:
Data:
Version: 3 (0x2)
Serial Number: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX (20 bytes)
Signature Algorithm: sha256WithRSAEncryption
Issuer:
C = IT
O = Notartel S.p.A
organizationIdentifier = VATIT-05364151000
OU = Qualified Trust Service Provider
CN = Notartel Qualified Electronic Signature CA 2021
Subject:
C = IT
SN = {cognome}
GN = {nome}
serialNumber = {tipodocumento}{nazionedocumento}-{numerodocumento} (For all persons in possession of a Tax Code, it will be TINIT-{codicefiscale})
CN = {nome} {cognome}
dnQualifier = {pk-cms}

Validity
Not Before: Date of first issue
Not After : Date of first issue + 1 year

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)

X509v3 extensions:
Authority Information Access:
CA Issuers - URI:http://ca.notartel.it/pki/certificates/ca_notartel_2021.cer
OCSP - URI:http://ocsp.notartel.it

X509v3 Subject Key Identifier:
XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

X509v3 Authority Key Identifier:
keyid:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

X509v3 Basic Constraints: critical
CA:FALSE

X509v3 Certificate Policies:
Policy: 1.3.76.16.6
User Notice:
Explicit Text: agIDcert
Policy: 0.4.0.194112.1.2
Policy: Policy Qualifier CPS
CPS: https://ca.notartel.it/documentazione/cps_ca_notartel.pdf
Policy: 1.3.6.1.4.1.41870.10.2
Policy: 1.3.6.1.4.1.41870.10.3
User Notice:
Explicit Text: Il presente certificato ha il solo scopo di firmare digitalmente l'atto con identificativo {id-atto} - This certificate has the sole purpose of digitally signing the act with id {id-atto}

X509v3 CRL Distribution Points:
Full Name:
URI:http://crl.notartel.it/pki/crls/ca_notartel_2021.crl

X509v3 Key Usage: critical
Digital Signature, Non Repudiation

qcStatements:
QcCompliance (0.4.0.1862.1.1)
QcRetentionPeriod (0.4.0.1862.1.3) [
INTEGER - 20
]
QcSSCD (0.4.0.1862.1.4)
QcEuPDS (0.4.0.1862.1.5) [
SEQUENCE[
IA5_STRING - https://ca.notartel.it/documentazione/pds_notartel_pfr_it.pdf
PRINTABLE_STRING - it
]
SEQUENCE[
IA5_STRING - https://ca.notartel.it/pki/documentazione/pds_notartel_pfr_en.pdf
PRINTABLE_STRING - en
]
]

7.1.5 Version Number(s)

The certificate “version” field contains value “2”, indicating an ISO/IEC 9594-8 version 3 certificate.

7.1.6 Certificate Extensions

The following extensions are required.

a) keyUsage (OID: 2.5.29.15), with contentCommitment (formerly “nonRepudiation”) bit (1) on; this extension is CRITICAL;

b) certificatePolicies (OID: 2.5.29.32), specifying the OID of the Qualified Certificate Policy8 and the URIs pointing to the Manuale Operativo [6] and to this CPS in abidance of which the certificate was issued; this extension is NOT critical;
c) CRLDistributionPoints (OID: 2.5.29.31), specifying the URL pointing to the CRL where revocation (and suspension) information related to the certificate at issue SHALL be published when necessary; HTTP or LDAP schema is used; where more than one URL is specified all these values SHALL point to a set of information consistent with the provisions of the latest published CRL; this extension is NOT critical;
d) authorityKeyIdentifier (OID: 2.5.29.35); this extension is NOT critical;
e) subjectKeyIdentifier (OID: 2.5.29.14); this extension is NOT critical;
f) qcStatements with the following values specified in ETSI TS 101 862:
    1) id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1);
    2) id-etsi-qcs-QcRetentionPeriod (OID: 0.4.0. 1862.1.3); the value is greater or equal to «20»;
    3) id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4).
    4) id-etsi-qcs-QcPDS (OID: 0.4.0.1862.1.5): this extension contains link to Disclosure Statement
    5) optional id-etsi-qcs-QcType of type id-etsi-qct-esign (OID: 0.4.0.1862.1.6.1): indicates electronic signature of natural person.

This extension is NOT critical.

g) subjectAlternativeName (OID: 2.5.29.17):
    1) rfc822Name: where present it specifies the email address of the subject

Additionally, the following extensions MAY be used:

h) optional SubjectDirectoryAttributes (OID: 2.5.29.9); this extension SHALL not contain the same information as in the “issuer” and “subject” fields, but MAY contain other information; where the dateOfBirth attribute (OID: 1.3.6.1.5.5.7.9.1) is specified, it is coded in GeneralizedTime format; this extension is NOT critical.
i) authorityInfoAccess (OID: 1.3.6.1.5.5.7.1.1); this extension, where used to access an OCSP Responder, SHALL specify in the accessDescription field the ways to access the OCSP service and SHALL indicate:
    1) accessMethod, specifying id-ad-ocsp (OID: 1.3.6.1.5.5.7.48.1);
    2) accessLocation, specifying the URI that points to Notartel CA OCSP Responder. This URI provides an absolute address to the OCSP Responder. Where more access Description are specified indicating the id-ad-ocsp in the

[8] ETSI TS 1021 456 has been abided by.

accessMethod attribute, these provisions specify alternate paths to retrive, via OSCP the status of the certificate at issue.

3) CAIssuer, specifying the ldap URL to the root Certificate.

This extension is NOT critical.

7.1.7 Algorithm Object Identifiers

Algorithms used for signature and for hashing are indicated here

Algorithm	OID
rsaEncryption	1.2.840.113549.1.1.1
SHA-256	2.16.840.1.101.3.4.2.1
sha256WithRSAEncryption	1.2.840.113549.1.1.11

7.1.8 Name Forms

For Type of names see 3.1.1.
The Subject Name is an X.500 distinguished name.

7.1.9 Name Constraints

No stipulation.

7.1.10 Certificate Policy Object Identifier

This CPS refers to the QCP-n-qscd certificate policy for European Union (EU) qualified certificates issued to natural persons with private key related to the certified public key in a Qualified electronic Signature/seal Creation Device (QSCD), as specified in ETSI EN 319 411 – 2 [25] identified with the following OID

- Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2) (ETSI EN 319 411 – 2 [25] – QCP public + QSCD)

7.1.11 Usage of Policy Constraints Extension

No stipulation.

7.1.12 Policy Qualifiers Syntax and Semantics

This attribute specifies the address where this CPS can be found, as per RFC 5280 [13].
The CPSuri qualifier of the extension “certificatePolicies” contains pointers in the form of URIs to this Certification Practice Statement (CPS) and to the Manuale Operativo [6].

7.1.13 Processing Semantics for the Critical Certificate Policies Extension

No stipulation: Agid decision, currently in force, requires that the **certificatePolicy** extension is not critical (see Section 7.1.2).

7.2 CRL Profile

7.2.1 Version Number(s)

The CRL version number field contains the integer “1”, indicating a ISO 9594-8 version 2 Certificate Revocation List.

7.2.2 CRL and CRL Entry Extensions

The CRL is conformant with RFC 5280 [13].

7.2.2.1 CRL Extensions

As per Agid decision no Delta CRLs is supported, which excludes extensions related to Delta CRLs.

- Authority Key Identifier: Hexadecimal representing 160bit SHA-1 of the CA public key
- CRL Number: implemented as per RFC 5280, § 5.2.3, as a monotonically increasing sequence number per CRL Type (e.g. for each partitioned CRL)
- CRL contains the extension ExpiredCertsOnCRL (OID 2.5.29.60), in compliance with Agid determniation 147/2019

7.2.2.2 CRL Entry Extensions

The following CRL Entry extensions are implemented.

1. Serial number: serial number of end entity certificate;
2. Reason Code: refer to section 4.9.1.4;
3. Invalidity Date: date of revocation

7.3 OCSP Profile

OCSP profile is compliant with IETF RFC 6960 [23].

7.3.1 Version Number(s)

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

7.4 CRL Profile TSU Certificate Profile

TSU and TSA CA certificates, and CRLs comply with ISO/IEC 9594-8 [2].

TSU certificate profiles comply with RFC 5280 [13], RFC 3739 [16], ETSI EN 319 422 and Italian rules of law.

Certificate fields are populated as per the base certificate structure (ISO 9594-8 [2]).

Note: provisions specified in this chapter abide by the currently in force Europaean and Italian rules of law. They will be adapted to new European or Italian rules of law when they come in force.

Certificate:

Data:

Version: 3

Serial Number: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX (20 bytes)

Signature Algorithm: sha256WithRSAEncryption

Issuer:

C = IT

O = Notartel S.p.A.

organizationIdentifier = VATIT-05364151000

OU = Qualified Time Stamping Authority

CN = Notartel Qualified TimeStamp CA 2021

Subject:

C = IT

O = Notartel S.p.A.

organizationIdentifier = VATIT-05364151000

OU = Qualified Time Stamping Authority

CN = Notartel Qualified Time-Stamping Authority TSU 01

Validity

Not Before: Data della prima emissione

Not After : Data della prima emissione + 10 Anni

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

X509v3 extensions:

Authority Information Access:

CA Issuers - URI:http://ca.notartel.it/pki/certificates/tsa_notartel_2021.cer

OCSP - URI:https://ocsp.notartel.it

X509v3 Subject Key Identifier:

XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

X509v3 Authority Key Identifier:

keyid:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

X509v3 Certificate Policies:

qcp-legal-qscd (0.4.0.194112.1.3)

cps (1.3.6.1.5.5.7.2.1) [

IA5_STRING - https://ca.notartel.it/documentazione/cps_tsa_notartel.pdf

]

notartel-tsu (1.3.6.1.4.1.41870.12.1)

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.notartel.it/pki/crls/tsa2021.crl

X509v3 Key Usage: critical

Digital Signature

X509v3 Extended Key Usage: critical

Time Stamping

qcStatements:

QcCompliance (0.4.0.1862.1.1)

QcRetentionPeriod (0.4.0.1862.1.3) [

INTEGER - 20

]

QcSSCD (0.4.0.1862.1.4)

QcEuPDS (0.4.0.1862.1.5) [

SEQUENCE[

IA5_STRING - https://ca.notartel.it/documentazione/tsa_notartel_disclosure_statement_it.pdf

PRINTABLE_STRING - it

]

SEQUENCE[

IA5_STRING - https://ca.notartel.it/documentazione/tsa_notartel_disclosure_statement_en.pdf

PRINTABLE_STRING - en

]

]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

NOTARTEL internal Audit personnel regularly carries out Audit on each and all security related PKI procedures. An external Auditing Organization yearly perform audit revision.

All personnel that performs tasks related to CA and/or LRA related activities is audited.

The purpose is to ascertain if the following requirements are met:

1. actual compliance to procedures by personnel,
2. procedures efficaciousness and effectiveness,
3. actual possibility for the personnel to comply with the procedures.

The overall NOTARTEL security can be reviewed depending on these audit inspections outcomes.

8.1 Frequency and Circumstances of Assessment

In section 8.4 the audit frequency is specified.

NOTARTEL Internal Auditors may perform both scheduled and extemporaneous auditing.

Additionally, audit inspections on the Notartel Quality System are performed at regular intervals by an external Auditing Organization

8.2 Identity/Qualifications of Assessor

The Internal Auditing is performed by personnel of the internal NOTARTEL auditor department.

The External Auditing Company is certified to ISO 9001:2000

8.3 Assessor's Relationship to Assessed Entity

The PKI department has no hierarchical relationships with the Internal Auditing Department.

External Auditing is performed by an independent Company

8.4 Topics Covered by Assessment

Audit inspections are basically enacted on the following.

1. Audit log integrity
2. Audit log content
3. Compliance with the procedures set forth in the following sections of this CPS:
   a. 3 – Identification and authentication
   b. 4 - Certificate Life-Cyble Operational Requirements
   c. 5 – Facility, Management, and Operational Controls
   d. 6 – Technical Security Controls
   e. 7 – Certificate, CRL, and OCSP Profiles

f. 9 – Other Business and Legal Matters; this area in particular requires a sound procedural (i.e. legal, financial, insurance, etc.), more than technical, audit skill.

4. Cryptographic devices inventory correctness
5. Correctness of backup systems and devices inventory
6. Backup systems and devices operability
7. Matching the actual configuration of HW, SW, PKI, firewall, IDS systems, with their planned configuration as kept by the relevant appointed Manager.

Audit inspections addressing ICT topics are mostly based on audit log perusal; in some cases they may do penetration tests to ascertain that the stated security measures are in force and effective.

8.5 Actions Taken as a Result of Deficiency

Actions to be taken will be decided by the single manager mentioned in section 8.6, or even by Notartel Top Management, depending on the findings.

Deliberate security violation will be prosecuted as per the rules of law currently in force.

Where the violation may have exposed at risk the CA private key, provisions in section 5.7.3.2 apply.

8.6 Communications of Results

Audit outcomes documents shall be reported to all the interested managers in charge of functions related to: security, CA functions, RA functions, certificate status and other information publishing, infrastructures, and, if the audit is performed by an external Company, internal auditing.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The cost of certificatesis established at service activation time.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

The general provisions in Regulation EU 910/2014 art. 11 and in Dlgs 82/2005, art. 30, on Liability apply.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

As per AGID/DET/48, being Notartel a Public Administration, Notartel is not required to subscribe a specific insurance policy addressing the CA activity risks.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All Business related information, relevant to the CA and/or Subjects and LRAs, are kept confidential, as well as all personal data in abidance with the GDPR.

9.3.2 Information Not Within the Scope of Confidential Information

Information in Certificates, CRL, OCSP Responses, where applicable, and all information that is published in Notartel CA public web site, is not to be considered confidential.

9.3.3 Responsibility to Protect Confidential Information

All NOTARTEL department is responsible to protect the confidentiality of the information it manages classified as confidential at NOTARTEL and Notartel level.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

All information that relates to personal data is confidential and is protected as per GDPR, as per the applicable rules of law in force. Additional specific measures are in force in conformity of the GDPR detailed requirements.
Confidentiality is protected for all registration related information, as well as all information exchanged among the CA branch offices and the CA and any other information users will classify as confidential.

9.4.2 Information Treated as Private

All information related to Notartel CA security as well to the users' QSCD use and activation is required to be treated as private.

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

Users to whom Notartel related information are entrusted, that have been indicated as private, have specific obligations regarding ensuring their secrecy.

9.4.5 Notice and Consent to Use Private Information

When personal and however private information is collected from natural of legal persons, they are notified in abidance with GDPR, asking for their consent to process it too.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No stipulation in addition to what is law conformant.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

Notartel owns all the Intellectual Property rights regarding the documents developed for the CA activity.
All HW and SW products, Notartel provides Subjects, its personnel and its subcontractors with, in order to make them use and/or implement PKI related functions, is covered by Intellectual Property rights.

9.6 Representations and Warranties

All information directly submitted to the CA by the Subjects is provided under the submitters' responsibility of authenticity.
Apart from this, Notartel CA warrants that all information it is provided with, is painstakingly replicated into the information provided to the public, such as certificates and revocation information.

9.6.1 CA Representations and Warranties

No additional stipulation as to the previous subsection.

9.6.2 RA Representations and Warranties

No additional stipulation as to the previous subsection.

9.6.3 Subscriber Representations and Warranties

9.6.4 Relying Party Representations and Warranties

No additional stipulation as to the previous subsection.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Certificates issued by Notartel CA can only be used to ascertain the authenticity of origin and integrity of content of the documents a signature refers to, supported by such certificate.
Certificate revocation information can only be used to assess the correspondent certificate validity, effective on the revocation publication time.

9.8 Limitations of Liability

Notartel CA can only be held liable consistently with what is stated in art. 11 of the EU Regulation 910/2014 and in Dlgs 82/2005, art. 30. In particular it cannot be held liable in all cases when it has not acted negligently, or when the damage depends on the certificate being used beyond its limitations of use, or when the certificate owner has not complied with what is specified in this CPS and in the relevant contract, or when any party has not complied with this CSP stipulations.

9.9 Indemnities

No stipulation.

9.10 Communications of Results

9.11 Term

No stipulation.

9.12 Termination

No stipulation.

9.12.1 Effect of Termination and Survival

No stipulation.

9.13 Individual Notices and Communications with Participants

Any change in the agreements binding the CA to its possible certification service providers, as well as the CA itself to the Subjects, shall be submitted to the counterpart with the timing and terms indicated in the specific agreements

9.14 Amendments

9.14.1 Procedure for Amendment

Amendments to this CPS may be applied whenever changes to the applicable Italian rules of law, to the related standards, to statutory requirements occur that make the current text obsolete, in parts or as a whole.
Notartel CA will review this CPS consistently with the new rules and legal or technical requirements within a time period, since their coming to force, that depend on the specific change.

9.14.2 Notification Mechanism and Period

Notartel CA SHALL personally notify in writing, that includes digitally signed documents, Subjects of the next new CPS publication in advance.
Relying Parties will be notified by means of publication on Notartel web site of a suitable communication, that will occur in advance before the new CPS publication

9.14.3 Circumstances Under Which OID Must be Changed

No stipulation.

9.15 Dispute Resolution Provisions

This service is offered to Subjects as regulated by the Italian law and the Manuale Operativo [6]. To resolve each controversy relative to its validity, interpretation, execution and resolution, the “Foro di Roma” (Tribunal of Rome) will be competent.

9.16 Governing Law

The Italian rules of law in force at the moment of a possible dispute will govern its settling.

9.17 Compliance with Applicable Law

The Italian rules of law govern this CSP.

9.18 Miscellaneous Provisions

No stipulation: these issues will be handled in the single certification service contract.

9.19 Entire Agreement

No stipulation.

9.19.1 Assignment

No stipulation.

9.19.2 Severability

Should, due to changes in the rules of law, or to a Court sentence, or to any other juridical instrument, one or more stipulation of the present Certification Practice Statement become no more law-abiding, the other stipulations applicability will not be automatically affected.
During the time period during which this CSP is reviewed, the present CPS will therefore be interpreted as if the inapplicable section(s) do(es) not exist.

9.19.3 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.20 Other Provisions

No stipulation.

Approved by the GM of Notartel S.p.A. – S.B.

Rome, 18/07/2024