AGID

Agency for Digital Italy

Qualification and accreditation area

AgID - AGENCY FOR DIGITAL ITALY

OPERATIVE MANUAL FOR THE "AgID CA" SERVICE

CERTIFICATION PRACTICE STATEMENT

Version 8.0

Drawn up by:	Qualification and accreditation area
Approved by:	Gualtiero Asunis

DISTRIBUTION: PUBLIC

Contents

Change History

Description of changes	Version	Date
First issue	1.0	18/10/2017
Par. 4.4.1 – Reference to WHOIS deleted (no longer used) Par. 8.4 – Duration of website certificates limited to 2 years	2.0	28/02/2018
Par. 2.2.1 – Clarification: AgID CA1 is "technically constrained" Par. 5.3 – Mandatory Certificate Transparency introduced for SSL Server certificates issued after 30 April 2018 Par. 8.4 – CST List extension introduced to the SSL Server certificate	3.0	27/04/2018
Par. 5.1 – Review of the procedure Par. 8.4 – Duration of website certificates limited to 1 year	4.0	17/09/2020
Entire document: references to certificates for websites deleted (SSL Server). Complete restructuring of the document to comply with RFC3647. Reference to Mozilla Root Store Policy added.	5.0	22/06/2021
The whole document: references reintroduced to the certificates for websites (SSL Server) issued by an intermediate CA dedicated to this.	6.0	29/11/2021
Complete review of the document. Incorporation of CA/Browser Forum Baseline Requirements for S/MIME certificates	7.0	09/01/2024
Par: 4.10 and par.7: Correction of typos	8.0	24/07/2024

1 Introduction

1.1 Purpose of the document

By Decree No. 177 of 1 December 2009, the CNIPA was reorganised into a new body, called DigitPA, which has taken over the CNIPA's certification activities.

With D.P.R. No. 68 of 11 February 2005 and the Decree of the Minister for Innovation and Technologies of 2 November 2005, containing the "Technical rules for drafting, transmission and validation, including temporary, of certified email", CNIPA (and therefore to DigitPA) is assigned the exclusive task of issuing Certified Email Managers with server certificates automatically recognised by market products.

According to DECREE-LAW No. 83 of 22 June 2012 "Urgent measures for Italy's growth ", art. 19 - Establishment of the Agency for Digital Italy - "the **Agency for Digital Italy is established**, under the supervision of the President of the Council of Ministers or the Minister delegated by him, the Minister of Economy and Finance, the Minister for Public Administration and Simplification, the Minister of Economic Development and the Minister of Education, University and Research".

According to the same Decree-Law, art. 20 "the Agency also carries out (...) the coordination, guidance and regulation functions entrusted to DigitPA under current legislation". The functions of the AgID were subsequently confirmed and supplemented by art. 14 bis of Legislative Decree No. 82 of 7 March 2005 and subsequent amendments; therefore the functions of the certifier previously assigned to DigitPA are attributable and attributed to the AGID.

This **Certification Practice Statement** (CPS), also called the "Operating Manual", defines the procedures applied by the AgID CA for the issuance and management of digital certificates for server systems. In particular, three types of certificates are issued:

- for **electronic signature** (e.g. S/MIME signature of Certified Email Receipts, signature of LDIF files,...)
- for **authentication** to SSL servers (i.e. for SSL client authentication)
- for **SSL Server**, i.e. activation of the SSL/TLS protocol on websites

The first type of certificates (S/MIME) is mainly used by Certified Email Managers for fulfilling the requirements of the Certified Email regulations, as well as by other actors in the Certified Email network (including e.g. AgID itself).

The second type can be used to authenticate a system that acts as a client in the context of an SSL interview in which the authentication of both parties involved is required. In particular, within the Certified Email service, they are used for access to the Certified Email Managers' Index (IGPEC).

The third type is used to activate the SSL/TLS protocol on websites managed by the AgID or in any case on domains that fall under the control of the AgID.

This CPS is structured in accordance with the public specification RFC 3647 [CPF].

Regarding SSL Server certificates, the AgID complies with the current version of the **Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates** published on http://www.cabforum.org. In the event of inconsistency between this document and such Requirements, the Requirements shall take precedence.

Regarding S/MIME certificates (Signature Certificates), the AgID complies with the current version of the **Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates** published on http://www.cabforum.org. In the event of inconsistency between this document and such Requirements, the Requirements shall take precedence.

The hosting and operational management of the AgID certification service is entrusted to the Temporary Grouping of Companies (RTI) awarded the CONSIP CIG 9290583F9D Tender, with the company Fastweb S.p.A. (hereinafter abbreviated to "RTI") as agent.

1.2 Identification of the document

This CPS is identified by the version number shown on the first page.

This CPS is referenced by the following OID (Object Identifier) within the certificates issued, in the CertificatePolicies extension:

1.3.76.16.3.1 – Certification of server public keys

This CPS is published in PDF format on the Certifier's website at the following URL:

http://www.agid.gov.it/cps-ca

1.3 PKI Participants

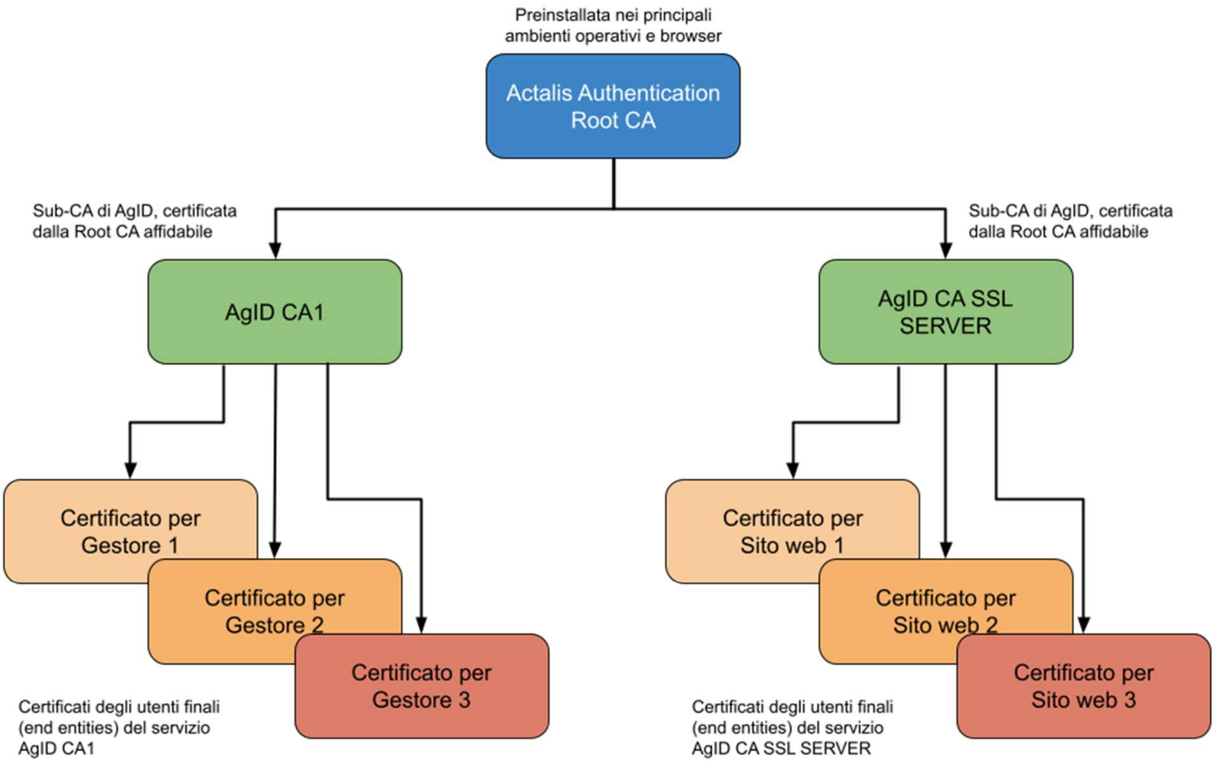
1.3.1 Certification Authority

Since 20/11/2017, a CA infrastructure has been in operation using an AgID certification key called "**AgID CA1**". Since 25/11/2021, a second certification key called "**AgID CA SSL SERVER**" has also been used. These two intermediate CA keys, with which the Subscriber certificates are issued, are in turn certified by the Root CA of Actalis S.p.A., pre-installed in the most popular operating environments and browsers on the market. In this way, without the need for intervention by the end user, it is possible to:

- recognise the reliability of the electronic signatures affixed by the Certified Email Managers;
- gain secure access (authenticated and encrypted) to websites using the HTTPS protocol.

Hereinafter, the term "**AgID CA**" will refer to both CAs where it is not necessary to make a distinction.

The PKI on which the service described in this CPS is based is laid out in the following figure:



Preinstallata nei principali ambienti operativi e browser
Actalis Authentication Root CA
Sub-CA di AgID, certificata dalla Root CA affidabile
Sub-CA di AgID, certificata dalla Root CA affidabile
AgID CA1
AgID CA SSL SERVER
Certificato per Gestore 1
Certificato per Gestore 2
Certificato per Gestore 3
Certificato per Sito web 1
Certificato per Sito web 2
Certificato per Sito web 3
Certificati degli utenti finali (end entities) del servizio AgID CA1
Certificati degli utenti finali (end entities) del servizio AgID CA SSL SERVER

Figure 1: Diagram of the reference PKI

Both issuing CAs, **AgiD CA1** and **AgID CA SSL SERVER**, operate under the responsibility of the **AgID**, whose main identification and contact data are shown below:

Official name	Agency for Digital Italy (AgID)
General Manager	Mario Nobile
Registered office	Via Liszt, 21 – 00144 Rome
Object Identifier	1.3.76.16
Telephone	+39 06 852641
Operational headquarters	Via Liszt, 21 – 00144 Rome
Email Address	protocollo@pec.agid.gov.it
Main website	http://www.agid.gov.it

Below are the identification data for the certificates of the AgID's two issuing CAs:

Data	Value
Subscriber (Subject)	**CN** = AgID CA1 **OU** = Solutions Area for the Public Administration **O** = Agency for Digital Italy **L** = Rome **C** = IT
Issuer	**CN** = Actalis Authentication Root CA **O** = Actalis S.p.A./03358520967 **L** = Milan **C** = IT
Key identifier (Subject Key Identifier)	A5FD85050EC3F1D6654A206CE2DB4D60932B8AA0
Validity period	**FROM**: 21/09/2021 **TO**: 09/22/2030

Data	Value
Subscriber (Subject)	**CN** = AgID CA SSL SERVER **OU** = Solutions Area for the Public Administration **O** = Agency for Digital Italy **L** = Rome **C** = IT
Issuer	**CN** = Actalis Authentication Root CA **O** = Actalis S.p.A./03358520967 **L** = Milan **C** = IT
Key identifier (Subject Key Identifier)	2AB7A610B6863F43B8FDCF4AFA88BF329323CFB4
Validity period	**FROM**: 24/11/2021 **TO**: 09/22/2030

For more details on the Root CA, please refer to the CPS published on the Actalis website (https://www.actalis.it/docu- menti-it/cps_certificati_ssl_server_e_code_signing_it.aspx).

The "AgID CA SSL SERVER" is also a "technically constrained" Certification Authority and as such can only issue certificates for websites under the AgID's control.

For more details on the constraints applied, please refer to paragraph 7.1.5.

1.3.2 Registration Authority (RA)

The tasks of the Registration Authority are carried out by the RTI.

1.3.3 Users (subscribers)

- **Signature** certificates are provided exclusively to accredited Certified E-mail Managers[1] and other actors of the Certified E-mail network, including e.g. the AgID itself;
- **Authentication** certificates are provided exclusively to accredited Certified E-mail Managers and to other actors of the Certified E-mail network, including e.g. the AgID itself (see previous point);
- The **SSL Server** certificates are issued exclusively for domains under the AgID's control.

1.3.4 Relying Parties

The "Relying Parties" (RP) are all persons who rely on the information contained in the certificates issued in accordance with this CPS. For example (non-exhaustive list):

- those who send or receive certified email messages, insofar as they receive "Certified Email Receipts" signed with certificates issued in accordance with this CPS;
- The server operators that accept SSL client authentication based on authentication certificates issued in accordance with this CPS;
- those who access websites on which SSL Server certificates issued in accordance with this CPS are installed;

1.4 Use of certificates

As stated beforehand, this CPS concerns the issuance and management of certificates of the following types:

- Signature certificates (S/MIME);
- Authentication certificates;
- certificates for websites (SSL Server).

Certificates issued under this CPS shall only be used for the purposes stated above (depending on the type of certificate).

1.5 CPS Manager

1.5.1 Organisation responsible for the document

This CPS is reviewed, approved and published by the Agency for Digital Italy – AgID.

The person responsible for this CPS is:

[1] The official list of accredited Certified Email Managers is published on the AgID website at http://www.agid.gov.it/infrastrutture-sicurezza/pec-elenco-gestori

CPS Manager	
Name	Gualtiero
Surname	Asunis
Telephone	+39 06 852641
Email	asunis@agid.gov.it

1.5.2 Contact details

For more information about this CPS or the CA service described here, please send an email to: richiesta-certificati@pec-ic.agid.gov.it.

The CA makes available to all interested parties a certified email mailbox that allows you, at any time, to report to the CA any problems related to certificates already issued (and already in use), such as to justify a revocation which may also be immediate:

alert@pec-ic.agid.gov.it

Examples of issues that can be reported through this channel:

- private key compromised
- unlawful use of the certificate

The reporting person must provide at least the following information, or the report will be ignored:

- given name and surname;
- personal / direct telephone number;
- respective organisation (if applicable)
- description (as detailed as possible) of the alleged problem;
- sufficient information for identifying the certificate that is the subject of the report. Reports must be drawn up in Italian or English.

The CA undertakes, within 24 hours, to take charge of the correctly prepared reports, to initiate an investigation of the reported problem (to ascertain its existence) and to take the necessary measures, depending on the case and the severity of the problem (see paragraph 5.9.2). The priority assigned to the report will depend on:

- the nature of the alleged problem;
- the identity of the reporting person (e.g. any reports by the Courts will be treated with greater priority than other reports);
- the legislation that applies to the problem (e.g. reports relating to unlawful acts will be considered as having a higher priority than other reports).

If the reported problem is confirmed, the CA will decide on the measures to be taken (e.g. revocation of the certificate) and will notify the reporting person by email.

Note: those who send unwanted messages ("spam") will be prosecuted in accordance with current regulations.

1.6 Definitions and acronyms

The following are the specific terms and abbreviations used in this CPS:

Definition	Description
AgID	Agency for Digital Italy
AgID CA1	Name of the AgID's Certification Authority that issues certificates for the certified email network; it operates under the responsibility of the AgID; the service is outsourced to RTI.
AgID CA SSL SERVER	Name of the AgID's Certification Authority that issues certificates for websites; it operates under the responsibility of the AgID; the service is outsourced to RTI.
Administration	Administration/Public body
CA	Certification Authority
Certifier	The entity that provides public key certification services or that provides other services related to the former.
CPS	Certification Practice Statement - this document
CRL	Certificate Revocation List - list of revoked certificates
CSR	Certificate Signing Request - certification request in accordance with RFC2314
FQDN	Fully-Qualified Domain Name
Certified email manager	Company/Administration/Entity that manages a Certified Email service in accordance with current regulations, accredited by the AgID.
HSM	Hardware Security Module (hardware encryption module)
No provision	Statement in accordance with the [SMBR], if it is not necessary to enter details for the purposes of the CPS.
PEC - Certified email	Certified Electronic Mail referred to in D.P.R. No. 68 of 11 February 2005
PKI	Public Key Infrastructure.
RA	Registration Authority
RSA	Rivest-Shamir-Adleman
RTI	Temporary Grouping of Companies
SSL	Secure Sockets Layer. Secure communication protocol over a TCP/IP network specifically aimed at securing access to websites.
TLS	Transport Layer Security. Current name of the protocol formerly known as SSL (see)

Some terms defined in the CAB Forum [BR] regulations are translated as follows:

- "Subscriber" is translated here as "Subscriber Organisation" or "Subscriber"
- "Applicant" is translated here as "Applicant Organisation" or "Applicant"

1.7 Regulatory framework

The relevant legal regulations for this CPS are listed below:

Reference	Description
[CAD]	Legislative Decree No. 82 of 5 March 2005, as amended
[DPCM200309]	Prime Ministerial Decree of 22 February 2012: "Technical rules on the generation, affixing and verification of advanced, qualified and digital electronic signatures", OJ No.117 of 21-05-2013
[DLVO19603]	Legislative Decree No. 196 of 30 June 2003, "Code regarding the protection of personal data "
[DPR6805]	D.P.R. No. 68 of 11 February 2005
[DMPEC]	Decree of the Minister for Innovation and Technologies, containing the "Technical regulations for the drafting, transmission and validation, which may also be temporary, of certified e-mails" of 2 November 2005
[CNIPACR56]	CNIPA Circular. 21/05/2009 – No. 56
[D-L 22 June 2012, No. 83]	Urgent measures for the Country's growth (12G0109) Official Journal 26 June 2012, No. 147, S.O.
[GDPR]	Regulation (EU) No. 679/2016 on Data Protection (GDPR)
[EIDAS]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014

1.8 Other references

Further relevant technical standards and regulations for this CPS are listed below:

[BR]	CAB Forum: “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates”, https://cabforum.org/baseline-requirements-documents/
[SMBR]	CAB Forum: “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted S/MIME Certificates", https://cabforum.org/smime-br/
[CPF]	RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", https://www.ietf.org/rfc/rfc3647.txt
[CSR]	RFC 2314: "PKCS #10: Certification Request Syntax - Version 1.5", https://www.ietf.org/rfc/rfc2314.txt
[CPROF]	RFC 5280: "Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile", https://www.ietf.org/rfc/rfc5280.txt
[OCSP]	RFC6960: "X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP”, https://tools.ietf.org/rfc/rfc6960.txt

2 Publications and repositories

2.1 Repositories

AgID makes available the information on the revocation of the Subscribers' certificates.

As regards intermediate CA certificates (i.e. the two issuing CAs registered to AgID indicated in §1.3.1), the information on revocation is published by the Root CA (please refer to the relevant CPS published on the Actalis website).

2.2 Published information

AgID publishes at least the following documents on its website, relating to the CA service described in this CPS, at http://www.agid.gov.it/cps-ca:

- Certification Practice Statement (CPS) – this document
- the certificate issuance request procedure
- the certificate request forms
- the CA certificates (Root CA, AgID CA1, AgID CA SSL SERVER)

For anything not detailed in this CPS, the provisions of §2.2 of the [BRs] apply.

2.3 Timing or frequency of publications

The provisions of §2.3 of the [BRs] apply.

2.4 Access control on repositories

Access to the repository in read-only mode is open to anyone.

3 Identification and authentication

In general, the certificates issued under this CPS contain information for clearly identifying the Subscriber. Pseudonyms and generic and/or ambiguous identifiers are not allowed.

3.1 Naming rules

3.1.1 Types of names

Subscribers' certificates issued under this CPS contain a non-null Distinguished Name (DN) in accordance with the ITU-T X.500 standard (ISO / IEC 9594) in the Subject and Issuer fields.

3.1.2 Significance of names

No provision.

3.1.3 Anonymity and pseudonymity of the Subscribers

Not applicable.

3.1.4 Rules for interpreting names

No provision.

3.1.5 Uniqueness of names

No provision.

3.1.6 Recognition, verification and role of registered trademarks

Names that violate the property rights of parties other than the Subscriber are not allowed in the certificates.

3.2 Initial identity validation

3.2.1 Verification of possession of the private key

Demonstration of the Applicant's possession of the private key corresponding to the requested certificate is based on cryptographic verification of the CSR (Certificate Signing Request) sent to the CA. As part of the certificate request, in fact, the Applicant must send its public key to the CA in the form of a CSR in PKCS#10 format [CSR]. The CA verifies that the CSR is correctly signed.

3.2.2 Validation of the requesting organisation and domains

3.2.2.1 Identity

Before accepting a certificate application, the CA verifies that the applicant Organisation, as stated in the certificate application documents (see paragraph 4.1), exists, is active, is named as stated by the Applicant, except for insignificant details, and what its registered office (address) is. To this end, the CA consults reliable public information sources such as the National PA Index, the Register of Companies, etc., as appropriate, in compliance with the provisions of the [BRs].

3.2.2.2 DBA/Tradename

Not applicable.

3.2.2.3 Country verification

See paragraph 3.2.2.1.

3.2.2.4 Verification of ownership or control of the domain or mailbox

For **SSL Server type certificates**, the CA must verify that the requesting Organisation has control of the Internet domains to be included in the certificate. This verification is carried out by one or more of the methods permitted by section 3.2.2.4 of the [BRs].

For Signature certificates (**S/MIME**), the CA must verify that the requesting Organisation has control of the email address to be included in the certificate. This verification is carried out by one or more of the methods permitted by section 3.2.2 of the [SMBRs].

3.2.2.5 IP Address Authentication

Not applicable.

3.2.2.6 Validation of wildcard domains

Not applicable.

3.2.2.7 Accuracy of information sources

Before using any source of information for the purpose of validating the requests, the CA assesses the reliability, the accuracy and the resistance to alterations or falsifications of the source, in accordance with paragraph 3.2.2.7 of the [BRs]. See also paragraph 3.2.2.1.

3.2.2.8 Domain CAA Record

The provisions of paragraph 3.2.2.8 of the [BRs] apply.

3.2.3 Authentication of individual identities

Not applicable.

3.2.4 Subscriber information not verified

In general, the CA does not verify the correctness of the information received from the applicant that is not intended to be included in the certificate and that is not necessary for issuing the certificate.

3.2.5 Authorisation Verification

Before accepting a certificate request, the CA verifies that the request is authentic; to this end, the CA verifies that the **digital signature** (i.e. **qualified electronic signature**) affixed to the application documentation (see paragraph 5.1) is a valid qualified electronic signature according to the regulations in force (in particular according to the [CAD]). It is also required that the signatory's certificate contain the **organisationName** (O) attribute in the Subject field and that its value corresponds to the name of the requesting Organisation.

3.2.6 Identification and authentication of renewal requests

The renewal process is similar to the first issue process: it consists of the Subscriber generating a new pair of keys, to replace the expiring one, and of a request to the CA for a corresponding new certificate, using the same methods as the first issue. For renewal, the same identification and authentication processes that apply to the first issue are followed.

3.2.7 Identification and authentication of revocation requests

The Organisation holding a certificate may request that it be revoked by sending the CA a certified email message (see section 4.9.2 for operational details). The authentication of revocation requests is based on the fact that they must be transmitted by certified email.

4 Operational requirements for certificate management

4.1 Certificate request

4.1.1 Who can apply for certificates

Certificates governed by this CPS can only be requested by:

- the Agency for Digital Italy (AgID)
- Certified email managers

4.1.2 Request and responsibility process

For each certificate to be issued, the Applicant must send the Agency for Digital Italy a certificate issuance request applying the following procedure:

1) The Head of the Organisation uses the electronic "**Registration Request"** form, available on the CA website (http://www.agid.gov.it/cps-ca) and fills it in. The file name .**doc** thus generated must have the following structure: <OrganisationName>–<certificate type>–<progressive>–<data>–RR.doc. The <certificate type> can have the following values: "signature", "authentication", "SSL server"; the <date> must be in the following format: YYYYMMDD.

2) The Head of the Organisation **digitally signs** the document obtained in point 1.

3) The Server Manager (specified in the form referred to in point 1) generates the request for CSR certification for the server to be certified, in PKCS#10 format. The CSR file name must have the following structure: <OrganisationName>–<certificate type>–<progressive>–<date>.csr. The <certificate type> can have the values indicated in point 1). The <date> must be in the format YYYYMMDD. To generate its own key pair, the **RSA** algorithm must be used, with a key length of **2048 bits**.

4) The Organisation Manager generates an archive file named <Organisation Name>–< certificate type >–<progressive>–<date>-Request Certificato.zip containing the digitally signed file referred to in point 2 and the CSR file generated in point 3.

All Certificate issuance requests (i.e. the .zip files obtained in point 4) are sent as an attachment to a certified email message addressed to richiesta-certificati@pec-ic.agid.gov.it which must the following subject:

"AgID-CA-Certificate Request <Organisation Name>"

4.2 Processing of requests

4.2.1 Carrying out identification and authentication functions

Upon receipt of a certificate request, all the previously described verifications (previous chapter 3 and paragraphs of this chapter) are performed automatically, where possible and permitted, or manually by a Validation Specialist when necessary or mandatory, in compliance with the [BRs].

Depending on the age and applicability of the information already available, the CA may reuse the previous validations for the purpose of issuing the certificate, within the limits allowed by the [BRs] and [SMBRs] according to the type of certificate.

If the necessary checks are not passed, the CA reports any problems to the Applicant, via certified email, and suspends the issuance procedure pending the possible resolution of the problems detected.

One week after reporting the problems, in the absence of feedback from the requesting Organisation, the case is closed and, if it still wishes to obtain the certificate, the requesting Organisation must send the CA a new request for certification as described in par. 5.1.

4.2.2 Approval or rejection of requests

The provisions of paragraph 4.2.2 of the [BRs] apply.

4.2.3 Request processing times

The processing times are consistent with what is stipulated in the contract for acquisition of the services essential for management, maintenance and support of the shared SPC infrastructures for AgID following the award of the open procedure tender, announced by Consip on behalf of the AgID, pursuant to art. 60, LegislativeDecree No. 50/2016 and subsequent amendments, (ID 2572 - published in the Official Journal of the European Union No. S-132 of 12/07/2022 and GYRU No. 82 of 15/07/2022). CIG 9290583F9D.

4.3 Issuance and delivery of the certificate

4.3.1 The CA's actions during issuance of the certificate

If the checks referred to in the previous section are passed, the CA carries out the following activities:

- it checks that the CSR is correctly coded and does not contain unexpected information;
- it checks that the information contained in the CSR is consistent with that indicated in the "Registration Request" form (see par. 5.1);
- it checks that the applicant is in possession of the private key corresponding to the CSR, as described in par. 3.2.1.

If the above checks are passed, the CA operator:

- provides for registration of the applicant in the CA database[2];
- it generates the certificate and sends it, together with the certificate of the intermediate CA, from the certified email address emissione-certificati@pec-ic.agid.gov.it to the certified email address of the subscriber Organisation from which the certificate request was received and, for information, to the e-mail box of the server manager specified on the "Registration Request" form.

If, on the other hand, the checks are not successful, the CA reports in detail all the problems encountered to the Applicant (AGID at the certified email address emissione-certificati@pec-ic.agid.gov.it and the entity responsible for the server entered in the registration request form at the email address entered in the registration request form), via certified email, and suspends the issuance procedure pending the possible resolution of the problems detected.

After one week from the reporting of the problems, in the absence of feedback from the requesting Organisation, the case is closed and, if it still wishes to obtain the certificate, the requesting Organisation must send the CA a new request for certification as described in paragraph 4.1.

SSL Server certificates comply with the Certificate Transparency requirements in accordance with the RFC 6962 specification. When a website certificate (i.e. SSL Server type) is about to be issued, a pre-certificate is first generated and subjected to an adequate number of qualified CT logs, in accordance with Google's or Apple's Chromium CT Policy. Each CT log returns signed certificate timestamp (SCT) as proof of inclusion in the log. Only at this point is the final certificate generated, in which the SCTs are incorporated as an extension (with OID 1.3.6.1.4.1.11129.2.4.2).

4.3.2 Certificate installation

Installation of the certificate is the responsibility of the Subscriber Organisation.

4.4 Certificate Acceptance

If the Applicant finds any inaccuracies or defects in the certificate, it must immedi-ately inform the CA by certified email at emissione-certificati@pec-ic.agid.gov.it.

In the absence of communications from the Subscriber, the certificate is considered accepted once 5 (five) days have elapsed from the date of delivery of the certificate.

4.5 Using the key pair and certificate

The certificates and the related keys must be used only for the intended purposes, as reported in paragraph 1.4.

4.6 Certificate renewal

The same procedure applies for the issuance of a new certificate.

[2] The applicant's registration consists of storing, in the CA database, the identification data of the applicant Organisation and other data necessary for generating the certificate.

4.7 Key regeneration

The same procedure applies for the issuance of a new certificate.

4.8 Modification of the certificate

To remedy any errors in the generation of the certificate (e.g. operational errors by the CA or errors by the Requesting party in completing the request), it is necessary to issue a new certificate. For this purpose, the Applicant must provide a new CSR (containing a new public key). In any case, a certificate containing incorrect information will be revoked by the CA as soon as it becomes aware of it.

4.9 Certificate revocation

Revocation results in the early termination of the validity of a certificate, starting from a given moment (date/time). The revocation of a certificate is irreversible and is completed with its publication in the Certificate Revocation List (CRL) published by the Certifier. The Subscriber of a revoked certificate must promptly remove (uninstall) the certificate from the associated server.

4.9.1 Circumstances for revocation of the certificate

With regard to the Subscriber certificates, the conditions requiring revocation include (non-exhaustive list):

- request from the Subscriber;
- order of the Courts;
- Subscriber's private key compromised (*);
- cessation of the Certificate Subscriber's activity (*);
- the certificate contains incorrect or no-longer-valid information (*);
- issuing CA's private key compromised;
- the Subscriber has not complied with one or more of the provisions of this CPS (*);
- the use of a domain contained in the certificate is no longer allowed for the Subscriber (*);
- the use of an email address contained in the certificate is no longer permitted for the Subscriber (*);
- in the case of signature certificates and Authentication certificates: the Subscriber has been removed from the list of Certified Email Managers accredited and/or by IGPEC and/or is no longer entitled to use the certificate at the discretion of AgID;
- termination of the CA service provided by the AgID under this CPS, in the absence of a replacement CA that is responsible for revoking and publishing information on the status of the certificates;
- the certificate is used improperly and/or unlawfully[3] (*);
- the certificate does not comply with this CPS (*);
- the certificate does not comply with the Requirements [BR] (*).

[3] No matter how, and on whose advice, the CA becomes aware of these situations (see also paragraph 4.13): if the situation is confirmed, the CA revokes the certificate

In all these cases, after ascertaining their actual occurrence, the AgID CA revokes the certificate **within 24 hours** and notifies the Subscriber.

(*) No matter how the CA becomes aware of these situations (see also para. 1.5.2).

Note: If the CA discovers that the certificate is used by the Subscriber for illegal activities (e.g. "Phishing", malware distribution, etc.) the CA shall carry out an *immediate* and unannounced revocation of the certificate. Similarly in the event that the CA discovers that the certificate mistakenly contains CA=TRUE in the KeyUsage extension.

Although not specified herein, the [BRs] apply.

4.9.2 Who can request revocation

Revocation may be requested (as the case may be):

- by the Certificate Subscriber;
- by AgID as CA;
- by the Courts;
- by the Root CA (Actalis).

In addition, anyone can report to the CA facts or circumstances that (if confirmed) may, as appropriate, justify revocation of the certificate (see paragraph 1.5.2),

Please note that, in some circumstances, the Subscriber is obliged to promptly request revocation of the certificate (see chap. 9).

4.9.3 Revocation procedure

The Subscriber may request the revocation of his certificate for any reason, but must request revocation of the certificate in the following circumstances:

- the certificate contains incorrect or no-longer-valid information;
- the private key corresponding to the certificate is compromised.

The latter circumstance must be promptly communicated to the CA; in any case, AgID assumes no responsibility for the improper use of the private key associated with the certified public key.

To request the revocation of a certificate, the applicant (who may be the Subscriber or the AgID itself) must send a **certified email** message to the CA at emissione-certificati@pec-ic.agid.gov.it with the subject "**AgID-CA Revocation request**" (otherwise the message will not be taken into account).

The message must contain sufficient information to identify the certificate that is to be revoked, e.g.:

- the Subject DN and the certificate's serial number
- or the certificate itself (as an attached file).

In addition, the message must specify the reason for the revocation request, e.g.

- certificate no longer needed,
- private key compromised,
- etc.

In the event that the information is incomplete or incorrect, the CA reports the problem to the applicant, via certified email, while waiting for the necessary clarifications.

If the request is clear and complete, the CA proceeds to revoke the certificate within the established timeframe, then confirms its revocation to the applicant via certified email.

4.9.4 Grace period for revocation requests

There is no grace period for requests to revoke certificates.

4.9.5 Maximum implementation times for revocation

The provisions of paragraph 4.9.5 of the [BRs] apply.

4.9.6 Revocation verification requirements

See paragraph 9.6.4.

4.9.7 Frequency of issuance of CRLs

See paragraph 4.10.1.

4.9.8 Maximum CRL latency

No provision.

4.9.9 Availability of online revocation verification services

Please refer to paragraphs 4.10 and 7.3.

4.9.10 Requirements for online revocation verification services

The provisions of paragraph 4.9.10 of the [BRs] apply.

4.9.11 Other methods of publishing revocation

There are no other ways to publish revocations besides the CRL and OCSP services.

4.9.12 Special requirements in the event of a key being compromised

See paragraph 4.9.1.

4.9.13 Circumstances for suspension

Not applicable.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Suspension procedure

Not applicable.

4.9.16 Limits on the suspension period

Not applicable.

4.10 Certificate status information services

The status of the certificates (active, suspended, revoked) is made available to all interested parties by publishing the Certificate Revocation List (CRL) in the format defined in the specification [RFC5280].

The CRL is accessible with HTTP protocol at the following URLs:

- http://ca1.agid.gov.it/CRL (signing and authentication certificates)
- http://ca1.agid.gov.it/SSLCRL (SSL Server certificates)

The HTTP address of the CRL is shown in the certificates themselves, in the CRLDistributionPoints extension (see heading 7).

The CRL is regenerated and republished at least every 6 hours, even if there have been no new revocations;

For SSL Server type certificates, there is also an online verification service based on the OCSP protocol (Online Certificate Status Protocol), compliant with specification [RFC6960]. This service is provided to the following URLs:

- http://ca1.agid.gov.it/OCSP (signing and authentication certificates)
- http://ca1.agid.gov.it/SSLOCSP (SSL Server certificates)

4.11 Termination of the contract

No provision.

4.12 Key escrow and key recovery

Not applicable.

5 Physical and operational security measures

The requirements of chapter 5 of the [BRs] are observed.

5.1 Physical security

The technological infrastructure of the AgID CA is managed by the RTI on behalf of AgID. In particular, the AgID CA processing systems are installed at the following Fastweb S.p.A. datacentres:

- FASTWEB BERNINA DATA CENTRE
  Via Piazzi 7, corner of Via Bernina - 20158, Milan
- FASTWEB CARACCIOLO DATA CENTRE
  Via Amari 6/8 - 20155, Milan

The security measures adopted there provide adequate guarantees regarding:

- Characteristics of the building and of the construction;
- Active and passive anti-intrusion systems;
- Physical access control;
- Electrical power supply and air conditioning;
- Fire protection;
- Flood protection;
- How magnetic media is stored;
- Magnetic media storage sites.

5.2 Operational security

The RTI defines and maintains a Security Plan that analyses AgID CA assets, risks to which they are exposed and describes the technical and organisational measures for ensuring an adequate level of security of operations. The risk analysis is reviewed periodically (at least annually).

5.2.1 Trusted roles

The following trusted roles are formally assigned within the scope of the CA service governed by this CPS:

- System Administrator
- System Operator
- System Auditor
- Security Officer
- Validation Specialist
- Registration & Revocation Officer

5.2.2 Number of people required to carry out the activities

The requirements of paragraph 5.2.2 of the [BRs] are complied with.

5.2.3 Identification and authentication for each role

All the trusted roles indicated in par. 5.2.1 use appropriate identification and authentication systems for access to the CA processing systems.

5.3 Safety of personnel

5.3.1 Qualifications, experience and authorisations required

The requirements of the [BRs] are complied with.

5.3.2 Background check

No provision.

5.3.3 Training requirements

The requirements of the [BRs] are complied with.

5.3.4 Training refresher frequency

The requirements of the [BRs] are complied with.

5.3.5 Rotation of tasks

No provision.

5.3.6 Penalties for unauthorised actions

No provision.

5.3.7 Checks on personnel who are not employees

The requirements of the [BRs] are complied with.

5.3.8 Documentation provided to staff

All personnel assigned to carry out the activities necessary for issuing and managing the certificates governed by this CPS are provided with the necessary documentation for performing their duties, in accordance with their role.

5.4 Audit log management

The requirements of section 5.4 of the [BRs] are complied with.

5.5 Archiving of records

The provisions of paragraph 5.5 of the [BRs] apply.

5.6 Renewal of CA keys

No provision.

5.7 *Impairment and disaster recovery*

"Disaster" means a harmful event, the consequences of which result in the service becoming unavailable under ordinary conditions, such as instances of failures and/or the unavailability of one or more of the items of equipment (computers, HSMs, wiring, technical rooms, power supply, etc.) necessary for providing the AGID CA certification services. In these cases, specific procedures are envisaged for recovery of the AgID CA certification service as soon as possible. These procedures are described in the Security Plan. For this purpose, a backup of the data, applications, logs, and any other files necessary for complete recovery of the service is carried out daily.

5.8 *Termination of the CA or the RAs*

No provision.

6 Technical security measures

6.1 *Logical security requirements of CA systems*

The CA platform consists of various software modules. To ensure the security of data and operations, all system and application software used for CA functions implements the following security functions:

- access control;
- identification and authentication of users and processes;
- attribution and investigation of any security-related event;
- management of storage resources aimed at preventing the possibility of tracing information previously contained or recorded by other users;
- self-diagnosis and integrity of data and software (monitoring of alignment between operational and reference copies, software configuration control, virus protection);
- hardware and software configuration to ensure continuity of service.

6.1.1 Generation of the key pair

The provisions of paragraph 6.1.1 of the [BRs] apply.

6.1.2 Delivery of the private key to the Subscriber

Subscribers' key pairs must be generated by the Subscribers themselves.

6.1.3 Delivery of the public key to the CA

The Applicant must provide its public key to the CA in the form of a Certificate Signing Request (CSR) compliant with the PKCS#10 standard.

6.1.4 CA public key distribution

AgID publishes its public keys, in the form of intermediate CA certificates, on its website (see https://www.agid.gov.it/it/piattaforme/posta-elettronica-certificata/certificati-gestori-pec-siti-web).

Regarding the Root CA's public key, please refer to the Actalis CPS.

6.1.5 Key length

The cryptographic keys of the issuing CAs and the Subscribers are of the RSA type.

The RSA keys of the two AgID issuing CAs ("AgID CA1" and "AgID CA SSL SERVER") have a length of at least 2048 bits.

The Subscribers' RSA keys comply with the following requirements:

- for Signature certificates (S/MIME), the key length is 2048 bits;
- for Authentication certificates, the key length is 2048 bits;
- for SSL Server certificates, the key length is 2048 bits.

6.1.6 Generation of parameters and key quality

The provisions of paragraph 6.1.6 of the [BRs] apply.

6.1.7 Key Usage (extension X.509 v3)

The provisions of paragraph 6.1.6 of the [BRs] apply.

6.2 Protection of the private key and security of cryptographic modules

6.2.1 Security requirements for cryptographic modules

The keys of the two AgID-issuing CAs ("AgID CA1" and "AgID CA SSL SERVER") are generated and stored inside a hardware cryptographic module (HSM) wirh at least the FIPS PUB 140 Level 3 security certification.

6.2.2 Multi-person control (N of M) of the private key

No provision.

6.2.3 Security deposit (key escrow) of the private key

Not applicable.

6.2.4 Private key backup

Please refer to paragraph 5.2.2.

6.2.5 Storage of the private key

No stipulation other than what is established in the [BRs].

6.2.6 Transfer of the private key from/to the cryptographic module

No stipulation other than what is established in the [BRs].

6.2.7 Storing the private key on the cryptographic module

The CA private keys are stored on HSMs that meet the requirements stated in paragraph 6.2.1.

6.2.8 How the private key is activated

No provision.

6.2.9 How the private key is deactivated.

No provision.

6.2.10 How the private key is destroyed

No provision.

6.2.11 Classification of the cryptographic modules

See paragraph 6.2.1.

6.3 Other aspects of key management

No stipulation other than what is established in the [BRs].

6.4 Activation data

No provision.

6.5 Computer security

The operating systems of the computers used to support the CA infrastructure comply with the specifications provided by the ITSEC class F-C2/E2 or Common Criteria EAL4, equivalent to the C2 of the TCSEC standards.

6.6 Lifecycle security

No provision.

6.7 Network security

The certification service has a network security infrastructure based on the use of firewalling mechanisms and the SSL/TLS protocol, creating a secure channel between all parties authorised to access the CA systems. The system is also supported by specific security products (network anti-intrusion, monitoring, virus protection) and all related management procedures.

In addition, a vulnerability assessment (VA) is carried out at least annually, using indipendent specialists, which also covers the online services provided by the CA, to assess the need for security reinforcement.

It also complies with the requirements of the "Network and Certificate System Security Requirements" published
at https://cabforum.org/working-groups/netsec/ .

6.8 Time reference

All the processing systems used by the CA are kept aligned with the exact time provided by a precise, reliable time server.

7 Certificate profile, CRL and OCSP

7.1 Certificate profile

7.1.1 Version numbers

Certificates issued under this CPS comply with the X.509 **v3** standard.

7.1.2 Certificate content and extensions

Certificates comply with the [BRs] or the [SMBRs], depending on the type of certificate.

7.1.2.1 Certificate of the CA that issues certificates for the certified email network

The certificate of the issuing CA that issues certificates for Certified Email Managers (signing and authentication certificates) has the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<Includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Root CA Subject DN>
Validity	(not stipulated)

Subject	CN = AgID CA1
	OU = Solutions Area for the Public Administration
	O = Agency for Digital Italy
	L = Rome
	C = IT

SubjectPublicKeyInfo	<2048-bit RSA public key>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true, pathLen=0
AuthorityKeyIdentifier (AKI)	<Root CA Extension Value>
SubjectKeyIdentifier (SKI)	<public key SHA1 digest>
KeyUsage	critical: keyCertSign, cRLSign

CertificatePolicies	PolicyOID = 1.3.76.16.3.1
	CPS-URI = <URL of this CPS on the AgID site>

NameConstraints	<as determined by the Root CA>
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
SubjectAlternativeName (San)	<absent>
AuthorityInformationAccess (AIA)	<HTTP address of the OCSP Service>
CRLDistributionPoints (CDP)	<ARL HTTP address>

7.1.2.2 Certificate from the CA issuing SSL Server certificates

The certificate of the issuing CA that issues SSL Server certificates has the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<Includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Root CA Subject DN>
Validity	12 months

Subject	CN = AgID CA SSL SERVER
	OU = Solutions Area for the Public Administration
	O = Agency for Digital Italy
	L = Rome
	C = IT

SubjectPublicKeyInfo	<2048-bit RSA public key>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true, pathLen=0
AuthorityKeyIdentifier (AKI)	<Root CA Extension Value>
SubjectKeyIdentifier (SKI)	<public key SHA1 digest>
KeyUsage	critical: keyCertSign, cRLSign

CertificatePolicies	PolicyOID = 1.3.76.16.3.1
	CPS-URI = <URL of this CPS on the AgID site>

NameConstraints	<as determined by the Root CA>
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) serverAuth (1.3.6.1.5.5.7.3.1)
SubjectAlternativeName (San)	<absent>
AuthorityInformationAccess (AIA)	<HTTP address of the OCSP Service>
CRLDistributionPoints (CDP)	<ARL HTTP address>

7.1.2.3 Signature Certificate (S/MIME)

The Signature Certificate (S/MIME) has the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<Includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	< Subject of the issuer CA >
Validity	<3 years>
Subject	C = <country where the organisation is based> ST = <province where the organisation is based> L = <location where the organisation is based> O = <the organisation's official name> **organisationIdentifier** = <as required by [SMBR]> CN = <**same value as attribute O**>
SubjectPublicKeyInfo	<2048-bit RSA public key>
SignatureValue	<signature of the issuing CA>
Extension	**Value**
Basic Constraints	(absent)
AuthorityKeyIdentifier (AKI)	<value of the issuing CA's SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1 digest according to RFC5280>
KeyUsage	critical: digitalSignature
ExtendedKeyUsage (EKU)	emailProtection (1.3.6.1.5.5.7.3.4)

CertificatePolicies	PolicyOID = 1.3.76.16.3.1.1
	PolicyOID = **2.23.140.1.5.2.1**
	(CAB Forum smime organisation-validated legacy)
	CPS-URI = <URL of this CPS on the AgID site>

SubjectAlternativeName (San)	rfc822Name=<owned email address / under the control of the Organisation subscribing to the
CRLDistributionPoints (CDP)	<HTTP address for access to the CRL>

7.1.2.4 Certificate for Authentication

The Authentication Certificate has the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<Includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	< Subject of the issuer CA >
Validity	<3 years>
Subject	C = <country where the organisation is based> ST = <province where the organisation is based> L = <location where the organisation is based> O = <official name of the organisation> OU = <optional > CN = <…>
SubjectPublicKeyInfo	<2048-bit RSA public key>
SignatureValue	<signature of the issuing CA>
Extension	**Value**
Basic Constraints	(absent)
AuthorityKeyIdentifier (AKI)	<value of the issuing CA's SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1 digest according to RFC5280>
KeyUsage	critical: digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)	**clientAuth** (1.3.6.1.5.5.7.3.2)

CertificatePolicies	PolicyOID = 1.3.76.16.3.1.2
	CPS-URI = <URL of this CPS on the AgID site>

SubjectAlternativeName (San)	**(absent)**
CRLDistributionPoints (CDP)	<HTTP address for access to the CRL>

7.1.2.5 Website certificate (SSL Server)

The website certificate (SSL Server) has the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<Includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	< Subject of the issuer CA >
Validity	<1 year>

Subject	C = IT
	ST = <province where the organisation is based>
	L = <location where the organisation is based>
	O = <the organisation's official name>
	CN = <FQDN contained in SAN extension>

SubjectPublicKeyInfo	<2048-bit RSA public key>
SignatureValue	<signature of the issuing CA>
Extension	**Value**
Basic Constraints	(absent)
AuthorityKeyIdentifier (AKI)	<value of the issuing CA's SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1 digest according to RFC5280>
KeyUsage	critical: digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) serverAuth (1.3.6.1.5.5.7.3.1)

CertificatePolicies	PolicyOID = **2.23.140.1.2.2** (**organisation-validated**)
	PolicyOID = 1.3.76.16.3.1.3
	CPS-URI = <URL of this CPS on the AgID site>

SubjectAlternativeName (San)	<One or more FQDNs, in accordance with the [BR]>
CRLDistributionPoints (CDP)	<HTTP address for access to the CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	List of Signed Certificate Timestamps according to RFC 6962

7.1.3 Algorithm identifiers

The provisions of §7.1.3 of the [BRs] apply.

7.1.4 Name forms

Certificates issued under this CPS contain a non-null Distinguished Name (DN) compliant with ITU-T X.500 (ISO / IEC 9594) in the Subject and Issuer fields.

In particular, the following rules apply to the Subject field of the Subscribers' certificates:

- The **countryName** (“**C**”) attribute of the Subject is always present and contains the 2-letter code (ISO 3166-1 alpha-2) of the country in which the Organisation subscribing to the certificate has its registered office;
- The attribute **stateOrProvinceName** ("**ST**") of the Subject is always present and contains the name (not the initials) of the Province in which the Organisation holding the certificate has its registered office;
- The attribute **localityName** ("**L**") of the Subject is always present and contains the name of the location (city) in which the Organisation subscribing to the certificate has its registered office;
- The **organisationName** ("**O**") attribute of the Subject is always present and contains the official name of the Organisation subscribing to the certificate;
- The **organisationIdentifier attribute**(OID 2.5.4.97) of the Subject is *present only in the Signature certificates* (S/MIME) and contains the identification number of the owner Organisation with the coding provided for by [SMBR];
- The **commonName** (“**CN**”) attribute of the Subject is always present and contains:
  - in the case of Website certificates (**SSL Server**), one of the FQDNs included in the **SubjectAlternativeNames** extension;
  - in the case of **Signature certificates** (S/MIME), the same value as the **organizationName** attribute;
  - in the case of **Authentication certificates**, a string at the discretion of the requesting Organisation, provided that it is not misleading with respect to the Subscriber's identity;
- The **SubjectAlternativeNames** (SAN) extension is assigned a value as follows:
  - in the case of **SSL Server** Certificates: one or more full domain names (FQDNs) under the control of the subscriber Organisation (AgID);
  - in the case of certified email **Signature** Certificates: an email address under the control of the subscriber Organisation;

  In the case of **Authentication Certificates,** this extension is absent.

SSL Server certificates are not issued for internal addresses (internal server names), i.e. belonging to private networks. Website addresses that may appear in SSL Server certificates must be FQDNs (Fully Qualified Domain Names). In addition, no SSL Server certificates are issued for IP addresses.

7.1.5 Name constraints

Both issuing CAs used for the issuance of the certificates governed by this CPS are *technically constrained* CAs through the NameConstraints extension in compliance with the [BRs]. In particular:

- The "AgID CA1" may issue certificates only for organisations that have been expressly authorised by the AgID and, with regard to Signature certificates, only for email addresses that have been validated as described in §3.2.2;
- The "AgID CA SSL SERVER" can issue certificates only for the AgID and only for domains that have been validated as described in §3.2.2;

7.1.6 Policy identifiers

The OID Policy **2.23.140.1.2.2** (organisation-validated) defined in the [BRs] is inserted in the CertificatePolicies extension of SSL Server certificates.

The OID Policy **2.23.140.1.5.2.1** (organisation-validated legacy) defined in the [SMBRs] is inserted in the SSL Server Signature Certificates (S/MIME).

7.1.7 Use of the PolicyConstraints extension

No provision.

7.1.8 Syntax and Semantics of the policy qualifiers

No provision.

7.1.9 Processing rules for the extension of CertificatePolicies

No provision.

7.2 CRL Profile

The CRLs issued by the "AgID CA" comply with the public specification RFC 5280 [CPROF].

The provisions of paragraph 7.2 of the [BRs] also apply.

7.3 OCSP Profile

The OCSP service provided for the "AgID CA" complies with the public specification RFC 6960 [OCSP].

The provisions of paragraph 7.3 of the [BRs] also apply.

8 Compliance checks

8.1 Frequency and circumstances of checks

The provisions of Chapter 8 of the [BRs] apply.

8.2 Identity and qualification of inspectors

The provisions of Chapter 8 of the [BRs] apply.

8.3 Relations between the CA and the auditors

The provisions of Chapter 8 of the [BRs] apply.

8.4 Areas covered by the checks

The provisions of Chapter 8 of the [BRs] apply.

8.5 *Actions resulting from non-conformities*

If there are found to be certificates that do not comply with this CPS, these certificates will be revoked and, if necessary, replaced with new correct certificates. In the event of other non-conformities, the resulting actions will be evaluated by the AgID and/or Root CA in light of the provisions of the applicable rules and regulations.

8.6 *Reporting of the results of the checks*

The provisions of Chapter 8 of the [BRs] apply.

8.7 *Self-assessments (self-audit)*

The provisions of Chapter 8 of the [BRs] apply.

9 General terms and conditions of service

This section governs the service relationship between the AgID and the Subscribers of certificates issued under this CPS.

Before requesting the issuance of a certificate, the Applicant is required to read and approve the general conditions for provision of the service reported within the CPS. By signing the "Registration Request" forms referred to in the Operational Processes paragraph, the signatory declares that they are aware of and approve these conditions.

The reports for the provision of server certification services are subject to Italian law. In the provision of its services, AgID operates in accordance with legislation on the protection of personal data (privacy).

9.1 *Service fees*

Not applicable.

9.2 *Financial responsibility*

No provision.

9.3 *Confidentiality of the information processed*

No provision.

9.4 *Processing and protection of personal data*

Applicable laws apply.

9.5 *Intellectual property rights*

This CPS is the property of the AgID which reserves all related rights.

The Subscriber retains all rights to its domain names and/or email addresses, if any.

With regard to the ownership of other data and information, the laws in force apply.

9.6 Obligations and guarantees

9.6.1 The CA's obligations and guarantees

The Certifier undertakes to:

- Operate in full compliance with this CPS.
- Before issuing a certificate, obtain from the requesting Organisation, acceptance of the AGID CA service general conditions.
- Verify the origin and authenticity of the certificate issuance requests.
- Verify that each certificate request is authorised by the requesting Organisation.
- Verify that, when the certificate was issued, the Subscriber had the corresponding private key.
- Ensure that, when the Signature certificate was issued, the applicant had ownership or control of the email address included in the certificate.
- Ensure that, when the SSL certificate was issued, the applicant had the right to use or de facto control of the domain names listed in the Subject field of the Certificate and in the SubjectAltName extension.
- Ensure that the information contained in the certificates was correct and truthful when the certificates were issued.
- Provide an efficient service, available 24/7, for the revocation of certificates.
- Provide an efficient online service, available 24/7, to consult on the status (valid or revoked) of certificates issued and not yet expired.
- Process the Subscribers' personal data in compliance with current regulations.
- Promptly revoke certificates in the circumstances provided for in this CPS.

9.6.2 The RAs' obligations and guarantees

Not applicable.

9.6.3 The Subscribers' obligations and guarantees

The Subscriber has an obligation to:

- Read this CPS carefully before requesting a certificate.
- During the application and registration phase, provide the CA with accurate and truthful information.
- Generate and store its private key safely, taking the necessary precautions to avoid damage, alteration or its unauthorised use.
- Send the certification request to the CA in the manner indicated in this CPS.
- Install and use the certificate only after checking that it contains correct information.
- Never, for whatever reason, to use its private key for issuing certificates.
- Use the certificate only for the purposes provided for in this CPS, and only for lawful purposes.

- Promptly inform the AgID in the event that the information in the issued certificate is no longer valid, requesting that the certificate be revoked.
- Promptly inform the AgID if you believe that the security of the server on which the certificate has been installed may have been compromised, requesting that the certificate be revoked.
- Promptly remove a revoked certificate from the server.
- Respond promptly to CA requests regarding the possible misuse of the certificate or compromised key.

The Subscriber accepts that, if and as soon as it discovers that a certificate is used by the Subscriber for unlawful activities (e.g. "Phishing", distribution of malware, etc.) and/or for the issuance of other certificates, the CA will revoke the certificate immediately and without prior notice.

9.6.4 The Relying Party's obligations and guarantees

A "Relying Party" is defined as anyone who relies on a certificate to make decisions (such as: providing confidential information to the Certificate Subscriber, considering as reliable and making use of the information provided or transmitted by the Certificate Subscriber, etc.). With respect to certificates issued under this CPS, the relying parties are required to:

- make a reasonable effort to acquire sufficient information on the operation of certificates and PKIs in general;
- check the status of the certificates issued by the AgID on the basis of this CPS, by accessing the information services described in section 5.10;
- rely on a certificate only if it has not expired, been suspended or revoked.

9.6.5 Obligations and guarantees of other parties

No provision.

9.7 Disclaimer of warranties

The CA has no further obligations and does not guarantee anything in addition to what is expressly indicated in this CPS or provided for by current regulations.

9.8 Limitations of liability

The AgID is not liable with respect to the Applicant or third party users for damages of whatever kind deriving from the non-issuance of the certificate or from improper use of the certificate.

The AgID's liability with respect to the Applicant or third parties is in any case limited to the cost of issuing the certificate, except in cases where art. 1229 of the Civil Code does not allow such limitation.

9.9 Compensation

No provision.

9.10 Duration and termination of the contract

No provision.

9.11 Notices and communications

The AgID accepts communications related to this CPS, as well as reports concerning problems, to be sent using the methods indicated in paragraph 1.5.2.

9.12 Amendments

No provision.

9.13 Jurisdiction

No provision.

9.14 Governing Law, interpretation and jurisdiction

These General Conditions are subject to Italian law. For any disputes that may arise between the parties regarding the provisions of this CPS, the Court of Rome shall have exclusive jurisdiction.

9.15 Compliance with applicable laws

The provisions of paragraph 9.15 of the [BRs] apply.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS constitutes the provisions governing the Subscriber's use of the Certificate and also governs relations between the Subscriber and CA. A request for a Certificate implies the Subscriber's full and unconditional acceptance of this.

9.16.2 Assignment of the contract

No provision.

9.16.3 Severability

The CA shall comply with paragraph 9.6.13 of the [BRs].

9.17 Other provisions

The certificate is normally issued within 3 working days of receipt of the "Certificate issuance request" during the hours in which this service is available (Monday to Friday, from 8:00 a.m. to 8:00 p.m., Saturday from 8:00 a.m. to 2:00 p.m., excluding holidays), provided that the request is correct.

END OF DOCUMENT