PKI Disclosure Statement

« CertEurope eID Certification Authorities »

Version: 1.3
Update: 00
Creation date: 14/11/2016
Last update: 13/09/2019
Status: Official
Written by: CertEurope
Verified by: COSSI
Approved by: COSSI

CertEurope, une société du groupe Oodrive

www.certeurope.fr

26, rue du Faubourg Poissonnière, 75010 Paris – France

Tel : +33 (0)1 45 26 72 00 / Fax : +33 (0)1 45 26 72 01

Modifications

Date	Etat	Version	Commentaires
14/11/2016	Official	1.0	
07/02/2017	Official	1.1	Corrections after audit : update offers' list
25/04/2019	Official	1.2	Add new profiles: - PSD2 (QCP-L and QCP-W client/server) - RGS* only (no face-to-face requirement) - EIDAS only (no RGS requirements)
13/09/2019	Official	1.3	Review and update references (RGPD)

Summary

1 Introduction

This document is the PKI Disclosure Statement and Abstract herein after referred as PDS.

This document does not substitute or replace the Certificate Policy and/or Certificate Practice Statement under which digital certificates issued by CertEurope.

The purpose of this document to summarize the key points of the CertEurope CPs and CPSs for the benefit of the Subscribers, Certificate Holders and Relying Parties.

2 Contact

CertEurope, une société du groupe Oodrive

contact@certeurope.fr – www.certeurope.fr

26, rue du Faubourg Poissonnière, 75010 Paris – France

Tel : +33 (0)1 45 26 72 00 / Fax : +33 (0)1 45 26 72 01

3 Certificate type, validation procedure and usage

3.1 Identification and Validation

Issued certificates aim at identifying:

- individual with high level of trust, in conformity with requirements of
  - ETSI EN 319 411-2 levels : QCP-N and QCP-N-QSCD
  - ETSI EN 319 411-1 levels : LCP, NCP and NCP+
- entity or organisation with high level of trust, in conformity with requirements of:
  - ETSI EN 319 411-2 levels : QCP-L + (PSD2 QCStatements)
  - ETSI EN 319 411-1 levels : LCP, NCP and NCP+
- website with high level of trust, in conformity with requirements of:
  - ETSI EN 319 411-2 level QCP-W + (PSD2 QCStatements)
  - ETSI EN 319 411-1 levels : DVCP, OVCP and EVCP

During registration, CertEurope has processes to identify subject and certificate requester and to validate information contained within a certificate (see CP/CPS Section 3). Individual identity is checked against ID.

The following describes the full range of the CertEurope eID trust chain

3.1.1 eID User

3.1.1.1 Qualified offer for physical persons

Level	Regulation	Description
**	RGS v2	Certificate distributed on a qualified cryptographic support
*	RGS v2	Certificate on a software keystore without face-to-face
QCP-N-QSCD	EIDAS	Certificate distributed on a qualified cryptographic support
QCP-N	EIDAS	Certificate on a software keystore

OID	Usages		Qualifications	
	SIGN	AUTH	RGS v2	EIDAS
1.2.250.1.105.**23.411.2.1**.1.*1.0*	X		*	QCP-N
1.2.250.1.105.**23.411.2.1**.2.*1.0*	X	X	*	QCP-N

1.2.250.1.105.**23.411.2.2**.1.*1.0*	X		**	QCP-N-QSCD
1.2.250.1.105.**23.411.2.2**.2.*1.0*	X	X	**	QCP-N-QSCD
1.2.250.1.105.**23.411.2.3**.1.*1.0*	X	X		QCP-N
1.2.250.1.105.**23.411.2.3**.2.*1.0*	X	X		QCP-N-QSCD
1.2.250.1.105.**23.411.1.4**.1.*1.0*	X	X	*	

3.1.1.2 Certified offer for physical persons

Level	Referential	Description
NCP+	319 411-1	Certificate distributed on a cryptographic support
NCP	319 411-1	Certificate after a face-to-face
LCP	319 411-1	Certificate distributed without a face-to-face

OID	Usages		Certification
	SIGN	AUTH	
1.2.250.1.105.**23.411.1.1**.1.*1.0*	X		ETSI EN 319 411-1 **LCP**
1.2.250.1.105.**23.411.1.1**.2.*1.0*		X	ETSI EN 319 411-1 **LCP**
1.2.250.1.105.**23.411.1.1**.3.*1.0*	X	X	ETSI EN 319 411-1 **LCP**
1.2.250.1.105.**23.411.1.2**.1.*1.0*	X		ETSI EN 319 411-1 **NCP**
1.2.250.1.105.**23.411.1.2**.2.*1.0*		X	ETSI EN 319 411-1 **NCP**
1.2.250.1.105.**23.411.1.2**.3.*1.0*	X	X	ETSI EN 319 411-1 **NCP**
1.2.250.1.105.**23.411.1.3**.1.*1.0*	X		ETSI EN 319 411-1 **NCP+**
1.2.250.1.105.**23.411.1.3**.2.*1.0*		X	ETSI EN 319 411-1 **NCP+**
1.2.250.1.105.**23.411.1.3**.3.*1.0*	X	X	ETSI EN 319 411-1 **NCP+**

3.1.2 eID Corp

3.1.2.1 Qualified seals for legal persons

Level	Regulation	Description
**	RGS v2	Seal certificate distributed on a qualified cryptographic support
*	RGS v2	Seal certificate without face-to-face
QCP-L-QSCD	EIDAS	Seal certificate distributed on a qualified cryptographic support (not available yet)
QCP-L	EIDAS	Seal certificate
QCP-L (PSD2)	EIDAS+PSD	Seal certificate for PSD2 Usage

OID	Usages		Qualifications	
	SIGN	AUTH	RGS v2	EIDAS
1.2.250.1.105.**24.411.2.1**.1.*1.0*	X	X	*	QCP-L
1.2.250.1.105.**24.411.2.2**.1.*1.0*	X	X	**	QCP-L
1.2.250.1.105.**24.411.2.3**.1.*1.0*	X	X		QCP-L
1.2.250.1.105.**24.411.1.4**.1.*1.0*	X	X	*	
1.2.250.1.105.**24.411.2.5**.1.*1.0*	X	X		QCP-L (PSD2)

3.1.2.2 Certified seals for legal persons

Niveau	Référentiel	Description
NCP+	319 411-1	Seal certificate distributed on a cryptographic support

Niveau	Référentiel	Description
NCP	319 411-1	Seal certificate
LCP	319 411-1	Seal certificate without face-to-face

OID	Usages		Certification
	SIGN	AUTH	
1.2.250.1.105.**24.411.1.1**.1.*1.0*	X	X	ETSI EN 319 411-1 **LCP**
1.2.250.1.105.**24.411.1.2**.1.*1.0*	X	X	ETSI EN 319 411-1 **NCP**
1.2.250.1.105.**24.411.1.3**.1.*1.0*	X	X	ETSI EN 319 411-1 **NCP+**

3.1.3 eID Website

3.1.3.1 Qualified SSL/TLS offers for websites

Niveau	Réglementation	Description
**	RGS v2	SSL Certificate on a cryptographic device
*	RGS v2	SSL Certificate
QCP-W	EIDAS	SSL Certificate on a cryptographic device
QCP-W	EIDAS	SSL Certificate
QCP-W (PSD2)	EIDAS+PSD	SSL certificate for PSD2 Usage

OID	Usages		Qualifications	
	AUTH	CNFD	RGS v2	EIDAS
1.2.250.1.105.**25.411.2.1**.1.*1.0*	X		*	QCP-W
1.2.250.1.105.**25.411.2.1**.2.*1.0*	X	X	*	QCP-W
1.2.250.1.105.**25.411.2.2**.1.*1.0*	X		**	QCP-W
1.2.250.1.105.**25.411.2.2**.2.*1.0*	X	X	**	QCP-W
1.2.250.1.105.**25.411.2.3**.1.*1.0*	X			QCP-W
1.2.250.1.105.**25.411.2.3**.2.*1.0*	X	X		QCP-W
1.2.250.1.105.**25.411.1.4**.1.*1.0*	X		*	
1.2.250.1.105.**25.411.1.4**.2.*1.0*	X	X	**	
1.2.250.1.105.**25.411.2.5**.1.*1.0*	X			QCP-W (PSD2)
1.2.250.1.105.**25.411.2.5**.2.*1.0*	X	X		QCP-W (PSD2)

3.1.3.2 Certified SSL/TLS offers for websites

Niveau	Référentiel	Description
EVCP	319 411-1	Certificat de site web qui requiert une validation étendue des informations d'une organisation
OVCP	319 411-1	Certificat de site web qui requiert une validation des informations de l'organisation
DVCP	319 411-1	Certificat de site web qui requiert une validation des informations sur le nom de domaine.

OID	Usages	Certification

	AUTH	CNFD	
1.2.250.1.105.**25.411.1.1**.1.*1.0*	X		ETSI EN 319 411-1 **DVCP**
1.2.250.1.105.**25.411.1.1**.2.*1.0*	X	X	ETSI EN 319 411-1 **DVCP**
1.2.250.1.105.**25.411.1.2**.1.*1.0*	X		ETSI EN 319 411-1 **OVCP**
1.2.250.1.105.**25.411.1.2**.2.*1.0*	X	X	ETSI EN 319 411-1 **OVCP**
1.2.250.1.105.**25.411.1.3**.1.*1.0*	X		ETSI EN 319 411-1 **EVCP**
1.2.250.1.105.**25.411.1.3**.2.*1.0*	X	X	ETSI EN 319 411-1 **EVCP**

3.2 Registration Procedure

CertEurope performs certificate's holder registration process and certificate issuance in conformance with Sections 4.1, 4.2 and 4.3 of the CP/CPS.

4 Reliance limits

Any usage other than those defined in the CP/CPS is prohibited. In particular, the CP/CPS does not allow a Subscriber to issue a certificate to a Certification Authority. Certificates shall be used only in accordance with applicable law.

5 Obligations of subscribers

Subscriber's obligations are defined in the Subscriber Agreement

6 Obligations of relying parties

Relying Party obligations are defined in the Subscriber Agreement

7 Certificate status checking obligation of relying parties

Obligations are exposed in the Subscriber Agreement.

8 Limited warranty and disclaimer of liability

Limitations are exposed in the Subscriber Agreement.

9 Applicable agreements, certification practice statement, certificate

Applicable documents are available at the address: https://www.certeurope.fr/chaine-de-confiance

- the CP/CPS;
- the Subscriber Agreement;
- The Terms and Conditions;

10 Privacy policy

The collected personal data are essential for the execution of the contract, in compliance with applicable regulations, in particular Regulation (EU) 2016/679 of 27 April 2016. (See Section 9.4 of the CP/CPS).

11 Refund policy

CertEurope does not apply a refund policy, in the limit of the applicable laws. See the Subscriber Agreement

12 Applicable law, complaints and dispute resolution

CertEurope set up a procedure for complaint management.

IN CASE OF LITIGATION BETWEEN THE PARTIES RESULTING FROM THE INTERPRETATION, APPLICATION AND/OR EXECUTION OF THE CONTRACT, AND IN THE ABSENCE OF MUTUAL AGREEMENT BETWEEN THE AFOREMENTIONNED PARTIES, THE ONLY COMPETENT JURISDICTION IS THE PARIS TRIBUNAL.

13 CA and repository licenses, trust marks and audit

CertEurope eID Certification Authorities audits are performed in conformance with ETSI EN 319 411-1 and ETSI EN 319 411-2 on regular basis by an independent auditor organism (See CP/CPS Section 8).