PKI DISCLOSURE STATEMENT FOR THE CEDACRI QUALIFIED ELECTRONIC SIGNATURE SERVICE

1 INTRODUCTION

This document is the PKI Disclosure Statement, pursuant to European Regulation
ETSI EN 319_401, ETSI EN 319_411-2 e ETSI EN 319_411-1, relating to the qualified electronic signature service of the Qualified Trust Service Provider (QTSP) hereinafter also referred to as Cedacri, whose registered offices are in Collecchio (Parma), at Via del Conventino no. 1, with tax ID – VAT no. 00432960342, 0521 8071, Fax: 0521 807901.
Cedacri operates in accordance with the relevant applicable European (Regulation EU no. 910/2014 - eIDAS) and national regulations (Legislative Decree no. 82 of 7 March 2005, as subsequently amended – Digital Administration Code).
This document does not substitute the General Terms and Conditions of the service or the Qualified Electronic Signature Operating Manual - CP and CPS (hereinafter referred to as the “Operating Manual”), which are published on the website www.cedacricert.it .

2 CONTACT INFORMATION

Cedacri S.p.A.
Via del Conventino, 1
43044 Collecchio (Parma)
Tel. +039 0521 8071 (switchboard)
Tel. +039 0521 807901
Website: www.cedacricert.it
Information email address: info@cedacricert.it

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.

3 TYPES OF CERTIFICATE, USE THEREOF AND VALIDATION PROCEDURES

The service involves the issuance of a qualified certificate related to the public key of the Holder Subject (hereinafter referred to as the "Subject") and its publication in accordance with the procedures indicated in the Operating Manual.
The certificates are issued to natural persons, subject to the conditions published on the website www.cedacricert.it in the "Download" section.
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.
For more information on the policies supported
(e.g. the relevant OIDs and other characteristics), see the documentation published at the address indicated above in the DOCUMENTATION section.
The certificate issuance process provides for the following two cases:

- keys generated on USB tokens;
- keys generated on HSMs and intended to be used for automatic signing.

The qualified certificate issued has a validity of 1,095 days, unless revoked.
If requested, the QTSP shall deliver directly to the Subject, upon payment of the relevant cost, a secure signature creation device that can store the private key thereof and generate digital signatures within it.
The issuance of a digital certificate can take place only after identification and certain registration of the requestor. Cedacri manages the entire life cycle of the certificate, including the temporary suspension of its validity or definitive revocation.

4 LIMITATIONS OF USE

Qualified certificates are issued for the affixing of qualified electronic signatures.
Additional limitations of use may be specified in the individual certificates via the UserNotice feature in the CertificatePolicies extension.
Any limitations of value of the transactions in which the certificate can be used are specified in
the individual certificates via the QCStatements extension, by means of the item QcEuLimitValue.
The holders' registration information and the event log relating to the CA service
are stored by Cedacri for 20 years.

5 HOLDERS' OBLIGATIONS

The Subject is responsible for the truthfulness of the data communicated in the Activation Request.
If the Subject, at the time of identification, has, including through the use of untrue personal documents, concealed their real identity or falsely declared to be somebody else, or, in any way, acted in such a way as to compromise the identification process and the relevant facts indicated in the certificate, they shall be considered liable for all damage resulting to the QTSP and/or third parties due to the inaccuracy of the information contained in the certificate, with the obligation to guarantee and hold harmless the QTSP for any requests for damages.
The Subject is also liable for damage resulting to the QSTP and/or third parties in the event of the delayed activation by the Subject of the procedures provided for by the Operating Manuals for the revocation and/or suspension of the certificate.
The Subject, in view of the fact that the use of a digital signature for which a qualified certificate has been issued offers the possibility to sign significant deeds and documents to all intents and purposes of Italian law and attributable exclusively to the Subject, is required to observe the utmost diligence in using, storing and protecting the private key, the signature device and the associated activation code (PIN).

Specifically, the Subject is required, pursuant to Article 32 of the Digital Administration Code, to adopt all technical and organisational measures aimed at preventing the use of the asymmetric key system or the digital signature from causing harm to others.
Said Subject is required to protect the secrecy of the private key, by not communicating or disclosing to third parties the personal identification number (PIN) required to activate the key, making sure to type it in such a way as not to allow it to come to the knowledge of others, and storing it in a secure place that is different from the place where the device containing the key is stored.
The private key for which the qualified certificate has been issued is strictly personal. The secure signature device containing it may not, for any reason, be transferred to given for use to third parties.
The Subject must autonomously ensure compliance with the hardware and software requirements necessary for the correct use of the digital signature.
Specifically, the Subject shall adapt its hardware and software systems to the security measures provided for by the legislation in force.
The digital certificate can be issued in the name of the person who requests and uses it (the Subject), or in the name of a Subject, with the option for the certificate to be used by persons other than the Subject (the User).
In the event that the certificate is issued in the name of the Subject, with the option for it to be used by Users, both parties are subject to the rights and obligations set out in this contract, unless expressly provided otherwise.
In the event that the private key becomes compromised (e.g. due to loss of the PIN for the secure signature device or its disclosure to unauthorised third parties), immediately cease using the key and ensure that it is not used again.

6 OBLIGATIONS FOR VERIFYING THE CERTIFICATES' STATUS

The verification can be carried out by consulting the CRL published by the QTSP
or by applying to the OCSP service provided by the QTSP, at the addresses (URLs) contained in the certificates.

7 LIMITATION OF GUARANTEE AND RESPONSIBILITIES

The obligations of the QTSP are those indicated in the regulations in force, the Operating Manual and the contracts between the Subject and the QTSP.
The QSTP does not provide any guarantee concerning the correct functioning and the security of the hardware and software equipment used by the Subject, concerning uses of the private key, the secure signature device and the qualified certificate other than those provided for by the Italian regulations in force and by the Operating Manual, concerning the regular and ongoing functioning of national and/or international electrical and telephone lines, concerning the validity and significance, including of a probationary nature, of the qualified certificate or of any message, deed or document associated therewith or created via the keys to which the certificate relates in relation to persons subject to legislation other than Italian law, or concerning their secrecy and/or integrity (in the sense that any violations of the latter are, usually, identifiable by the Subject or by the recipient via a dedicated verification procedure).

8 APPLICABLE AGREEMENTS, CP AND CPS

The applicable agreements and terms and conditions are set out in the following published documents:

- General terms and conditions of the service, available on Cedacri's website at the address http://www.cedacricert.it/cedacricert/it/download/Offerta.html
- Certificate Policy (CP) and Certification Practice Statement (CPS) or “Operating Manual”, available on the website http://www.cedacricert.it/cedacricert/it/documentazione/

9 PRIVACY PROTECTION

Cedacri complies with Italian (Legislative Decree 196/2003) and EU (Regulation EU No. 679/2016) legislation on privacy, as well as with the recommendations and provisions of the Personal Data Protection Authority.
For further information, see the general terms and conditions of the service, following the indications provided in the previous paragraph.

10 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.

11 APPLICABLE REGULATIONS, COMPLAINTS AND COMPETENT COURT

The service provided by Cedacri is subject to Italian and European law.
Cedacri has put in place a process of handling any complaints that should be sent by email to: info@cedacricert.it guaranteeing a time to take charge of the request of up to 7 days.
For all legal disputes brought by or against Cedacri and relating to the aforementioned service provided by Cedacri, the Law Courts of Parma shall have exclusive competence.

12 ACCREDITATIONS, TRUSTMARKS AND CONFORMITY CHECKS

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 European Regulation (referred to chap 1 in accordance to eIDAS assessment framework defined by ACCREDIA.
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.