Cedacri Qualified Electronic Signature Operating Manual- CP and CPS

Document Code:	IA00G009-011
Document status:	Approved
Issued on:	30/05/2023
Issued by:	CISO

Document Owner	Giuliano Merlo	
Written by:	Domenico Garuffi	
Issue*:	ORGA, ICTGE	30/05/2023 Date*
Approved by:	CISO	29/05/2023 Date
Document Code*:	IA00G009-011	30/05/2023
Document status*:	Approved	
Distribution:	Public	

First Version Issued on:	05/06/2017
Printed on:	30/05/2023

KEY

*The writer **shall not complete** the fields marked with asterisk " * " since the relevant information is **automatically** updated upon printing based on the indications set forth on the document front-page. To update these fields, right-click and, from the context menu, select **update field.***
*To update every page with the correct header, double-click on the header, select the code field, issue date and title with the mouse right button, then select **update field** from the context menu. Even though not relevant, the other fields shall be filled **at least with a <whitespace> character.***

Distribution

Distribution is a field to be filled in by hand and may take up the following values:

- *Public, if the document may be circulated with no restrictions, both within the organization and to external entities;*
- *Reserved, if the document may be distributed only to Cedacri Users or within a Project Group (please, specify which Project Group);*
- *Confidential, if the document may be distributed within the organization to certain persons (please, specify which persons)*
- *User, if the document in intended for the Customer's Organization*
- *<other>, please, specify.*

History of changes made

Changes made from Version 1 to Version 2 (June 2017)

Maximum updates in accordance with company policy in place

Changes made from Version 2 to Version 3 (June 2017)

Edit par.1.2

Added in par.9.12 the complaints management

Changes made from Version 3 to Version 4 (August 2017)

Edit Annex 10.1

Edit Annex 10.2

Changes made from Version 4 to Version 5 (October 2017)

Update par.5.7

Update par.5.8

Changes made from Version 5 to Version 6 (September 2018)

Update par. 1.4.1

Update par. 4.5.2

Update par. 5.3.3

Update par. 9.4

Update par. 9.4.4

Update par. 9.14 – GDPR

Changes made from Version 6 to Version 7 (July 2019)

Update chap.9 – Other Legal and Business Aspects

Update par. 1.3.1 – Certification Authority

Update par. 1.2 - Name and identification details of the document

Update par. 2.2.2 – Publication of certificates

Update par. 2.2.3 – Publication of revocation and suspension lists

Update par 4.5.3 – Limitations of use and value

Update par 9 – Other legal and business aspects

Addition par 10.4 – ASN1 Dump Root CA Certificate EJBCA

Addition par 10.5 - ASN1 Dump End User EJBCA

Changes made from Version 7 to Version 8 (August 2020)

Update par. 1.2 – Organizational Unit Issuer

Update par. 1.5.2 – Document's responsible Unit

Update par.10 – Delete all Cedacricert CA 2017 references

Changes made from Version 8 to Version 9 (February 2021)

Update par. 1.2 – Organizational Unit Issuer

Update par. 1.3.1 – Organizational Details

Update par. 1.5.2 – Document's responsible Unit

Changes made from Version 9 to Version 10 (June 2021)

Update par. 1.5.4 – Revision of the Operating Manual and history of changes made

Update par. 3.2.3 – Identification of a natural person

Update par. 4.9.3 – Procedures for requesting revocation

Changes made from Version 10 to Version 11 (May 2023)

Update par. 1.3.1 – Organizational Details update

Update par. 5.7.1 – Incident communication process update

Added paragraph 1.7 - References and Annexes.

TABLES OF CONTENTS

1. INTRODUCTION

1.1. GENERAL FRAMEWORK

Generally speaking, a digital signature enables a subject to express the authenticity and integrity of a computerised document through the use of a pair of asymmetric keys (one public and one private), in such a way that anyone who comes into possession of said document can always verify that it is fully valid.

This document is the Operating Manual of the **Qualified Trust Service Provider** (QTSP), hereinafter also referred to as Cedacri, which provides qualified electronic signature services.

This manual contains the policies and practices followed during the process of identifying and issuing the qualified certificate and everything that makes a qualified certificate reliable, in accordance with the regulations in force on trust services, qualified electronic signature and digital signature.

The publication of this Operating Manual and the inclusion of references to said document in the certificates shall enable users to assess the characteristics and reliability of the certification service and, therefore, of the link between key and subject.

Its content is based on the regulations in force as at the issue date and incorporates the recommendations set out in the document “Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” © Internet Society 2003.

1.2. NAME AND IDENTIFICATION DETAILS OF THE DOCUMENT

This document is a follow-up to the corporate document named "Operating Manual" with the following characteristics:

Code IA00G009

Issued by System Security and Certification Area

Document name Cedacri Qualified Electronic Signature Operating Manual- CP and CPS

Valid date: This document is valid as of the date of approval of the Conformity Report issued by the CAB.

The document is associated with the object identifier (OID) that identifies Cedacri: ***1.3.76.27***.

The policies for qualified certificates relate to:

Operating-manual-qualified certificate issued to natural person	in accordance with policy QCP-n 0.4.0.194112.0
Operating-manual-qualified certificate issued to natural person and keys via qualified signature creation device (QSCD)	in accordance with policy QCP-n-qscd 0.4.0.194112.2

For the new CA EJBCA, the policies for qualified certificates are related to:

- Operating-manual-qualified certificate issued ti natural person in according with policy QCP-n 0.4.0.194112.1.2

- Operating-manual-qualified certificate issued to natural person and keys via qualified signature creation device (QSCD) in according with policy QCP-n-qscd 0.4.0.194112.1.2

This document is published in electronic format on the website of the QTSP, at the address: http://www.cedacricert.it/ , in the “Documentation” section.

1.3. PARTICIPANTS AND RESPONSIBILITIES

1.3.1 Certification Authority

The **Certification Authority** is the trusted third party that issues qualified digital signature certificates, signing them with its own private key, known as a CA key or root key.

Cedacri is the Certification Authority (**CA**) that issues, publishes in the register and revokes Qualified Certificates, operating in compliance with the technical rules issued by the Supervisory Authority and in accordance with the provisions of the eIDAS Regulation and the Digital Administration Code.

The complete data of the organisation that performs the function of CA are as follows:

0

Company name	***Cedacri S.p.A.***
Registered office	***Corso Monforte, 30 20122 Milano (Milano)***
Legal representative born in role	***Luca Peyrano Milano (Milano), 09 gennaio 1971 Executive Chairman***
Milan Monza Brianza Lodi Register of Companies no.	***00432960342***
VAT no.	***00432960342***
Group VAT no.	***02952290340***
ABI code	***89002***
UNINFO Object Identifier (OID)	***1.3.76.27***
ISO-OID P.E.N.	***8414***
Telephone no.	***0521 8071 (switchboard)***
Fax no.	***+39 0521 807373***
Website	www.cedacricert.it
Email	servizifiduciari-cedacri@iongroup.com
Certified email address	servizifiduciari@postacert.cedacri.it

The **Certification Authority** is required to adopt all appropriate technical and organisational measures for such a service.

Specifically, the Certificator that issues qualified certificates is required to:

- verify the identity of the person requesting a Certificate;
- issue the relative qualified certificate in accordance with the terms;
- inform the holders of the characteristics of the service;
- adopt the necessary security measures for the processing of personal data;
- ensure that the secure device for generating the signature has the

characteristics required by the regulations;
- ensure that the holder always maintains exclusive control of their signature keys;
- ensure that private signature keys generated within HSMs cannot be exported;
- keep the list of revoked Certificates up to date;
- keep the list of suspended Certificates up to date;
- manage all procedures necessary for the purposes of the aforementioned activities, in accordance with adequate security standards;
- keep records of all information relating to the management of the qualified certificate for at least 20 years.

The QTSP is directly responsible towards the subjects for the work it has carried out, without prejudice to any right to compensation.

1.3.2 Registration Authority (RA)

The Certificator may issue a mandate to perform the functions of **Registration Authority** to Banks, Credit Institutions or other Entities that have signed a specific mandate agreement with the Certificator.

The role of **Registration Authority** is carried out by personnel explicitly authorised and trained by the QTSP.

The operator:

- identifies with certainty the user requesting the certification of a public key;
- sends the QTSP the user's certification request;
- archives a copy of the agreement signed by the user with a copy of the attached identity document;
- provides the user with everything required to complete the certificate request procedure.

The list of Registration Authorities will be published on the website www.cedacricert.it .

The role of Registration Authority is currently being performed by Cedacri.

1.3.3 Subject

The **Subject** is the natural person who is the holder of the qualified certificate in which the essential identification data are inserted. In some parts of the manual and in some limitations of use, the Subject may also be defined as the 'Holder', and is required to:

- provide the QTSP with all necessary information upon requesting a certificate;
- use the private key exclusively for the purposes for which the corresponding public key is certified;
- diligently store the signature device;
- store the information required to use the private key (signature device PIN) in a different place to the device containing the key;
- immediately request the revocation of the certificate in the event of loss, theft, damage or destruction of the signature device;
- immediately request the revocation of the certificate in the event of certainty that the private key used has been compromised;
- cease using the pair of keys once the certificate has expired;
- provide a valid email address;
- inform the QTSP of any subsequent changes to their email address, sending an

email signed using their certificate to the address: servizifiduciari-cedacri@iongroup.com;
- adopt all organisational and technical measures required to prevent damage to others;
- promptly inform the QTSP of any changes to their identification data and/or powers of representation or other titles relating to their activity or positions held (change, termination, revocation).

The QTSP is not liable for any damage caused to the subject, users or third parties as a result of non-compliance, by the Subject, with their obligations as Holder and, more generally, the obligations set out in this manual.

The QTSP, without prejudice to the right to revoke or suspend the certificate, may terminate at any time, pursuant to Article 1456 of the Civil Code, the contractual relationship in place with the Holder, if the latter fails to comply with a single one of the obligations set out in this section.

1.3.4 User

The User is the person who receives a computerised document signed with the digital certificate of the Subject, and who relies on the validity of said certificate (and/or on the digital signature therein) to assess the correctness and validity of the document, in the contexts in which it is used.

The **User** of certified public keys is required to perform, at least, the following actions:

- verify that the type of certificate used for the signature;
- verify the lists of revoked and suspended certificates published by the Certificator to ensure that the certificate was valid at the time of signature;
- verify the existence of any limitations on use of the certificate;
- verify that the certificate has been issued by a certificator published on the lists kept at the Digital Italy Agency.

Holders' data cannot be used for unsolicited communications, such as advertisements or similar, even if they are published.

1.3.5 Requestor

The Requestor is the natural or legal person that asks the CA to issue digital certificates for a Subject, possibly assuming the costs involved and acquiring the right to suspend or revoke said certificates. The role, where present, can also be assumed by the RA.

More specifically, the following cases may apply:

- The Requestor may coincide with the Subject, if this is a natural person;
- The Requestor may be the legal person that requests the certificate for natural persons connected thereto by commercial relations or in the context of organisations.

The Requestor may be the natural or legal person from which the powers of signature or the role of the Subject derive. In this case, where the Requestor is also defined as an 'Interested Third Party', the certificate includes an indication of the Organisation with which the Subject is associated, and/or their role.

If not otherwise specified in the contractual documentation, the Requestor coincides with the Subject.

1.3.6 Authorities

Digital Italy Agency -AgID

The Digital Italy Agency (**AgID**) is the body responsible for overseeing providers of trust services, pursuant to Article 17 of the eIDAS Regulation. In this role, AgID oversees qualified trust service providers established in Italy in order to ensure that they comply with the requirements set forth by the Regulation.

Conformity Assessment Body

The Conformity Assessment Body (**CAB**) is an accredited organisation in accordance with the provisions of the eIDAS Regulation, which is competent to assess whether qualified trust service providers and the qualified trust services provided by them conform to the applicable regulations and standards.

1.4. CERTIFICATE USAGE

1.4.1 Permitted uses

Certificates issued by the CA in accordance with the terms indicated in this operating manual are Qualified Certificates pursuant to the Digital Administration Code and the eIDAS Regulation.

The certificate issued by the CA shall be used to verify the qualified signature of the Subject to which the certificate pertains.

Cedacri makes a free of charge tool available to its customers. This tool allows users to affix and verify digital signatures in standard format, and to request and verify time stamps.

Other verification products may be available on the market, with functionalities and limitations in accordance with the provider's indications.

1.4.2 Non-permitted uses

Use of the certificate outside of the limits and contexts specified in the operating manual and the agreements is prohibited, as is use that in any way violates the established limitations of use and value (*key usage*, *usernotice*).

1.5. ADMINISTRATION OF THE OPERATING MANUAL

1.5.1 Contacts

Cedacri is responsible for the definition, publication and updating of this document. A call centre is available for service users, for any kind of information concerning the procedures described in this manual. The service is available 24/7, including on public holidays, on 840 033033.

1.5.2 Subjects responsible for approving the Operating Manual

The person responsible for this document is the Cedacri's CISO - Chief Information Security Officer. This document is approved by corporate management.

1.5.3 Approval procedures

The preparation and approval of the manual follows the procedures set out in the company's Quality Management System, in accordance with ISO 9001..

At least once a year, the Trust Services Provider carries out a check to ensure that this Operating Manual conforms to the actual process of providing the certification service.

1.5.4 Revision of the Operating Manual and history of changes made

Each new version of the Operating Manual annuls and replaces the previous version in force; nevertheless, certificates issued during the applicability of previous versions remain valid until their first expiry.

As described in the previous section, all changes to the manual are tracked in a dedicated section called “History of changes made” and, once approved, the document is promptly published and made available in accordance with the procedures provided for. For any technical or procedural modification that involves significant changes, the CA must undergo an audit by an accredited CAB, present the Conformity Assessment Report (CAR) and the Operating Manual to the Supervisory Authority (AgID), and await permission for publication.

At least one annual review of the Operating Manual is guaranteed.

1.5.5 Notification period and mechanism

The Operating Manual is published:

- in electronic format on the website http://www.cedacricert.it/cedacricert/it/documentazione/;
- in electronic format on the public list of certificators kept by AgID.
- It can be requested in paper format from: auditing-cedacri@iongroup.com.

1.6. DEFINITIONS AND ACRONYMS

1.6.1 Definitions

As per EU Regulation 910/2014 (eIDAS), Article 3:

1) ‘electronic identification’ means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

2) ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

3) ‘person identification data’ means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person, to be established;

4) ‘electronic identification scheme’ means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

5) ‘authentication’ means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

6) ‘relying party’ means a natural or legal person that relies upon an electronic identification or a trust service;

7) ‘public sector body’ means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

8) ‘body governed by public law’ means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (1);

9) ‘signatory’ means a natural person who creates an electronic signature;

10) ‘electronic signature’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

11) ‘advanced electronic signature’ means an electronic signature which meets the requirements set out in Article 26;

12) ‘qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

13) ‘electronic signature creation data’ means unique data which is used by the signatory to create an electronic signature;

(14) ‘certificate for electronic signature’ means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

(15) ‘qualified certificate for electronic signature’ means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

(16) ‘trust service’ means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or

b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;

(17) ‘qualified trust service’ means a trust service that meets the applicable requirements laid down in this Regulation;

(18) ‘conformity assessment body’ means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008,

which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;

(19) 'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

(20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

(21) 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;

(22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;

(23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;

(24) 'creator of a seal' means a legal person who creates an electronic seal;

(25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

(26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;

(27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

(28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;

(29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;

(30) 'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;

(31) 'electronic seal creation device' means configured software or hardware used to create an electronic seal;

(32) 'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;

(33) 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

(34) 'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;

(35) 'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

(36) ‘electronic registered delivery service’ means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(37) ‘qualified electronic registered delivery service’ means an electronic registered delivery service which meets the requirements laid down in Article 44;

(38) ‘certificate for website authentication’ means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

(39) ‘qualified certificate for website authentication’ means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

(40) ‘validation data’ means data that is used to validate an electronic signature or an electronic seal;

(41) ‘validation’ means the process of verifying and confirming that an electronic signature or a seal is valid.

1.6.2 Acronyms

QTSP Qualified Trust Service Provider

CA Certification Authority

HSM Hardware Security Module

HA High Availability

CRL Certificate Revocation List

OCSP Online Certificate Status Protocol

TSA Time Stamp Authority

TSU Time Stamp Unit

QSCD Qualified Signature Creation Device

RAO Registration Authority Operator

RA Registration Authority

1.7. REFERENCES AND ANNEXES

[1]

Cedacri S.p.A.

IA99Q013 – Codice di Comportamento

Documento Interno

[2]
Cedacri S.p.A.
XQ99Q880 – Gestione delle Risorse Umane
Documento Interno

2. PUBLICATION AND ARCHIVING

2.1. ARCHIVING

The published certificates, CRLs and operating manuals are published and available 24/7.

2.2. PUBLICATION OF INFORMATION ABOUT THE CERTIFICATION

2.2.1 Publication of the Operating Manual

This Operating Manual can be found in electronic format at the QTSP's website.

This Operating Manual, the list of certification key certificates and the other information relating to the CA required by law are published within the certificators' list.

2.2.2 Publication of certificates

The lists of certificates in force (subject to the Subject's authorisation for publication) can be available at http://www.cedacricert.

2.2.3 Publication of revocation and suspension lists

The Certificate Revocation Lists (CRLs) and Certificate Suspension Lists (CSLs) are available at http://www.cedacricert.it/ and can be accessed by following the instructions on the browser menu.

2.3. PERIOD OR FREQUENCY OF PUBLICATION

2.3.1 Frequency of publication of the Operating Manual

The frequency with which the Operating Manual is published varies according to when changes are made.

If the changes are significant, the QTSP must undergo an audit by an accredited CAB, present the Conformity Assessment Report (CAR) and the Operating Manual to the Supervisory Authority (AgID), and await permission for publication.

2.3.2 Frequency of publication of revocation and suspension lists

Revoked certificates are included on the CRL, which is issued by the QTSP, published and time-stamped.

The aforementioned list is ordinarily published daily, every eight hours.

In the event of a request for immediate revocation, the CRL shall be published immediately.

2.3.3 Control of access to public archives

Information relating to certificates published, CRLs and operating manuals is public, and is suitably protected.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1 Name types

The identifier of the Subject is a Distinguished Name (DN), i.e. an extended formatted sequence of the Subject's personal data, issued in accordance with the RFC 5280 and ETSI standards and the indications of the Presidential Decree.

3.1.2 Need for the name to have a meaning

The DN feature uniquely identifies the Subject to which the certificate is issued.

3.1.3 Anonymity and pseudonymity of requestors

Anonymity is not permitted, while pseudonymity is governed by Article 5, paragraph 2 of the eIDAS Regulation and the Digital Administration Code.

3.1.4 Rules for interpreting name types

The rules for interpreting name types are governed by ETSI EN 319 412-2, paragraph 4.2.4.

3.1.5 Uniqueness of names

In the case of a natural person, in order to guarantee the Subject's uniqueness, the certificate must indicate the forename and surname, as well as a unique identification code:

- the tax ID for Italian citizens;
- the tax identification number (TIN) for foreign citizens. The TIN can be assigned by the authorities of the country of which the Subject is a citizen, or by the country in which the organisation in which they work is headquartered.

In the absence of a tax ID or TIN, the certificate can include an identification code taken from a valid identity document that is used in the context of recognition procedures.

3.2. INITIAL VALIDATION OF IDENTITY

This chapter describes the procedures used to identify the Subject or the Requestor upon their request for issuance of a qualified certificate.

The identification procedure requires the Subject to be recognised by the CA, including through a possible RA or a person mandated by the latter, which verifies their identity by means of the procedures defined in the Operating Manual.

3.2.1 Method of proving possession of the private key

Cedacri establishes that the Requestor possesses or controls the private key corresponding to the public key to be certified by verifying the signature with the public key to be certified.

3.2.2 Authentication of the identity of organisations

N/A

3.2.3 Identification of a natural person

Before being able to proceed with the actual issuance of the certificate, the Subject's data have to be stored in the Certificator's archives. This process is carried out by the QTSP, by means of the operator dedicated to the function of Registration Authority Operator (RAO), and is performed as follows:

- The Requestor contacts the company through dedicated channels (email to servizifiduciari-cedacri@iongroup.com or trouble ticketing system), to obtain an appointment with a Cedacri RAO in order to issue the Certificate;
- The RAO carries out the recognition of the user in accordance with the regulations in force;
- The RAO produces the contractual documentation based on the predefined request form, which is filled out with the personal data of the user; the documentation is signed for acceptance by the user;
- The RAO connects to the Cedacricert system and, using an internal connection, performs the authentication in the system;
- The RAO carries out the registration by inserting the Requestor's personal data, plus all the information necessary for the subsequent management thereof.

As defined in Article 24 of the eIDAS Regulation, when issuing a qualified certificate for a trust service, the QTSP verifies, using means that are appropriate and in compliance with national law, the identity and, where necessary, any specific attributes of the natural person to whom the qualified certificate is issued. The information is verified by the QTSP directly by means of the concrete presence of the natural person.

The RAO must accept that the Requestor has provided all information necessary for the identification, supported by suitable documentation.

The request form for the qualified certificate contains both data relating to the Subject's identity and information that makes it possible to manage the relationship between the QTSP and the Subject.

The essential data for the issuance of the certificate that the Requestor must provide are as follows:

- Surname and Forename
- Date and Place of Birth
- Tax ID
- Residence address
- Email address

It is also essential to verify the presence of a currently valid identity document and the Requestor's tax ID.

In the event that use of a pseudonym is requested in the certificate in lieu of real data, Cedacri, as the QTSP, shall store the information relating to the Requestor's real identity for 20 years.

If it is requested, directly by the Requestor, or with the consent of any Interested Third Party, that the certificate include information relating to Roles, Titles and/or Professional Qualifications and Powers of Representation, the RAO must accept that the Requestor, in addition to the necessary documentation and identification information, has also

produced suitable documentation to prove the actual existence of the specific role, including by proving it through self-certification.

The company name or the name and identification code of the Organisation shall be included in the certificate if the latter has requested or authorised the issuance of the certificate to the Subject, including without explicit indication of a role.

As regards the inclusion in the certificate of limitations of value that indicate a limitation of value for unilateral deeds and contracts for which the certificate may be used, without prejudice to the responsibility of the QTSP, it remains the responsibility of the Requestor to verify compliance with the limitations of use included in the certificate.

The request to insert other specific limitations of use must be assessed by the QTSP for legal, technical and interoperability aspects.

Without prejudice to the responsibility of the CA, the identity of the Subject can be ascertained by subjects authorised to carry out recognition, by means of the following procedures.

3.2.4 Identification of a legal person

N/A

3.2.5 Non-verified information about the Subject or Requestor

N/A

3.2.6 Validation of the authority

Cedacri or the RA verifies the information required, as defined in paragraphs 3.2.3 and 3.2.4, for the identification and validate the request.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RENEWAL OF KEYS AND CERTIFICATES

This paragraph describes the procedures used to authenticate and identify the Subject in the event of renewal of the qualified signature certificate.

The period of validity of the Certificate is that which falls within the interval of time specified by the Certificate fields “Valid from” and “Valid to”: the first indicates the date and time of the start of the validity, while the second states the date and time of the end of the validity.

Certificates issued by Cedacri S.p.A. - Servizio Cedacricert have a validity of no greater than three years.

Subjects intending to renew their Certificate must file a request with the QTSP at least 30 days prior to the expiry of the Certificate in their possession. Said request must be signed with the currently valid keys, in such a way that the QTSP is able to verify the identity of the Requestor. The Subject shall be notified of the successful renewal of the Certificate by email sent to the most recently communicated email address.

Once the new Certificate has been received, the private key relating to the old Certificate must no longer be used.

The old Certificate shall be stored, as of its expiry date, in the QTSP's archives for 20 years.

Once the validity period of the Certificate has lapsed, it is no longer possible to renew it, and the Requestor must instead carry out a new registration.

3.4. IDENTIFICATION AND AUTHENTICATION FOR THE REQUEST FOR REVOCATION OR SUSPENSION

3.4.1 Request for Suspension

Suspension can take place at the request of the Subject, or on the initiative of the QTSP, or at the request of an Interested Third Party.

The suspension of a digital certificate can become necessary in the event that the certificate has to be revoked as a precaution (for example, if there is a possibility, but no certainty, of the loss of control of one or more data items for the use of the digital signature service).

Suspension can take place at the request of the Subject, or on the initiative of the QTSP, or at the request of an Interested Third Party, by filling out and signing the form.

Once suspended, the Certificate shall remain in that state for a maximum period of 90 (ninety) days, at the end of which period, if not yet restored, the Certificate shall be automatically and definitively revoked.

The procedures for the suspension of the Certificate are exactly the same as those described for the revocation thereof.

3.4.2 Request for Revocation

The Subject may request the revocation of the Certificate for one of the following reasons:

- the private key has been compromised, or one of the following cases is present:
- the secure signature device that contains the key has been lost;
- the key or its activation code (PIN) is no longer secret;
- an event has occurred that has compromised the level of reliability of the key;
- the Subject is no longer able to use the secure signature device in their possession (e.g. damage to the device).

In the event that the Subject submits the revocation request by filling out and signing the revocation form, the RAO, having ascertained that the form has been correctly filled out and signed, connects to the qualified certificate management site and revokes the Certificate as requested.

In the event of revocation by phone, the Certificate shall be temporarily suspended for six consecutive calendar days, pending the delivery by the Subject of the revocation form, duly filled out and signed. In this case, the revocation shall apply as of the date of suspension.

When the revocation is carried out, the Certificator automatically published the Certificate in the CRL and notifies the Subject that the revocation has taken place.

4. FUNCTIONALITY

4.1. CERTIFICATE REQUESTS

4.1.1 Who can request a certificate

The qualified certificate for a natural person can be requested by:

- the Subject, by applying directly to Cedacri using the contacts detailed on the website www.cedacricert.it or by applying to a Registration Authority (where applicable);
- the Requestor on behalf of the Subject, by applying directly to Cedacri using the contacts detailed on the website www.cedacricert.it or by applying to a Registration Authority (where applicable).

4.1.2 Registration process and responsibilities

The registration process comprises: the request by the Subject, the generation of the pair of keys, the request for certification of the public key and the signature of the agreements, not necessarily in that order. In the process, the various actors have different responsibilities and jointly contribute to the successful outcome of the issuance:

- **The Subject** is responsible for providing accurate and truthful information about their identity, carefully reading the material made available by Cedacri, including through the RA, and following the instructions issued by the CA and/or the RA when making their request for a qualified certificate. When the Subject is a legal person, these responsibilities fall upon the legal representative or person granted power of attorney who is requesting the qualified certificate;
- **The Requestor**, where present, is responsible for informing the Subject, on behalf of whom they are requesting the certificate, of the obligations arising from the certificate, providing accurate and truthful information about the identity of the Subject, and following the processes and instructions issued by the CA and/or the RA;
- **The Registration Authority**, where present (including through the Person in Charge of Registration), is responsible for identifying the Subject and the Requestor with certainty, informing the various subjects of the obligations arising from the Certificate, and following the processes defined by the CA in detail.
- **The Certification Authority** is ultimately responsible for identifying the Subject and for the successful outcome of the qualified certificate registration process.

4.2. PREPARATION OF THE REQUEST

The main purpose of the enrolment process is to issue the Certificate.

To that end, the Subject and/or the Requestor must:

- read this Operating Manual, the contractual documentation and any additional informative documentation;
- follow the identification procedures adopted by the QTSP, as described in paragraph 3.2.3;
- provide all information necessary for identification, supported, where necessary, by suitable documentation;
- sign the registration and certification request, accepting the contractual terms and

conditions governing the provision of the service, using the dedicated paper or electronic forms prepared by the CA.

4.2.1 Information that the Subject must provide

When requesting a qualified signature certificate, the Subject or Requestor requesting a certificate for a natural person must provide the following information:

- Surname and forename;
- Date and place of birth;
- Tax ID or equivalent identification code (TIN);
- Residence address;
- Details of recognition document presented for identification, e.g. type, number, issuing body and issue date;
- Email address for the CA to send communications to the Subject;

Optionally, the Subject (or the Requestor) may provide another name, by which they are commonly known, which will be inserted into a dedicated 'Common Name' field of the Certificate. If no additional name is provided by the Subject or the Requestor, the Common Name field shall be filled out with the forename and surname of the Subject.

4.2.2 Execution of the functions of identification and authentication

After the registration phase has been completed, the RAO begins the procedure of generating the pair of keys and issuing the Certificate.

The procedure consists of allowing the Subject to personalise the device's secret PIN and PUK codes, carrying out the necessary operations to create the pair of keys, uploading the relevant Certificate to the signature device.

Cedacri ensures that the signature PIN is selected autonomously by the Subject, and it is the responsibility of the latter (or of the Requestor) to remember the PIN.

4.2.3 Approval or rejection of the certificate request

After the initial registration, Cedacri may refuse to complete the issuance of the signature certificate in the event of the absence or incompleteness of information, checks on the coherence and consistency of the information provided, anti-fraud checks, doubts about the identity of the Subject or the Requestor, etc.

4.2.4 Maximum time for preparation of the certificate request

The period of time between the moment the registration request is made and the moment the Certificate is issued depends on the request procedure selected by the Subject (or Requestor) and on the possible need to collect additional information or to physically deliver the device.

4.3. ISSUANCE OF THE CERTIFICATE

4.3.1 Actions of the CA during issuance of the certificate

Issuance of the certificate on a signature device (smartcard or token)

The pair of cryptographic keys is generated by the RA directly on secure signature devices, using the applications made available by the CA, subject to secure authentication.

The RA sends the CA the request for certification of the public key in PKCS#10 format, signed digitally with the qualified signature certificate specifically authorised to that end.

The CA, having verified the validity of the signature on the PKCS#10 and the Subject's capacity to make the request, proceeds to generate the qualified certificate, which is sent via a secure channel within the device.

Issuance of the certificate on a remote signature device (HSM) for automatic signature

The Subject or the Requestor obtains authentication for the services or applications made available by the CA or RA.

The pair of cryptographic keys is generated by the RA directly on the HSM; the RA then sends the CA the request for certification of the public key in PKCS#10 format, which is digitally signed with the qualified signature certificate for automatic signature specifically authorised to that end.

The CA, having verified the validity of the signature on the PKCS#10 and the Subject's capacity to make the request, proceeds to generate the qualified certificate, which is stored on the HSM.

4.3.2 Notification to requestors that the certificate has been issued

In the event of issuance on a cryptographic device, the Subject (or the Requestor) does not need to be notified, since the certificate is present on the device that they have received.

4.3.3 Activation

In both cases cited in paragraph 4.3.1, the QTSP operates in such a way as to carry out the Certificate activation phase during the registration phase, which takes place at Cedacri's offices for RAO activities.

4.4. ACCEPTANCE OF THE CERTIFICATE

4.4.1 Conduct implying intent to accept the certificate

N/A

4.4.2 Publication of the certificate by the Certification Authority

The certificate is made public immediately after the completion of the registration phase and the issuance of the keys by the QTSP on the signature device.

4.4.3 Notification to other subjects that the certificate has been published

N/A

4.5. USE OF THE PAIR OF KEYS AND THE CERTIFICATE

4.5.1 Use of the private key and the certificate by the Subject

The Subject must store the signature device securely. Specifically, for the token, the Subject:

- must keep the information required to use the private key separate from the device;
- must ensure that the emergency code needed to suspend the certificate is stored and kept secret, and must use the certificate exclusively for the purposes provided for by the Operating Manual and by the national and international laws in force;
- must not affix electronic signatures using private keys for which the certificate has been revoked or suspended, and must not affix electronic signatures using a certificate issued by a revoked CA.

4.5.2 Use of the public key and the certificate by End Users

The End User must be familiar with the scope of use of the certificate, as set out in the Operating Manual and in the certificate itself. They must verify the certificate before using the public key contained therein and and check that the certificate has not been suspended or revoked by monitoring the relevant lists in the certificate register. They must also verify the existence and the content of any limitations of use of the pair of keys, powers of representation and professional qualifications.

To that end, Cedacri makes a free of charge tool available to its customers. This tool allows users to affix and verify digital signatures in standard format, and to request and verify time stamps.

Releases of operating systems compatible with the Cedacricert service, as well as the document containing instructions for the generation and verification of the digital signature, can be found on the official Cedacricert. website.

4.5.3 Limitations of use and value

Qualified signature certificates for automatic signature contain the limitation of use provided for by the Supervisory Authority, and additional Certificate Policies, identified by the following OIDs:

1.3.76.27.1.1.1.3	The certificate may only be used for unattended/automatic digital signature. The certificate may only be used for unattended/automatic digital signature.
1.3.76.27.1.1.1.1	The certificate holder must use the certificate only for the purposes for which it is issued. The certificate holder must use the certificate only for the purposes for which it is issued.

1.3.76.27.1.1.1.2	The certificate may be used only for relations with the (declare the subject). The certificate may be used only for relations with the (declare the subject).

The Subject or Requestor also has the option to ask the QTSP to insert personalised limitations of use into the certificate. The request to insert other specific limitations of use shall be assessed by the QTSP for legal, technical and interoperability aspects and actioned accordingly.

The Subject also has the option to ask the QTSP to insert limitations of value into the certificate that indicate a limitation of value for unilateral deeds and contracts for which the certificate may be used. The values must be expressed as positive whole numbers, with no decimals.

The QTSP is not liable for damage resulting from the use of a qualified certificate that exceeds the limitations imposed thereby or resulting from exceeding the limitation value.

Without prejudice to the QTSP's responsibility pursuant to the Digital Administration Code (Article 30, paragraph 3), it is the Subject's responsibility to verify compliance with the limitations of use and value inserted into the certificate.

For the new CA EJBCA, however, the limitation of use provided for by the Supervisory Authority, and additional Certificate Policies, is identified by the following OIDs:

1.3.76.27.1.1.2.3	The certificate may only be used for unattended/automatic digital signature.
1.3.76.27.1.1.2.1	The certificate holder must use the certificate only for the purposes for which it is issued.

4.6. RENEWAL OF THE CERTIFICATE

4.6.1 Reasons for renewal

Renewal allows the Subject to obtain a new signature certificate that can be used to sign documents and transactions.

4.6.2 Who can request a renewal

The Subject can request the renewal of the certificate prior to its expiry, only if it has not been revoked and if all the information provided upon the previous issuance is still valid; after the expiry date, it will not be possible to carry out the renewal, and the Subject will have to request a new certificate instead. The renewal procedure applies exclusively to certificates issued by Cedacri.

Certificates for automatic signature cannot be renewed, so subjects will have to request the issuance of a new certificate.

Certificates issued to a legal person cannot be renewed, so subjects will have to request the issuance of a new certificate.

4.6.3 Preparation of the request to renew the certificate

Renewal involves the reissuance of the certificate by the CA, but under favourable terms and conditions for the end customer.

4.7. REISSUANCE OF THE CERTIFICATE

The reissuance of the certificate takes place when – following a revocation - the Subject or the Requestor makes a request for issuance.

4.8. MODIFICATION OF THE CERTIFICATE

In case of changes in the data within the certificate, no changes can be made in any way. The certificate, as stated in Section 4.9.1 item 3, must be revoked and reissued with the corrected data.

4.9. REVOCATION AND SUSPENSION OF THE CERTIFICATE

The revocation or suspension of a certificate cancels the validity thereof prior to the established expiry date, and renders invalid any signatures affixed after the publication of the revocation. Certificates that have been revoked or suspended are inserted into a revocation and suspension list (CRL) signed by the CA that issued them, which is published in the certificate register according to a timetable determined by the CA (every eight hours). The CA may also issue an unscheduled CRL in certain specific circumstances. The revocation or suspension takes effect from the moment the list is published, using as a reference the date indicated in the CA's Monitoring Log.

4.9.1 Reasons for revocation

The conditions under which a request for revocation must be made are as follows:

1. the private key has been compromised, or one of the following cases is present:
    a. the secure signature device that contains the key has been lost;
    b. the key or its activation code (PIN) is no longer secret;
    c. an event has occurred that has compromised the level of reliability of the key;
2. the Subject is no longer able to use the secure signature device in their possession (e.g. damage to or deterioration of the device);
3. there is a change to the Subject's data present in the certificate, including data relating to the Role, which renders said data no longer correct;
4. the relationship between the Subject and the CA, or between the Requestor and the CA, comes to an end.
5. the conditions set out in the Operating Manual cease to apply.

4.9.2 Who can request revocation

Revocation can be requested by the Subject at any time and for any reason. The revocation of the certificate can also be requested by the Requestor, for the reasons and subject to the procedures set out in this Operating Manual and, lastly, the certificate can be officially revoked by the CA.

4.9.3 Procedures for requesting revocation

The revocation request can be made using various different procedures, depending on the Subject that carries it out.

Revocation requested by the Subject

The Subject is required to sign the revocation request, using the form present on the website www.cedacricert.it and deliver it personally to the RA or send it directly by recorded-delivery mail, certified email or fax, supported by a photocopy of a currently valid identity document.

The QTSP verifies the authenticity of the request and revokes the certificate, notifying the Subject or the Requestor immediately.

If the certificate which is the subject of the revocation request contains information relating to the Subject's Role, the QTSP shall inform any Interested Third Party with which specific contractual conditions are in place that the certificate has been revoked.

If, on the other hand, the certificate for which the revocation is being requested indicates the Organisation, the QTSP shall inform said Subject that the revocation has taken place.

Revocation requested by the Requestor or Interested Third Party

The Requestor may request the revocation of the Subject's certificate by filling out the relevant form, which is available on the website www.cedacricert.it, providing the reason for the request, attaching the relevant documentation, if present, and specifying the data of the Subject of the certificate communicated to the QTSP at the time of issuing the certificate.

The QTSP shall verify the authenticity of the request, communicate it to the Subject via the communication channels established when requesting the certificate, and revoke the certificate.

Revocation at the initiative of the Certification Authority

The QTSP, if the need arises, has the option to revoke the certificate, notifying the Subject of the revocation in advance and providing the reason for the revocation, as well as the date and time when it will take effect. The QTSP can autonomously revoke the unexpired certificate – for example - if the certificate is no longer compliant with the CP for which it was issued or in general when the QTSP becomes aware of changes which affect the validity / security of the certificate itself.

If the QTSP finds that the certificate which is the subject of the revocation request contains information relating to the Subject's Role, it shall inform any Interested Third Party with which specific contractual conditions have been agreed that the certificate has been revoked.

If the certificate for which the revocation is being requested also indicates the Organisation, the QTSP shall inform said Subject that the revocation has taken place.

4.9.4 Grace period for the revocation request

The grace period for the CRL is the period of time between the publication of the subsequent CRL and the expiry of the current CRL. So as not to cause disruptions to any party involved, this period is longer than the period of time that the CA needs to generate and publish a new CRL. Thus, the current CRL remains valid at least until it is replaced by the new CRL. This grace period shall not exceed 24 hours, in any event.

4.9.5 Maximum time for preparing the revocation request

The request is processed within 12 hours of the operator taking charge of it, provided that no further checks on the authenticity of the request are necessary.

4.9.6 Frequency of publication of the CRL

Revoked or suspended certificates are inserted into a revocation and suspension list (CRL), signed by the QTSP, and published in the public register. The CRL is published according to a schedule every eight hours (ordinary issuance), but the CA may, in specific circumstances, force an unscheduled issuance of the CRL (immediate extraordinary issuance), in the event that, for example, the revocation or suspension of a certificate takes place due to the suspected compromising of the secrecy of the private key (immediate revocation or suspension).

The time of publication of the CRL is attested using the date provided by the Cedacri Time Stamping Authority system as a time reference, and this is recorded in the monitoring log. Each item on the CRL has a dedicated extension containing the date and time of revocation or suspension.

Acquisition and consultation of the CRL is the responsibility of users, who may download it by going to the Cedacricert website. The CRL to be consulted for the specific certificate in question is indicated on the certificate itself, in accordance with the rules in force.

4.9.7 Maximum latency of the CRL

The maximum waiting time between the revocation or suspension request and its execution via publication of the CRL is eight hours.

4.9.8 Online service for verifying the certificate's revocation status

In addition to the publication of the CRL in the LDAP and HTTP registers (via the Cedacricert website), Cedacri also provides an OCSP service for verifying the certificate's status. The URL of the service is indicated in the certificate. The service is available 24/7.

4.9.9 Reasons for suspension

Suspension must be carried out if the following conditions apply:

1. a revocation request has been made without the possibility of ascertaining the authenticity of the request in time;
2. the Subject, the Requestor or Interested Third Party, the RA o the CA has acquired elements of doubt about the validity of the certificate;
3. a security problem has been identified;
4. a temporary interruption to the validity of the certificate is necessary.

In the aforementioned cases the suspension of the certificate shall be requested, specifying a period of time at the end of which the suspension can be followed either by a definitive revocation or by the reactivation of the certificate.

4.9.10 Who can request suspension

Suspension can be requested by the Subject at any time and for any reason. The suspension of the certificate can also be requested by the Requestor or the Interested Third Party, for the reasons and subject to the procedures set out in this Operating Manual, or the certificate can be officially suspended by Cedacri.

4.9.11 Procedures for requesting suspension

The suspension request can be made using various different procedures, depending on the Subject that carries it out. The suspension always has a limited duration. The suspension ends at midnight on the last day of the requested period.

Suspension requested by the Subject

The Subject must request suspension via one of the following methods:

1. by phoning the call centre and providing the information required to identify the certificate data;
2. the Subject is required to sign the suspension request and deliver it to the RA – Cedacri or send it directly to the CA by ordinary post, certified email or fax, supported by a photocopy of a currently valid identity document and tax ID.

If the CA finds that the certificate which is the subject of the suspension contains information relating to the Subject's Role, it shall inform any Interested Third Party with which specific contractual conditions have been agreed that the certificate has been suspended. If the certificate for which the suspension is being requested also indicates the Organisation, the CA shall inform said Subject that the suspension has taken place.

The CA shall verify the authenticity of the request, communicate it to the Subject via the communication channels established when requesting the certificate, and revoke the certificate.

Suspension requested by the Requestor or Interested Third Party

The Requestor or Interested Third Party may request the suspension of the Subject's certificate by filling out the relevant form, which is available on the website of the CA and from the RA, providing the reason for the request, attaching the relevant documentation, if present, and specifying the data of the Subject communicated to the CA at the time of issuing the certificate.

Cedacri shall verify the authenticity of the request, communicate it to the Subject via the communication channels established when requesting the certificate, and revoke the certificate.

Suspension at the initiative of the CA

Except in urgent cases, the QTSP notifies the Subject in advance of its intention to suspend the certificate, providing the reason for the suspension, the date it will take effect and the date it will end. This information shall, in any case, be communicated to the Subject as soon as possible.

If the QTSP finds that the certificate which is the subject of the suspension contains information relating to the Subject's Role, it shall inform any Interested Third Party with which specific contractual conditions have been agreed that the certificate has been suspended.

If the certificate for which the suspension is being requested also indicates the Organisation, the CA shall inform said Subject that the suspension has taken place.

4.9.12 Limitations on the suspension period

Upon the expiry of the suspension period requested, the validity of the certificate is restored through the removal of the certificate from the CRL. The reactivation takes place within the 24 hours following the end date of the suspension. If the expiry date of the suspension coincides with the expiry date of the certificate or is later than said date, the suspension is converted into a revocation, with effect from the beginning of the suspension.

It is possible to request the reactivation of the certificate prior to the end date of the suspension by sending the signed form, which can be found on the Cedacricert website, accompanied by a currently valid identity document. It can also be sent via certified email or fax.

4.10. Services concerning the certificate's status

4.10.1 Operational features

Information about a certificate's status can be obtained from the CRLs and the OCSP responder.

The serial number of a revoked certificate remains on the CRL even after the certificate's validity expires.

The information provided by the OCSP is updated in real time.

4.10.2 Availability of the service

The OCSP service is available 24/7.

4.10.3 Optional features

N/A

4.11. Termination of the CA's services

The relationship of the Subject and/or the Requestor with the Certification Authority ends when the certificate expires or is revoked, except in specific cases defined in accordance with specific contractual agreements between the parties.

4.12. Consignment to third parties and recovery of the key

Cedacri does not provide for the consignment of the key to third parties as part of the provision of this service.

5. SECURITY AND CONTROL MEASURES

All the safeguarding measures enacted by Cedacri S.p.A. are framed within the general context of the Security Manual, which provides the basic indications for management of the systems and the secure processing of data. The very existence of the Security Manual as a corporate document that is binding on the management constitutes the first safeguarding measure on the organisational front.

The general framework is supplemented by two instruments described in the Security Manual in which the application of the safeguarding measures is regulated:

- the Application Regulations, or Reference Manuals, which set forth and describe the safeguarding measures in the various contexts;
- the organisation of security personnel, with personnel dedicated to security and to privacy, as well as non-specialist personnel who perform accessory security and control functions.

This document is public and is available upon request to auditing-cedacri@iongroup.com

5.1. PHYSICAL SECURITY

All technical and logistical measures are put in place to prevent physical accidents and to protect the physical resources involved in the provision of the service, with regard to the following key aspects:

- Security of the perimeter;
- Physical access control;
- Security and safety of offices, premises and structures;
- Protection from external and environmental threats;
- Electricity supply and air conditioning;
- Network cabling and systems;
- Protection against fire;
- Protection against flooding;
- Procedures for storing magnetic storage media;
- Sites for storing magnetic storage media.

5.1.1 Position and construction of the structure

The Cedacri Data Centre is located in Collecchio (Parma), while the secondary site is situated at the office in Castellazzo Bormida (Alessandria) and is connected to the Data Centre; the two sites are interlinked by dedicated 10Gbps connections with different operators.

5.1.2 Physical access

Access to the buildings where CEDACRI carries out its operations is subject to rules setting down the relevant controls, modalities and management responsibilities.

The external perimeter of the

CEDACRI buildings is protected by a passive intrusion detection system, whereas the perimeter of the buildings is protected by and active intrusion detection system.

The access system for external staff includes the identification, registration and issuance of a badge at the reception desk, with a 24/7 presence and control.

A closed-circuit television system, with monitors at the reception desk, allows visual surveillance, including at night, of the outdoor areas of the Company complex.

The doors that are not used to enter the buildings (and specifically those used as emergency exits) are alarmed.

All points of entry from the outside are protected with doors and turnstiles that can be opened with a badge.

Inside the buildings, there are security areas that are subject to restricted access with doors that can be opened with a badge and PIN (e.g. Control Room, Machinery Room, CA Rack, Robot Room), which contain all the systems that combine to provide the digital signature service.

In compliance with the general principles of physical security, specific rules are set down for the delivery and collection of goods and materials.

5.1.3 Electrical and climate-control equipment

In compliance with the technical and operating standards indicated with regard to Tier III (Concurrently Maintainable Site Infrastructure) in the paragraph headed “Tier Performance Standards” of the document published by the Uptime Institute and headed “White Paper – Tier Classification Define Site Infrastructure Performance”, the main site in Collecchio and the secondary site in Castellazzo Bormida have achieved substantial compliance with the standard, as attested by the report issued by an inspector certified by the Uptime Institute as Accredited Tier Designer (certified ATD Number 250 Uptime Institute).

The technical premises are equipped with an electricity supply system designed to prevent faults and, above all, disruptions. The system supply includes the latest technology, with a view to increasing the reliability and ensuring the redundancy of the most critical functionalities for the purposes of the services provided.

The electricity supply to the Machine Room uses a dual supply by means of two different generation systems (Enel, emergency electrical generators, inverters, buffer batteries, etc.), which means that, in the event of the failure of one station, the other is able to fully support the entire load of the Machine Room.

The main system and facility features of the spaces are:

- Redundant supply derived from:
    a. Independent substations with availability to support the full load of the machine room;
    b. Redundant continuity generators for the individual substation (in the event of failure of a UPS, the other generators support the full load);
    c. Systems using fully independent privileged dual supply;
    d. Systems using a privileged single supply;
- Switch supplies;
- Continuity generators subject to 24-hour monitoring with the LIFE system from a specialist centre;
- Conditioning carried out with redundant direct expansion equipment, for both the electricity supply and the thermal power of the individual machine;
- Primary and emergency lighting.

Each technology cabinet installed at the data centre has two electrical lines that ensure high availability (HA) in the event of the interruption of one of the two available lines.

The technology cabinet is monitored remotely; constant checks are carried out on the status of the electricity line (on/off) and the electrical power absorbed (each line must not exceed 50% of the load).

The technical area is normally kept at between 20° and 27°, with a relative humidity ratio of between 30% and 60%. The systems are fitted with condensing batteries with a sealed condensation collection and release system controlled by anti-flooding probes. The entire conditioning system is equipped with emergency generators in the event of a lack of electricity. Each cabinet has a cooling capacity with a maximum load of 10KW, and a maximum of 15KW for two cabinets side by side.

5.1.4 Prevention of and protection against flooding

With regard to possible flooding, there are two submerged water pumps with electricity supply and connection to the continuity generators, as well as a water pump with an autonomous supply (diesel).

The operational staff are trained in the use of accident intervention measures, based on the provisions of Legislative Decree 81/2008.

5.1.5 Prevention of and protection against fire

The reserved areas in which the qualified digital signature service systems are located are subject to fire and flood prevention measures and, more generally, as regards physical accidents:

- they do not contain paper or flammables, or readily combustible fixtures and fittings, or unprotected electrical cables; the potential fire load is reduced to the minimum;
- there are no gas tanks there, and there are local fire extinguishment systems;
- the underfloor is kept clean with periodic interventions and the electrical connections that pass through it comply with Decree no. 37 [13] of the Ministry of Economic Development of 22 January 2008.

The entire C2 building is protected by a smoke detection system consisting of eight detectors.

Each floor of the building is fitted with UNI 45 hydrants (located close to the internal stairwells), which are perfectly equipped and maintained in accordance with the applicable regulations, namely UNI EN 14384:2006, UNI EN 14339:2006 UNI EN 14540:2006 and UNI 9487:2006 [15].

Various portable extinguishers are installed; their number and location make them sufficient to provide a first intervention, and they are perfectly equipped and maintained.

The Server Room in the reserved area of the C2 building also has an automatic fire extinguishment system in operation, with an NAF S3 extinguisher, which is capable of protecting the entire reserved area.

All the details of the detection and extinguishment systems are listed in the documentation “Fire Risk Assessment”, drawn up by Cedacri S.p.A. as provided for by Ministerial Decree 10/3/98, and in the relevant documentation on “General criteria for anti-fire security and emergency management in the workplace” (Legislative Decree 81/2008).

Staff are not usually to be found in the area. In the event of the detection of a fire, it is reported to the Internal Surveillance Unit, which is present 24/7.

5.1.6 Means of storage

As regards the storage platform, the solution in place involves the use of NetApp systems for NAS. For SANs, on the other hand, an infrastructure is in place based on HDS technologies, comprising VSP and G1000 platforms, with no virtualisation layer in the storage systems.

5.1.7 Provisions on the decommissioning of equipment

Cedacri adopts a policy of separated collection and sustainable disposal of waste. As regards the information content of electronic waste, Cedacri uses companies specialised in the disposal of special waste, and ensures that all media are cleaned in accordance with the procedures set forth for data and information security, rendering them completely unusable, and that said storage means are disposed of in a sustainable way.

5.1.8 Off-site backup

This is carried out at the disaster recovery site at the Castellazzo Bormida premises.

5.2. PROCEDURAL CONTROLS

5.2.1 Key roles

Cedacri defines, and keeps updated, procedures that represent the procedures for managing corporate processes, setting out roles and responsibilities and defining adequate controls in order to reduce the risk of accidental or deliberate misuse of the information system and the information itself.

In compliance with the Presidential Decree of 22 February 2013, Cedacri stipulates at least the following professional figures:

a) head of security;

b) head of the time stamping and certification service;

c) head of technical management of the systems; d) head of technical and logistical services;

e) head of checks and inspections (auditing).

Cedacri has assigned the aforementioned roles to internal personnel with accrued professional experience and a high level of technical skill and, in accordance with the Presidential Decree of 22 February 2013, Article 38, guarantees that roles a) and e) are assigned to different individuals.

5.3. STAFF SCREENING

CEDACRI considers human resources as a key and indispensable component of its business.

At all levels of the organisation, staff are subject to a process for assessment and development of skills, as well as information, training and awareness-raising regarding information security.

Moreover, the terms of liability, for security and/or legal matters, shall be set, which extend to a period after the termination of the work contract (for example, obligations concerning confidentiality and intellectual property).

Refer to document XQ99Q880 Management of Human Resources which describes the human resource management process starting from the selection phase, the period of permanence in the company and any changes in role, up to the phase of termination of the employment relationship.

5.3.1 Qualifications, experience and authorisations required

Refer to document XQ99Q880 Management of Human Resources.

5.3.2 Procedures for checking previous experience

Refer to document XQ99Q880 Management of Human Resources

5.3.3 Training requirements

Refer to document XQ99Q880 Management of Human Resources.

5.3.4 Frequency of training updates

Refer to document XQ99Q880 Management of Human Resources

5.3.5 Frequency of work shift rotation

In order to ensure that the service provided complies with quality requirements and service levels, Cedacri has a Control Room that operates 24/7, in shifts.
As a result of this need to guarantee the presence of qualified and competent staff, the structure of the working hours of the Control Room shift staff guarantees 24-hour coverage from Monday to Sunday, using the following shifts:

- · Morning;
- · Afternoon;
- · Night.

The other Cedacri structures follow split working hours, without shifts.

5.3.6 Sanctions for unauthorised actions

Upon recruitment, CEDACRI employees are informed of the employment contract conditions and specifically of the corporate rules on security, ethics and privacy, and they sign the Company “Code of Conduct” for acceptance.

Confidentiality clauses and obligations of the employees are specified also in the applicable Italian national collective bargaining agreement for the sector.

Refer to document XQ99Q880 Management of Human Resources

5.3.7 Checks on non-employee staff

Although Cedacri assigns the key roles for the provision of the qualified digital signature service to internal staff, the company has relations with suppliers which are leading companies operating in the sector of ICT supplies, such as hardware, software, TLC equipment, data and energy transmission, technology systems, and security technologies and services. Moreover, Cedacri has set down and implements rigorous procedures for the acquisition, management, acceptance and assessment of supplies from third parties that may impact the quality and security of the services it provides.

Specifically, confidentiality agreements are entered into with Suppliers/Providers, by signing supply/provision agreements, the “General Conditions of Supply/Provision” and NDAs (Non-Disclosure Agreements).

5.3.8 Documentation that staff must provide

Refer to document XQ99Q880 Management of Human Resources

5.4. AUDIT LOGGING

In compliance with ETSI EN 319 411-2 and the applicable regulations, the main events relating to the management of the certificates' life cycle are recorded, as are those relating to logical access to the systems, the operations performed by staff, and the entry and exit of visitors to the premises in which the certification activity is carried out.

For every event, the event type, date and time of occurrence is recorded and, if available, any other information that may be useful for identifying the actors involved in the event and the outcome of the operations.

These records are known collectively as the 'audit log'. The files that make up the log are periodically transferred to a permanent means of storage.

The integrity of the audit log is guaranteed by transferring and storing the log in the corporate log management system (Splunk). It is then archived and stored for a period of no less than 20 years.
The date/time inserted as a time reference in each record pertaining to the audit log is maintained in line with the exact time (UTC).

5.4.1 Frequency of audit log processing and storage

The processing and grouping of the data, as well as storage thereof in the storage system, usually takes place on a monthly basis.

5.4.2 Storage period of the audit log

The audit log is stored for 20 years.

5.4.3 Protection of the audit log

The audit log is kept in such a way as to guarantee the authenticity of the annotations and to permit the reconstruction, with the necessary accuracy, of all significant events. Logical access is strictly limited to those in charge of the relevant work, in accordance with need-to-know policies.

5.4.4 Backup period of the audit log

Suitable copies of the audit log are prepared, in accordance with the corporate policies in place.

5.4.5 Storage system of the audit log

The audit log data are collected via ad hoc automatic procedures and periodically transferred to the corporate log management system, which guarantees their integrity, among other aspects.

5.4.6 Vulnerability assessments

Cedacri implements and maintains a vulnerability management process that makes it possible to:

- Manage any vulnerability detected by the regular scans of the systems in an effective way;
- Assign correct priority to remediation actions by weighing the vulnerability seriousness against the business criticality of the system on which the threat has been identified;
- Monitor the risk exposure status of the internal/external systems having regard to any known vulnerability;
- Improve the systems' security;
- Control the implementation of the remediation plan;
- Ensure that useful information be managed and stored in the appropriate way;
- Produce suitable reporting for external audits.

5.4.7 Notification in the event of identification of vulnerability

The corporate security incident management process is applied (see paragraph 5.7.1).

5.5. ARCHIVING OF DATA

In accordance with Regulation ETSI EN 401, chapter 7.10, the QTSP stores the following information relating to the certificate issuance and management processes:

- issuance requests
- documentation provided by requestors
- certificate signing requests (CSRs) provided by requestors
- personal data of requestors and holders (where they are different)
- suspension or revocation requests
- all certificates issued

The aforementioned data are stored for at least 20 years after the certificates' expiry date.

5.6. REPLACEMENT OF THE CA PRIVATE KEY

At least 90 days prior to the certificate's expiry, the Certificator begins the replacement procedure for the pair of certification keys, generating a new pair of keys, in compliance with the terms provided for by the aforementioned Presidential Decree.

Each replacement shall require a change to this manual and communication to the Supervisory Authority (AgID).

5.7. COMPROMISING OF THE CA PRIVATE KEY AND DISASTER RECOVERY

5.7.1 Incident management procedures

Despite having made available all measures for information safeguarding and security in relation to the digital signature service (e.g. backup, high-availability servers and secondary-site disaster recovery), Cedacri has activated procedures that describe the

methods of reporting events relating to information security, the classification thereof, the launch of the incident response plan and the gathering of evidence.
Incident is notified to the Supervisory Authority (AgiD) according to the methods shared by the Agency through the portal (https://trustservices.agid.gov.it).

5.7.2 Corruption of machines, software or data

In the event of damage to the HSM secure signature device containing the certification keys, the reserve copy of the certification key is used, which is suitably saved and stored at the secondary site in Castellazzo, and there is no need to revoke the corresponding CA certificate. In all cases, such incidents are treated as critical security incidents (see previous paragraph).

The software and data are subject to frequent backups, as required by internal procedures.

5.7.3 Procedures in the event that the CA private key is compromised

The Certificate can be revoked at the initiative of the QTSP in the event of suspicion or certainty that the CA private key has been compromised, in which case it shall carry out the following activities:

- inform the Subject about the revocation in advance, stating the date and time when it will take effect;
- revoke the Certificate and publish the CRL;
- update and inform the Subject and RA at the same time.

In all cases, the communication takes place via email to the address most recently communicated by the Subject.

5.7.4 Provision of CA services in the event of disaster

CEDACRI has set up an internal structure that is responsible for the implementation of all preventive measures in order to achieve the disaster recovery objective.

The plan, which applies to the primary processing site in Collecchio, provides for redundant systems to be deployed in order to meet the requirements for system availability as set down by the relevant contracts, and the restoration of processing services at the disaster recovery site, located at a distance of over 200 km from the primary processing site.

The operational continuity plan describes, at organisational and process level, the measures implemented by Cedacri to declare a disaster, manage it and return to a state of normality.

5.8. Termination of the CA or RA service

In the event of termination of the activity, Cedacri shall:

- at least 60 days before the exact termination date of the service, communicate this intention to the Supervisory Body (AgID) and CAB;
- at least 60 days before the exact termination date of the service, notify any third parties or delegated RA;
- at least 60 days notice, communicate the replacement QTSP to all customers

and publish an information note on the cedacricert website with all the necessary details;

- in the event that there is no substitute QTSP, notify all customers that the certificates issued and not yet expired on the date of termination will be automatically revoked;
- in the event that there is no substitute QTSP, arrange for all the necessary documentation to be filed with AgID within 30 days, which guarantees its preservation and availability;
- transfer to the QTSP substitute all the preservation of the evidence (log, control journal, request for the issuance of certificates, etc.) and transfer to this entity the responsibility to publish on its website the public key of the ceased CA;
- on the date of termination, destroy all the private certification keys and the cryptographic material necessary for the restoration of the keys, stipulating a special report describing all the steps of this activity.

6. TECHNICAL SECURITY CONTROLS

6.1. INSTALLATION AND GENERATION OF THE PAIR OF CERTIFICATION KEYS

In order to carry out its activity, the QTSP needs to generate the pair of certification keys for signing the Subjects' certificates.

The keys are generated only by staff explicitly appointed to carry out that function. The generation of the keys and the signature takes place within dedicated and certified cryptographic modules, as required by the applicable regulations, in reserved physical areas where access is reserved exclusively for strictly authorised staff with a badge and PIN.

The generation of the keys within the signature devices is preceded by the initialisation of the signature devices used by the QTSP for the certificate generation system, with which the Subjects' certificates are signed.

Once the pair of keys has been generated, the private keys are stored on an HSM cryptographic signature device, access to which is permitted via smartcard.

In accordance with dual-control rules, the smartcards are stored in separate anti-tampering envelopes, in different strongboxes, which can be opened by a limited number of people.

One of the dedicated HSMs is kept in Collecchio and the other in Castellazzo, and in both offices the aforementioned smartcards are stored in dedicated strongboxes.

The CA private keys are duplicated, for the sole purpose of their recovery following the breakdown of the secure signature device, in accordance with a controlled procedure that provides for the key and the context to be divided across several devices, as provided for by the HSM device security criteria.

The cryptographic module used to generate the keys and the signature has prerequisites that make it possible to guarantee:

- that the pair of keys meets the requirements imposed by the generation and verification algorithms used;
- the equal probability of generating all possible pairs;
- the identification of the subject activating the generation procedure;
- that the generation of the signature takes place within the device in such a way that is is not possible to intercept the value of the private key used.

The activities referred to under the previous points shall be documented, and said document shall be stored by the QTSP for 20 years.

6.1.1 Generation of the Subject's pair of keys

The asymmetric keys are generated within a secure signature creation device (SSCD) or qualified signature creation device (QSCD) using the native functionalities offered by said devices.

In the event that the device is not made available to the QTSP, the requestor must ensure that the device complies with the regulations in force, presenting the relevant documentation and being subject to periodic audits.

6.1.2 Delivery of the private key to the Requestor

The private key is contained in the cryptographic device (QSCD).

With the delivery of the cryptographic device to the Subject, the latter comes into full possession of the private key, which it can use only by using the PIN, which is known exclusively to the Subject; this device is delivered as soon as the keys are generated.

6.1.3 Delivery of the public key to the CA

The signer creates a request in PKCS#10 format with the public key generated.

6.1.4 Delivery of the public key to the users

The public key is contained in the certificate issued exclusively to the requesting subject.

Accordingly, if the Requestor asks for it, it is also published in the public register, from where it can be recovered by the User.

6.1.5 Algorithm and length of the keys

The pair of asymmetric certification keys is generated within a cryptographic hardware device, as mentioned above. The RSA asymmetric algorithm is used, with keys with a length of no less than 4,096 bits.

For the Subject's keys, the asymmetric cryptographic algorithm used is the RSA algorithm, and the length of the keys is no less than 2,048 bits.

6.1.6 Controls on the quality and generation of the public key

The devices used are certified in accordance with high security standards (see paragraph 6.2.1) and guarantee that the public key is correct and random. Before issuing the certificate, the CA verifies that the public key has not already been used.

6.1.7 Purpose of use of the key

The purpose of use of the private key is determined by the KeyUsage extension, as defined in standard X509. For the certificates described in this operating manual, the only permitted use is "*non-repudiation*", i.e. they can be used exclusively for signing.

6.2. PROTECTION OF THE PRIVATE KEY AND ENGINEERING CHECKS ON THE CRYPTOGRAPHIC MODULE

6.2.1 Controls and standards for the cryptographic module

The cryptographic modules used by Cedacri for the certification (CA) keys and for the OCSP responder are validated FIPS 140 Level 3 and Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) EAL 4 + with AVA_VAN.5.

The smartcards used by Cedacri are validated Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 an AVA_MSU.3) or EAL5 Augmented by ALC_DVS.2 , AVA_VAN.5 .

The cryptographic modules used by Cedacri for the Subject's automatic signature keys are validated FIPS 140 Level 3 and Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4.

6.2.2 Controls on more than one person for the CA private key

Access to the devices containing the certification keys can take place only with two people authenticated at the same time.

6.2.3 Consignment of the CA private key to third parties

N/A

6.2.4 Backup of the CA private key

The backup of the keys is contained in four different strongboxes, located in different offices at different sites, access to which is permitted only to staff who do not have access to the HSM devices. Any recovery therefore requires the presence of both staff with access to the devices and those with access to at least two strongboxes.

6.2.5 Archiving of the CA private key

N/A

6.2.6 Transfer of the private key from or to a cryptographic module

The private key is not stored unencrypted, and the QTSP can export it exclusively for backup reasons.

6.2.7 Storage of the private key on a cryptographic module

The certification key is generated and stored in a protected area of the cryptographic device, which prevents it from being exported. Moreover, in the event that the protection is forced, the device's operating system either blocks the device or renders it unreadable by deleting its content.

6.2.8 Method of activating the private key

The private certification key is activated through dual-control access to the cryptographic device containing the cryptographic material.

6.2.9 Method of deactivating the private key

For the deactivation of the CA private key, the HSM deactivation rules apply.

For the automatic signature service, the HSM must deactivate the keys when, for example, there is an electricity supply failure or the connection to the signature application shuts down unexpectedly. Keys thus deactivated can be reused only after a new authentication of the signer for the device.

6.2.10 Method of destroying the CA private key

The Cedacri staff appointed to this role must destroy the private key when the certificate has expired or been revoked, in accordance with the security procedures provided for by

the corporate security policies and the provisions set out in the policies of the supplier of the security equipment (HSM).

6.2.11 Classification of cryptographic modules

N/A

6.3. OTHER ASPECTS OF KEY MANAGEMENT

N/A

6.3.1 Archiving of the public key

N/A

6.4. VALIDITY PERIOD OF THE CERTIFICATE AND THE PAIR OF KEYS

The validity period of the certificate is determined based on:

- the level of the technology;
- the level of cryptographic knowledge;
- the planned use of the certificate.

The validity period of the certificate is expressed therein, in accordance with the procedure indicated in this manual.

The CA certificate has a duration of 20 years, whereas certificates issued to natural persons have a validity of no more than three years.

It will not be possible to issue qualified certificates that have a duration that exceeds the expiry date of the CA certificate.

6.4.1 Activation data for the private key

See paragraphs 4.2 and 6.3.

6.5. IT SECURITYCHECKS

6.5.1 Computer-specific security requirements

The systems that contribute to the qualified digital signature service are configured in such a way as to minimise the impact of any vulnerabilities, by eliminating all functionalities that do not serve the functioning and management of the CA.

All access by system administrators is tracked, logged and stored in accordance with the provisions of the applicable regulations.

6.6. OPERATIONS ON THE CONTROL SYSTEMS

Cedacri develops, maintains and monitors an Information Security and Quality Management System, in accordance with the ISO/IEC 27001 standard.

This system sets out procedures and controls for:

- Asset Management;

- Access Control;
- Physical and Environmental Security;
- Operational Security;
- Communication Security;
- Acquisition, Development and Maintenance of Systems;
- Accident Management;
- Operational Continuity.

These procedures follow a specific approval procedure and are shared with all staff through their publication in the company portal.

6.7. NETWORK SECURITY CONTROLS

All networks are adequately managed and controlled to protect them from any threats and to maintain the security of all systems and applications that use the same networks, including information in transit.

The security mechanisms, service levels and management requirements concerning network services are identified and set down in the relevant contracts with the providers where these services are contracted out, and in corporate procedures and/or in the contracts with Customers, where they are provided by Cedacri.
The Cedacri telecommunication network is configured so as not to have single weak points and avoiding components that do not have alternative routing and, thus, can cause a crisis of the entire network if they fail.
Connection to the Cedacri network is allowed only to known and acknowledged systems; all systems which data and transactions come from or are going to are identified and recorded.
Every connection between networks, sub-networks, network elements, machines or applications must be configured so that no Cedacri component is exposed to security erosion.

All systems with direct connections to the network have a sole address (no duplicate) by which they are identified.

The number of connections between the Cedacri telecommunication network and external networks is kept as low as possible.

The security systems that stand between the Cedacri networks and external networks are protected from any internal and external intruders and they are installed in places with restricted and controlled physical access.

All access to the connections between the Cedacri network and public networks shall be previously and expressly authorized and use operational modalities and technologies set down by a dedicated corporate structure.

It is forbidden to use independent modems installed on workstations that are simultaneously connected to the LAN and to other Cedacri telecommunication networks, for direct connection to the phone network.

All access to the internet is controlled by firewalls and, when made available, is in any case allowed exclusively for work reasons; moreover, a tool is in place to set down, by user category, which websites can be accessed.

Every user must strictly comply with the general rules set forth below:

6.8. TIME STAMPING

Generally speaking, a time stamp is a digitally signed data structure that securely and verifiably connects a given computerised document to a reliable time reference.

The QTSP uses a trusted system, whose keys are certified by a certification authority, or Time Stamping Authority, for its internal systems and to offer a time stamping service to its users. All the time stamps issued by the validation system are stored in a dedicated unmodifiable digital archive for a period of no less than 20 years. The time stamp is valid for the entire period for which it is stored by the service provider.

7. FORMAT OF THE CERTIFICATE, THE CRL AND THE OCSP

7.1. FORMAT OF THE CERTIFICATE

The certificate contains the information indicated in the certification request.

The format of the certificate produced is compliant with the eIDAS Regulation and the AgID Resolution, and thus guarantees full readability and verifiability in the context of European certificators and regulations.

Cedacri uses the ITU X.509 standard, version 3, for the entire PKI structure.

The Annex contains the layout of the root certificates and the subjects' certificates, for natural persons.

7.1.1 Version number

All certificates issued by Cedacri are X.509, version 3.

7.1.2 Extensions of the certificate

Qualified certificates are characterised by the extensions present in QCStatements, clause 3.2.6 of IETF RFC 3739. Their use is governed by ETSI 319 412-5.

For the extensions, see the Annex.

7.1.3 OID of the signature algorithm

The certificates are signed with the following algorithm:

sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11].

7.1.4 Name forms

Each certificate contains a unique serial number within the CA that has issued it.

7.1.5 Restrictions on names

See paragraph 3.1 on this matter.

7.1.6 OID of the certificate

See paragraph 1.2 on this matter.

7.2. FORMAT OF THE CRL

To create the CRLs, Cedacri uses the RFC5280 profile “Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)” and adds to the basic format with the extensions, as defined by RFC 5280: “Authority Key Identifier”, “CRL Number”, “Issuing Distribution Point” and “expiredCertsOnCRL”.

7.2.1 Version number

All CRLs issued by Cedacri are X.509, version 2.

7.2.2 Extensions of the CRL

For the extensions of the CRL, see the Annex.

7.3. FORMAT OF THE OCSP

In order to determine the revocation status of the certificate without making a CRL request, Cedacri uses the OCSP protocol in accordance with the RFC6960 profile “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”. This protocol specifies the data that must be exchanged by an application that wants to verify the status of the certificate.

7.3.1 Version number

The OCSP protocol used by Cedacri is compliant with RFC6960, version 1.

7.3.2 Extensions of the OCSP

For the extensions of the OCSP, see the Annex.

8. CONFORMITY CONTROLS AND ASSESSMENTS

Cedacri is a qualified electronic signature QTSP pursuant to European regulations; therefore, Cedacri is subject to periodic verification of conformity ("supervision") by the Conformity Assessment Body (CAB).

This conformity assessment is carried out pursuant to the eIDAS Regulation and Regulation ETSI EN 319 401, in accordance with the eIDAS assessment framework defined by ACCREDIA in response to Regulations ETSI EN 319_403 and UNI CEI EN ISO/IEC17065:2012.

In addition to this, Cedacri conforms to the standards ISO 9001 and ISO 27001, and the field of application includes the electronic signature service among the services provided by Cedacri.

Compliance with the security procedures and standards is verified through an internal audit process.

Internal audits are planned to verify the compliance of the Management System with the security requirements set down by Cedacri and by the reference international standards.

8.1. FREQUENCY OF OR CIRCUMSTANCES FOR CONFORMITY ASSESSMENT

The conformity assessment is carried out every two years, but every year the CAB performs a supervisory audit, at least once a year.

8.2. IDENTITY AND QUALIFICATIONS OF THOSE WHO CARRY OUT THE CONTROLS

The controls are carried out by DNV-GL.

Address: Via Energy Park 14, 20871 Vimercate MBTelephone:039 689 0029

8.3. RELATIONS BETWEEN CEDACRI AND CAB

There is no relationship between Cedacri and DNV-GL (for example, partnership relations or financial interests) that could in any way influence the outcome of the checks performed.

Cedacri's Internal Auditing structure reports directly to the Chairman / Chief Executive Officer and is independent of the other corporate structures.

It has to plan and execute/coordinate interventions aimed at ensuring, through ongoing, structured auditing activities, compliance with the procedures and standards adopted by Cedacri when performing its activities and internal processes, in line with the corporate strategies and policies and with the laws in force, with a view to improving the quality, efficiency and cost-effectiveness of corporate activities.

8.4. ASPECTS ASSESSED

The CAB assesses conformity with the Operating Manual, the Regulation and the applicable legislation of the procedures adopted, the organisation of the CA, the organisation of roles, staff training and contractual documentation.

8.4.1 Actions in the event of non-conformity

If the audit reveals any aspects that do not conform to the reference regulations, it shall be up to the CAB to decide whether to send the report to AgID in any case or to take the time it needs to verify the effectiveness of the corrective actions implemented in order to rectify the anomalies.

Any non-conformities identified by other auditors are brought to the attention of the Company Management, which establishes how to manage them on a case-by-case basis, taking into account the auditor's indications.

9. OTHER LEGAL AND BUSINESS ASPECTS

9.1. FEES

9.1.1 Fees for the issuance and renewal of certificates

Fees for the issuance, renewal, revocation and suspension of certificates shall be defined on a project basis.

These fees are, in any case, dependent on the quantities handled and subject to market performance and, therefore, are not published on the Certificator's website.

For information, write to the email address: servizifiduciari-cedacri@iongroup.com

9.1.2 Fees for access to certificates

Lists of the certificates in force (subject to the Subject's authorisation for publication) are available on the website http://www.cedacricert.it/ and can be accessed by following the instructions on the browser menu.

9.1.3 Fees for access to information about the suspension and revocation status of certificates

The Certificate Revocation Lists (CRLs) and Certificate Suspension Lists (CSLs) are available at http://www.cedacricert.it/ and can be accessed by following the instructions on the browser menu.

9.1.4 Fees for other services

See 9.1.1.

9.1.5 Reimbursement policies

Customers are obliged to pay compensation for any damage suffered by Cedacri in the following cases:

- false declaration in the certification request;
- omission of information about essential events or facts, whether through negligence or with the intention of deceiving Cedacri;
- use of names (e.g. domain names, commercial trademarks) in violation of intellectual property laws.

9.2. FINANCIAL LIABILITY

9.2.1 Insurance cover

The maximum compensation for any damage caused by non-compliance or negligence of the Certificator is fixed at:

- €500,000 per individual claim;
- €1,500,000 per insurance year.

9.2.2 Other activities

N/A

9.2.3 Guarantee or insurance cover for end subjects

See paragraph 9.2.1.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of application of confidential information

The context of the activities which are the subject of this manual does not cover the management of confidential information.

9.3.2 Information that does not fall within the scope of application of confidential information

N/A

9.3.3 Responsibility to protect confidential information

N/A

9.4. PRIVACY

The information collected by the QTSP when carrying out its functions is initially collected on paper media and subsequently entered into its IT system. This information should be considered confidential, except for that information intended for public use of the certificates, and therefore published in the Directory Server. There is no "sensitive" information pursuant to Legislative Decree no. 196 of 30 June 2003. The paper media are also archived electronically and maintained for a period of 20 years.

The data provided are divided into two categories: compulsory and optional, as indicated in the activation request.

Compulsory data are those data necessary for the performance of the services; their provision is compulsory and any refusal to provide them shall make it impossible to conclude the contract. Some of these data are published in the certificate, communicated and disseminated, including in countries outside of the European Union, through the insertion of the data into the certificates register.

In any case, the QTSP shall comply with the provisions of General Data Protection Regulation (EU) 2016/679, as subsequently amended, in the processing of the personal data that come into its possession and in the adoption of the relevant security measures.

9.4.1 Privacy programme

Cedacri adopts an integrated approach to the Quality and Security System, in accordance with the ISO 9001 and ISO 27001 standards, which guarantees a series of policies, practices and procedures for the management of corporate processes, as well as the integrity, confidentiality and availability of the data and information managed.

The system is live and is constantly updated; all the corporate policies and procedures are available to employees on the company intranet, together with adequate and periodic provision of courses on data and information security.

9.4.2 Data processed as personal

Data that correspond to the relevant definition pursuant to the regulations in force are processed as personal data; personal data means any information relating to a natural person that is identified or identifiable, including indirectly, through reference to any other information, including a personal identification number.

9.4.3 Data not considered personal

Data that are planned to be published by the CA's technical management, public keys, certificates (if requested by the Subject), and certificate revocation and suspension dates are not considered to be personal data.

9.4.4 Privacy policy and consent to the processing of personal data

The privacy policy is attached to the request forms and it is available on the website http://www.cedacricert.it/ in the Download section.

By filling out the “Activation request” form, Cedacri informs the Subject, pursuant to and for the purposes of Article 13 of General Data Protection Regulation (EU) 2016/679, that their personal data will be processed, through the use of paper archives and digital and electronic tools capable of guaranteeing the maximum level of security and confidentiality.

9.4.5 Disclosure of data at the request of the authorities

The disclosure of data at the request of the authorities is compulsory, and shall take place in accordance with the terms established from time to time by the authority in question.

9.4.6 Other reasons for disclosure

The data provided shall be processed in order to provide the services set out under the present contract and may be communicated to the companies that provide consultancy and technical assistance to the Certificator.

9.5. INTELLECTUAL PROPERTY

This manual is the property of Cedacri, which reserves all rights related thereto.

The Subject of the certificate maintains all possible rights over its commercial trademarks and brand names, as well as its domain name. With regard to the property of other data and information, the laws in force shall apply.

9.6. REPRESENTATION AND GUARANTEES

See the contracts between the CA and the subject for details about the guarantees and responsibilities incumbent on each party.

9.7. LIMITATION OF GUARANTEE

The Certification Authority does not provide any warranties on the proper operativity and safety of hardware and software used by the Subject; the use of a private keys, and/or certificates of signature different from those provided by current regulations and this Practice Statement; the continuity of national and/or international electricity and telephone lines; the validity and relevance, including probatory, of the subscription certificate - or of any message, deed or document associated with it or created by means of the keys to which the certificate is referred, without prejudice to the effectiveness of the handwritten signature recognized to the qualified electronic signature, in conformity with the art. 25 of Regulation EU n. 920/2014; the secrecy and/or integrity of any message, deed or document associated with the subscription certificate or created by means of the keys to which the certificate is referred to. The Certification Authority guarantees only the functioning of the Service, according to the levels speficied in paragraph 9.15 of the Certificate Practice Statement.End and termination

9.8. LIMITATION OF RESPONSIBILITY

The Certification Authority does not assume any obligation on monitoring the content, type, or electronic format of documents transmitted to the signature, nor assumes any liability whatsoever, for the validity and traceability of the same to the actual will of the Subject. The Certification Authority assumes no responsibility for the hashs of the documents submitted to the signature procedure, if calculated by an IT procedure indicated by the Subscriber or Subject other than the platforms provided by Cedacri. Except in case of wilful misconduct or negligence, the Certification Authority shall not be liable for any direct or indirect damage suffered by the Subjects and/or third parties as a result of the use or non-use of the subscription certificates issued in accordance with the provisions of this Statement and the General Conditions of Certification Services. Cedacri is not responsible for any direct and/or indirect damage also deriving from: loss, improper storage, improper use of identification and authentication tools and/or failure of the Subject in complying with the recommendations mentioned above. Moreover, the Certification Authority is not liable for any damages and/or delays due to malfunctioning or arrest of the computer system and internet network, since the phase of formation of the Contract for the Certification Services (hereinafter also referred to as "Contract"), and also during its execution. Except in the case of wilful misconduct or negligence, Cedacri shall not be burdened with charges or liability for direct or indirect damages of any nature or importance that may occur to the Subject, Subscriber and/or third parties caused by third parties unauthorized by Cedacri tampering or interfering with the service or equipment.

9.8.1 End

At the end of the relationship between the CA and the Subject, the certificate is revoked.

9.8.2 Termination

Such aspects are detailed in the contract governing the service.

9.8.3 Effects of the termination

The contract between the CA and the Subject is automatically terminated, resulting in the interruption of the service, in the event of revocation of the certificate.

9.9. Official communication channels

See the contact channels referred to in paragraph 1.5.

9.10. Dispute resolution and complaints

See the contracts that govern the service for details of dispute resolution procedures.

Cedacri has put in place a process of complaints management that should be sent by email to servizifiduciari-cedacri@iongroup.com guaranteeing a time to take charge of the request of up to 7 solar days. The internal management involves a system of problem ticketing traced and that allows the eventual escalation of the ticket to the competent specialist

9.11. Competent court

The relations between the CA and the Subject are governed by Italian law.

For any dispute that may arise from the services governed by the present contract, the competent court is that of Milano.

9.12. Applicable law

The applicable law for this operating manual is Italian law.

Listed below are some of the main laws in force at the time of publication of this manual:

1. 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, which repeals Directive 1999/93/EC (also referred to as the eIDAS Regulation)
2. Legislative Decree No. 82 of 7 March 2005 (Official Gazette no. 112 of 16 May 2005) – Digital Administration Code
3. Presidential Decree No. 445 of 28 December 2000 (Official Gazette no. 42 of 20 February 2001)
4. Legislative Decree No. 196 of 30 June 2003 (Official Gazette no. 174 of 29 July 2003) – Privacy Code, as subsequently amended and supplemented
5. Presidential Decree of 22 February 2013 (Official Gazette no. 117 of 21 May 2013) - Technical rules on generating, affixing and verifying advanced, qualified and digital electronic signatures, pursuant to Articles 20, paragraph 3, 24, paragraph 4, 28, paragraph 3, 32, paragraph 3 b), 35, paragraph 2, 36, paragraph 2, and 71.
6. Legislative Decree No. 231 of 21 November 2007, “Implementation of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, as well as Directive 2006/70/EC laying down implementing measures”, as subsequently amended and supplemented
7. Legislative Decree No. 206 of 6 September 2005, as subsequently amended and supplemented - Consumer Code
8. Personal Data Protection Authority Order of 26 March 2003 [1053753]
9. CNIPA Resolution No. 45 of 21 May 2009, as amended by subsequent decisions
10. General Data Protection Regulation (EU) 2016/679
11. Legislative Decree 101/2018 “Provisions for the adaptation of the National Regulations to the Provisions of the Regulation (EU) 2016/679 of the European

Parliament and of the Council, of 04/27/2016, relating to the protection of individuals with regard to the processing of personal data, as well as to free circulation of such data and repealing Directive 95/46/CE (general regulation on data protection)"

All the circulars and resolutions of the Supervisory Authority also apply, as do the implementing acts provided for by the eIDAS Regulation.

9.13. MISCELLANEOUS PROVISIONS

See the contracts governing the service for any other provision not covered in this manual.

9.14. OTHER PROVISIONS

The service is provided as per the following table:

Type of service	Days of availability	Times of availability
Availability of lists: Public keys Revoked keys (CRL) Suspended keys (CSL)	7 days a week	24 hours a day
Issuance of the qualified certificate	Working days	09:00 - 13:00 and 15:00 - 19:00
Suspension of the qualified certificate	7 days a week	24 hours a day
Revocation of the qualified certificate	7 days a week	24 hours a day

10. ANNEX

10.1. ASN1 DUMP ROOT CA CERTIFICATE: CEDACRICERT EU 2019

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (58 bit) 145225339350479356
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (4 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-00432960342
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String Cedacri SpA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Cedacricert EU 2019
    SEQUENCE (2 elem)
      UTCTime 2019-07-09 10:08:21 UTC
      UTCTime 2039-07-10 10:08:21 UTC
    SEQUENCE (4 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-00432960342
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String Cedacri SpA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Cedacricert EU 2019
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (1 elem)
        SEQUENCE (2 elem)
                                                          INTEGER (4096             bit)
891001467680908246696812084556822785855283030736394072037921073770813…
          INTEGER 65537
    [3] (1 elem)
      SEQUENCE (5 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (1 elem)
            OCTET STRING (20 byte) 4F2A6C3222EAC18E9DBFC997F49AC05B94F540AA
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
```

```
            BOOLEAN true
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              [0] (20 byte) 4F2A6C3222EAC18E9DBFC997F49AC05B94F540AA
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.76.27.1.1.2
                SEQUENCE (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String http://www.cedacricert.it/cedacricert/en/documentazione/
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            BIT STRING (7 bit) 0000011
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
    NULL
  BIT                                   STRING (4096                                  bit)
1100111100011101101101000110010100100110101000011110000101000110111001…
```

10.2. ASN1 DUMP END USER: CEDACRICERT EU 2019

```
SEQUENCE (3 elem)
  SEQUENCE (8 elem)
    [0] (1 elem)
      INTEGER 2
    INTEGER (63 bit) 8044746428757289316
    SEQUENCE (2 elem)
      OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
      NULL
    SEQUENCE (4 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-0011111111
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String Cedacri SpA
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Cedacricert EU 2019
    SEQUENCE (2 elem)
      UTCTime 2019-07-17 12:13:51 UTC
      UTCTime 2022-07-17 12:13:51 UTC
    SEQUENCE (8 elem)
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.6 countryName (X.520 DN component)
          PrintableString IT
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.97
          UTF8String VATIT-02144370547
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.10 organizationName (X.520 DN component)
          UTF8String OrgName
```

```
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.4 surname (X.520 DN component)
          UTF8String Cognome
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.42 givenName (X.520 DN component)
          UTF8String Nome
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.5 serialNumber (X.520 DN component)
          PrintableString TINIT-DGDFDF87C26G343F
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.3 commonName (X.520 DN component)
          UTF8String Nome Cognome
      SET (1 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.4.46 dnQualifier (X.520 DN component)
          PrintableString DGDFDF87C26G343F
    SEQUENCE (2 elem)
      SEQUENCE (2 elem)
        OBJECT IDENTIFIER 1.2.840.113549.1.1.1 rsaEncryption (PKCS #1)
        NULL
      BIT STRING (1 elem)
        SEQUENCE (2 elem)
                                                              INTEGER (2048             bit)
25513000521548391674762357327930318780190291616519842881795451608245 5…
          INTEGER 65537
    [3] (1 elem)
      SEQUENCE (8 elem)
        SEQUENCE (2 elem)
         OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.1 authorityInfoAccess (PKIX private extension)
          OCTET STRING (1 elem)
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                  OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.2 caIssuers (PKIX subject/authority
info access descriptor)
               [6] http://www.cedacricert.it/cedacricert/en/download/CertificatoRoot.html
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.48.1 ocsp (PKIX)
                [6] http://www.cedacricert.it/ocspqual
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.14 subjectKeyIdentifier (X.509 extension)
          OCTET STRING (1 elem)
            OCTET STRING (20 byte) B9359B2F374221FD09156C3031F9DA36DDC8D76E
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.19 basicConstraints (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            SEQUENCE (0 elem)
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.35 authorityKeyIdentifier (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              [0] (20 byte) 4F2A6C3222EAC18E9DBFC997F49AC05B94F540AA
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 1.3.6.1.5.5.7.1.3 qcStatements (PKIX private extension)
          OCTET STRING (1 elem)
            SEQUENCE (6 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.6.1.5.5.7.11.2
                SEQUENCE (1 elem)
                  OBJECT IDENTIFIER 0.4.0.194121.1.1
              SEQUENCE (1 elem)
                   OBJECT IDENTIFIER 0.4.0.1862.1.1 etsiQcsCompliance (ETSI TS 101 862
qualified certificates)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.3 etsiQcsRetentionPeriod (ETSI TS 101 862
qualified certificates)
                INTEGER 20
              SEQUENCE (1 elem)
```

```
              OBJECT IDENTIFIER 0.4.0.1862.1.4 etsiQcsQcSSCD (ETSI TS 101 862 qualified
certificates)
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.6
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.1862.1.6.1
            SEQUENCE (2 elem)
              OBJECT IDENTIFIER 0.4.0.1862.1.5
              SEQUENCE (1 elem)
                SEQUENCE (2 elem)
                  IA5String https://www.cedacricert.it/cedacricert/en/documentazione/
                  PrintableString en
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.32 certificatePolicies (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (2 elem)
              SEQUENCE (2 elem)
                OBJECT IDENTIFIER 1.3.76.27.1.1.2.1
                SEQUENCE (1 elem)
                  SEQUENCE (2 elem)
                    OBJECT IDENTIFIER 1.3.6.1.5.5.7.2.1 cps (PKIX policy qualifier)
                    IA5String https://www.cedacricert.it/cedacricert/en/documentazione/
              SEQUENCE (1 elem)
                OBJECT IDENTIFIER 0.4.0.194112.1.2
        SEQUENCE (2 elem)
          OBJECT IDENTIFIER 2.5.29.31 cRLDistributionPoints (X.509 extension)
          OCTET STRING (1 elem)
            SEQUENCE (1 elem)
              SEQUENCE (1 elem)
                [0] (1 elem)
                  [0] (1 elem)
                    [6] http://www.cedacricert.it/crl/crlEU2019.crl
        SEQUENCE (3 elem)
          OBJECT IDENTIFIER 2.5.29.15 keyUsage (X.509 extension)
          BOOLEAN true
          OCTET STRING (1 elem)
            BIT STRING (2 bit) 01
  SEQUENCE (2 elem)
    OBJECT IDENTIFIER 1.2.840.113549.1.1.11 sha256WithRSAEncryption (PKCS #1)
    NULL
  BIT                                     STRING (4096                                    bit)
100010110000100001010001101010110001100110011100010001110011010011001…
```

10.3. CRL AND OCSP EXTENSIONS

CRL Extensions

Extension	Value
Authority Key Identifier	160-bit SHA-1 hash of the value of the issuerPublicKey
CRL number	Il numero univoco della CRL assegnato dalla CA
ExpiredCertsOnCRL	GeneralizedTime date on which the CRL starts to keep revocation status information for expired certificates
Issuing Distribution Point	Identifies the CRL distribution point and scope for a particular CRL, and it indicates whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes
Invalidity Date	the UTC date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid

La richiesta OCSP contiene i seguenti campi:

Field	Value
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	DN Issuer's Hash
Issuer Key Hash	Hash of the issuer's public key.
Serial Number	Certificate's serial number

La risposta OCSP contiene i seguenti campi:

Field	Value
Response Status	OCSP response status
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN of the OCSP response certificate.
Produced at	Date in GeneralizedTime format of when the response was generated
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Subject Certificate Name Hash	subject DN hash of the verified certificate

Subject Certificate Key Hash	Public key Hash of the verified certificate
Serial Number	Serial number of the verified certificate
thisUpdate	The most recent time at which the status being indicated is known by the responder to have been correct.
nextUpdate	The time at which the verified certificate's status changed
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]