ZETESCONFIDENS

ENROLMENT METHODS AND PROCEDURES

Identifier:	**ZetesConfidens**
Subject:	**Enrolment Methods and Procedures**
Category:	**Procedure**
Version:	**1.3**
Status:	**Final**
Date:	**22/07/2020**
Author:	**Jos De Wachter / Bart Symons**
Classification:	**PUBLIC**
Copyright:	**© 2020 Zetes - All rights reserved.**

Table of Content

Document History

Version	Date	Author	Changes
1.3	22/07/2020	BS	Added new policy OIDs
1.2	05/07/2020	JDW	Certificate application and identity validation explained additionally
1.1	22/05/2020	JDW	Corrections after audit
1.0	07/03/2020	JDW	Initial document

1 INTRODUCTION

This document covers the enrolment methods and procedures for public Certificates issued by ZetesConfidens to End-Entities. Currently ZetesConfidens only issues End-Entities Certificates to natural persons. When End-Entities Certificates for legal entities will be issued a separate section will be added for the enrolment procedure.

2 CERTIFICATE POLICY OVERVIEW

2.1 Existing ZetesConfidens Issuing CAs

ZetesConfidens operates a 2-level CA hierarchy for issuing certificates: the Zetes TSP ROOT CA 001 is the top level CA issuing only certificates for Issuing CAs. This document applies to the following ZetesConfidens Issuing CAs:

- **Zetes TSP Qualified CA 001**
- **ZetesConfidens - Signature Creation Service - issuing CA 001**

2.2 Zetes TSP Qualified CA 001

The Zetes TSP Qualified CA 001 issues different types of Certificates under the following Certificate Policies:

Policy Type	ETSI CP OID	ZetesConfidens CP OID
OID branch	-	[1.3.6.1.4.1.47718.2.1.2].2
LCP	0.4.0.2042.1.3	[1.3.6.1.4.1.47718.2.1.2].2.4.1
NCP+	0.4.0.2042.1.2	[1.3.6.1.4.1.47718.2.1.2].2.4.2 [1.3.6.1.4.1.47718.2.1.2].2.1.10
QCP-n-qscd	0.4.0.194112.1.2	[1.3.6.1.4.1.47718.2.1.2].2.4.3 [1.3.6.1.4.1.47718.2.1.2].2.3.10

2.3 ZetesConfidens - Signature Creation Service - issuing CA 001

The ZetesConfidens - Signature Creation Service - issuing CA 001 issues different types of Certificates under the following Certificate Policy:

Policy Type	ETSI CP OID	ZetesConfidens CP OID
OID branch	-	[1.3.6.1.4.1.47718.2.1.2].5
LCP	0.4.0.2042.1.3	[1.3.6.1.4.1.47718.2.1.2].5.1
NCP+	0.4.0.2042.1.2	[1.3.6.1.4.1.47718.2.1.2].5.2
QCP-n-qscd	0.4.0.194112.1.2	[1.3.6.1.4.1.47718.2.1.2].5.3

3 ENROLMENT METHODS

3.1 Existing ZetesConfidens identity verification methods

Currently no legal persons are registered by ZetesConfidens.

The following registration methods with verification of the identity are currently used or investigated for use by ZetesConfidens:

- **Methods requiring (prior) physical presence (PP) of the natural person or of an authorised representative of the legal person**
    a) **Face-to-face** registration;
    b) remotely, using **electronic identification means under a notified scheme**, which meet the requirements set out in Article 8 eIDAS with regard to the assurance levels 'substantial' or 'high';
    c) by means of a **certificate of a qualified electronic signature** or of a qualified electronic seal issued in compliance with point (a) or (b);
    d) by using **other identification methods recognised at national level** which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body;
    e) by using **other identification methods** which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body;
    f) by using **other identification methods,** however the equivalent assurance in terms of reliability to physical presence is NOT confirmed by a conformity assessment body;
- **Methods without proof of (prior) physical presence**
    g) remotely, using **electronic identification means under a notified scheme**, where no prior physical presence is attested and which meet the requirements set out in Article 8 eIDAS with regard to the assurance levels 'substantial' or 'high'
    h) by using **other identification methods,** which meet the requirements set out in Article 8 eIDAS with regard to the assurance levels 'substantial' or 'high'

3.2 Mapping of Certificate Policies and Enrolment Methods

Naming of Registration methods under 4.1	LCP	NCP/NCP+	QCP-x-xxx	Enrolment method OID
(a) PP / face-to-face	√	√	√	1.3.6.1.4.1.47718.2.5.1
(b) PP / notified scheme	√	√	√	1.3.6.1.4.1.47718.2.5.2
(c) PP/ certificate of QES issued compliant to (a) or (b)	√	√	√	1.3.6.1.4.1.47718.2.5.3
(d) PP (CAB confirmed) / recognised at national level	√	√	√	1.3.6.1.4.1.47718.2.5.4
(e) PP (CAB confirmed) / other method	√	√	-	1.3.6.1.4.1.47718.2.5.5

(f) PP (unconfirmed) / other method	√	√	-	1.3.6.1.4.1.47718.2.5.6
(g) no eq. PP / notified scheme	√	-	-	1.3.6.1.4.1.47718.2.5.7
(h) no eq. PP / other methods	√	-	-	1.3.6.1.4.1.47718.2.5.8

3.3 Identification and authentication requirements for an individual Subject

3.3.1 Preregistration or listing of eligibility

Preregistration is not a mandatory phase in all circumstances. However, if the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence shall be provided of approval by the legal person and the natural person that the subject attributes also identify such organization.

Often this evidence is achieved in connection with the subscriber operating an authorized source and inviting subjects to (pre)register or apply for a certificate or where the subjects apply on their proper initiative, a listing of eligibility can be provided to the RA.

3.3.2 Application for certificates and Identity validation

Following a possible preregistration process, based upon an invitation by the subscriber or on its own initiative, a subject may apply for a certificate.

The identity of a Subject is authenticated by the RA.

The procedure follows the steps described below:

1) STEP 1 – ENR 1: **creation of a registration file containing the subject's identification** information (name, surname, date of birth, contact information, authentication-related information, and when relevant any relevant existing registration information (e.g. company registration unique identifier) of the associated legal person or other organizational entity identified in association with the legal person, etc.); this file can be prepared on-line or at the occasion of step 2 below.

2) STEP 2 – ENR 2: **validation** that the above information is genuine and belongs to the person requesting access to the signing service.
   To do so:
   a) For NCP+ and QCP-n-qscd certificates, the SUB-RA (or its authorised L-RA) relies on a **face to face registration in person or equivalent** .
      (i) face to face:
      - the Subject will have to appear in person in front of an authorized operator of the Local RA and present a valid and authentic identity document (national identity card, residence permit, passport, etc.) to the Local RA operator to conclude the registration process. The Local RA operator validates the authenticity of the presented documents and checks that the individual is the genuine holder of the presented documents according to rules defined by ZETESCONFIDENS internal instructions and - optionally - additional rules defined by the Subordinate RA and/or the Subscriber. Optionally, in addition to identifying and authenticating the Subject, the SUB-RA / L-RA validates the request and checks the Subject's entitlements.
      - The Subject profile is provided to the SUB-RA and transferred to the C-RA
      - the Subject is provided with information about the service and credential for further authentication purposes.

      (ii) equivalent to face to face:

- the SUB-RA relies on a IDP who performed a recent face to face validation of the subject's identity. E.g. Subjects who are holder of a Belgian electronic Identity Card or a Belgian electronic Residence Permit Card can use the SUB-RA online registration portal. Subjects authenticate (log on) with their eID card, which implies possession of the eID card and knowledge of the eID PIN code.

  For QCP-n-qscd certificates the equivalent method must be according to Article 24(1) of Regulation (EU) No 910/2014**.**
- the Subject profile is transferred to the C-RA
- the Subject is provided with information about the service and credential for further authentication purposes.

b) For LCP certificates, the registration method relies on the validation of an official form of identification that has at least the assurance level "substantial" as defined in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

Example of a registration process for a Belgian SUB-RA:

- a signed recto-verso copy of the Subject's identity document is provided through the SUB-RA online registration portal, together with other information provided by the subject (e.g. the mobile phone number and e-mail address).

  The SUB-RA verifies the validity of the identity document using the Belgian federal government's CheckDoc service (www.checkdoc.be) to check if the identity document (ID card, passport, residence permit) is known, genuine and hasn't been revoked.
- the Subject profile is transferred to the C-RA and a certificate and signature service account are created.
- the Subject is provided with information about the service and credential for further authentication purposes.

3) STEP 3 – ENR.AUTH: for subsequent requests (certificate request, signature activation requests), the Subject is authenticated with an **authentication means** that:

   i) is unambiguously linked to the person and has been mapped by the SUB-RA and/or the C-RA to that Subject account.

   ii) provides a secure mechanism to ensure sole control of the signature key by the Subject

   For this purpose, at the time of the registration validation ENR 2, the Subject receives or is associated with a credential that can be used to authenticate the Subject unambiguously toward the Signature Creation Service, and / or to provide a verifiable association between the Subject's request and the previously recorded identity data and attributes of the Subject.

3.3.3 Entitlement of additional attributes

In some cases, the CA may also certify professional attributes or membership attributes in addition to identity. The validation of these attributes is the responsibility of the Subscriber and the burden of proof falls upon the Subject and the Subscriber.

The Subscriber may attest to a Subject's professional attribute such as an official degree, a diploma, a mandate, etc., as specified in the applicable Subscriber's agreement.

The Subscriber may attest to a Subject's membership of or relationship with the organization it represents such as member, employee, associate, role, department, customer, etc.

The Subscriber cannot attest any relationship between a Subject and a third-party organization.

4 SUBJECT DEVICE AND SECURE CRYPTOGRAPHIC DEVICE

4.1 ZetesConfidens Subject Device Provisioning and SCD Management overview

ZetesConfidens provides or accepts the following Subject Devices for end-entity certificates:

- "Soft keys"
- PKI-enabled smartcard
- PKI-enabled smartcard with QSCD status
- Managed HSM
- Managed HSM with QSCD status

4.2 Mapping of Certificate Policies and Subject Device/(Q)SCD

Subject Device and Managed (Q)SCD	**LCP**	**NCP**	**NCP+**	**QCP-n**	**QCP-l**	**QCP-n-qscd**	**QCP-l-qscd**
Key in Software	√	√	-	√	√	-	-
Key in HW – smartcard	√	√	√	√	√	-	-
Key in HW – smartcard – qscd	√	√	√	√	√	√	√
Key in HW – Managed HSM	√	√	√	√	√	-	-
Key in HW – Managed HSM – qscd	√	√	√	√	√	√	√

Key generation process	**LCP**	**NCP**	**NCP+**	**QCP-n**	**QCP-l**	**QCP-n-qscd**	**QCP-l-qscd**
ZetesConfidens controlled	√	√	√	√	√	√	√
Key holder controlled – with explicit proof of possession of private key	√	√	√	√	√	√	√

Appendix A - REQUIREMENTS FOR EID MEANS, CHARACTERISTICS AND DESIGN

NOTE The elements of technical specifications and procedures outlined in this Annex are equivalent to the requirements specified in (EU) 2015/1502 6 ANNEX Clauses 2.1, 2.2.1 and 2.3.1 for assurance level substantial or higher.

A.1 Enrolment

A.1.1 Application and registration

Assurance level	Elements needed
Low	1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. 2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means. 3. Collect the relevant identity data required for identity proofing and verification.
Substantial	Same as level low.
High	Same as level low.

A.1.2 Identity proofing and verification (natural person)

Assurance level	Elements needed
Low	1. The person can be assumed to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid. 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.
Substantial	Level low, plus one of the alternatives listed in points 1 to 4 has to be met: 1. The person has been verified to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person andsteps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; OR 2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been

	taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents; OR 3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section A.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body; OR 4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body. *NOTE 1 In the context of the European Union the applicable regulatory requirement for a conformity assessment body is Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council.*
High	Requirements of either point 1 or 2 have to be met: 1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met: (a) Where the person has been verified to be in possession of photo or biometric identification evidence recognized by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source; or (b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section A.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid; OR (c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. r

	OR 2. Where the applicant does not present any recognized photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognized photo or biometric identification evidence are applied. *NOTE 2 In the context of the European Union the applicable regulatory requirement for a conformity assessment body is Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council.*

A.1.3 Identity proofing and verification (legal person)

Assurance level	Elements Needed
Low	1. The claimed identity of the legal person is demonstrated on the basis of evidence recognized by the Member State in which the application for the electronic identity means is being made. 2. The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source, where the inclusion of a legal person in the authoritative source is voluntary and is regulated by an arrangement between the legal person and the authoritative source. 3. The legal person is not known by an authoritative source to be in a tatus that would prevent it from acting as that legal person.
Substantial	Level low, plus one of the alternatives listed in points 1 to 3 has to be met: 1. The claimed identity of the legal person is demonstrated on the basis of evidence recognized by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable) its registration number and the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source, where the inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector and steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents; OR 2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section A.1.3 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body; OR 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body. *NOTE 1 In the context of the European Union the applicable regulatory requirement for a conformity assessment body is Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council.*
High	Level substantial, plus one of the alternatives listed in points 1 to 3 has to be met: 1. The claimed identity of the legal person is demonstrated on the basis of evidence recognized by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context and the evidence is checked to determine that it is valid according to an authoritative source; OR

	2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section A.1.3 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body and steps are taken to demonstrate that the results of this previous procedure remain valid; OR 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. *NOTE 2 In the context of the European Union the applicable regulatory requirement for a conformity assessment body is Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council.*

A.1.4 Binding between the electronic identification means of natural and legal persons

Where applicable, for binding between the electronic identification means of a natural person and the electronic identification means of a legal person ('binding') the following conditions apply:

It shall be possible to suspend and/or revoke a binding. The life-cycle of a binding (e.g. activation, suspension, renewal, revocation) shall be administered according to nationally recognized procedures.

The natural person whose electronic identification means is bound to the electronic identification means of the legal person may delegate the exercise of the binding to another natural person on the basis of nationally recognized procedures. However, the delegating natural person shall remain accountable.

Binding shall be done in the following manner:

Assurance level	Elements Needed
Low	1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above. 2. The binding has been established on the basis of nationally recognized procedures. 3. The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.
Substantial	Point 3 of level low, plus: 1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high. 2. The binding has been established on the basis of nationally recognized procedures, which resulted in the registration of the binding in an authoritative source. 3. The binding has been verified on the basis of information from an authoritative source.
High	Point 3 of level low and point 2 of level substantial, plus: 1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high. 2. The binding has been verified on the basis of a unique identifier representing the legal person used in the national context; and on the basis of information uniquely representing the natural person from an authoritative source.

A.2 Electronic identification means and authentication

A.2.1 Electronic identification means characteristics and design

Assurance level	Elements needed
Low	1. The electronic identification means utilises at least one authentication factor. 2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.
Substantial	1. The electronic identification means utilises at least two authentication factors from different categories. 2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
High	Level substantial, plus: 1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential 2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

A.2.2 Authentication mechanism

The following table sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

Assurance level	Elements needed
Low	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. 3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
Substantial	Level low, plus: 1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. 2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High	Level substantial, plus: The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

---------- Last page of this document ----------