ZETES TSP - QUALIFIED CA 001

TEST CERTIFICATES FOR THIRD PARTIES

Title:	Zetes TSP - Qualified CA 001
Subject:	Test certificates for third parties
Category:	Readme
Version:	1.0
Status:	Final
Publish date:	27/07/2017
Author:	Bart Symons
Classification:	PUBLIC
Copyright:	© 2017 Zetes - All rights reserved.

Table of Content

1 README

This document provides information about the set of test certificates that is made available to third parties for the Zetes TSP Qualified CA 001. These test certificates are representative for the real certificates issued in accordance with the following Certificate Policies and the following Certificate Profiles:

Certificates labelled AUT:

ZETES TSP NCP+ certificate for natural persons for the Subscriber OVB-OBFG

certificate policy OID:	1.3.6.1.4.1.47718.2.1.2.2.1.10	policy version 1.2
certificate profile OID:	1.3.6.1.4.1.47718.2.1.3.2.1.10	profile version 1.1

Certificates labelled QES:

ZETES TSP QCP-n-qscd certificate for natural persons for the Subscriber OVB-OBFG

certificate policy OID:	1.3.6.1.4.1.47718.2.1.2.2.3.10	policy version 1.2
certificate profile OID:	1.3.6.1.4.1.47718.2.1.3.2.3.10	profile version 1.1

The Certificate Policy and Certificate Profile document can be downloaded from http://repository.tsp.zetes.com.

The CA hierarchy for these test certificates is the following:

ZETES TSP Root CA 001

| Subject serialNumber = 001
| certificate serial number = 02 54 1A A9 50 D7 CE 1F

| SHA1 thumbprint = 37 53 D2 95 FC 6D 8B C3 9B 37 56 50 BF FC 82 1A ED 50 4E 1A
|

---- **ZETES TSP Qualified CA 001**
Subject serialNumber = 001
certificate serial number = 38 20 EE 9C 74 EC D1 47

SHA1 thumbprint = 16 98 DC 47 F4 F5 FF 95 6C 56 03 24 E1 96 5A A7 ED 38 E2 9D

This set of test certificates provides the capability to allow third parties to check and test the various certificate types. For this purpose, the test certificates are made available in a variety of certificate status conditions (valid, expired and revoked).

The test certificates clearly indicate that they are for testing purposes (a.o. in the subject name, organization name, Zetes TSP proprietary policy OID and in the user notice statement):

- **subject serial number** is the same format as for real certificates but all digits are set to zero
- **subject givenName** is“givenName_TEST”
- **subject surName** is“surName_TEST_xxxxxx”
  xxxxxx is a 6-digit number, unique for each certificate
- the name components of the **subject commonName** are “surname_TEST_xxxxxx givenName_TEST” with prefixes and suffixes as in the real certificate
- if an e-mail address is used for **emailAddress** or in the subject alternate name, then it is set to “test.test@example.com”
- **subject Organization and OrganizationalUnit** are the same as the real certificates but prefixed with “TEST “
- special **URL**s in test certificates *:
  - http://crt.test.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crt
  - http://ocsp.test.tsp.zetes.com
  - http://crl.test.tsp.zetes.com/ZETESTSPQUALIFIEDCA001.crl
  - http://crl.test.tsp.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl

- identical **URLs** in test certificates:
  - https://repository.tsp.zetes.com
  - https://pds.tsp.zetes.com

  these URL remain identical as those in the real certificates because the certificate must point to the real CP/CPS/PDS which also contain the information about the test certificates.
- **generic policy identifiers (OID)**:
  No differences, to allow testing whether 3rd party application correctly interpret and display these standardized generic OIDs
- **proprietary policy identifiers (OID):**

real OID CP QES certificates:	1.3.6.1.4.1.47718.2.1.2.2.3.10
test OID CP QES certificates:	2.999.1.3.6.1.4.1.47718.2.1.2.2.3.10
real OID CP AUT certificates:	1.3.6.1.4.1.47718.2.1.2.2.1.10
test OID CP AUT certificates:	2.999.1.3.6.1.4.1.47718.2.1.2.2.1.10

- **QC Statements**
  Test certificates contain the same key usage attributes and QC Statement attributes as the real certificates. To distinguish test certificates from real certificates, the **User Notice** attribute will contain a clear statement that the certificate is intended for test purposes only.

** Remark: The URLs in the test certificates that refer to the CRL, CA crt download and the OCSP service are different from the equivalent in the real certificates. Under normal conditions, these URLs shall be mapped to the same resource as the URLs in the real certificates, to allow for testing with the real infrastructure. At the discretion of Zetes TSP these URLs may be diverted to another resource, e.g. in case of abusive use of the test certificates.*

2 TABLE OF FILES WITH TEST CERTIFICATES

Files: PKCS12 files that include the complete certificate chain (no password)

CRT files with the end entity certificates and CRT files with the CA certificates

Certificate Policy ID : 1.3.6.1.4.1.47718.2.1.2.2.3.10				
Surname (also the filename)	**Type**	**Common Name**	**Title**	**Status of the certificate**
surName_TEST_000002	OBFG QES	QES surName_TEST_000002 givenName_TEST (avocat)	Avocat	Valid certificate
surName_TEST_000004	OVB QES	QES surName_TEST_000004 givenName_TEST (Rechtsanwalt)	Rechtsanwalt	Expired
surName_TEST_000007	OVB QES	QES surName_TEST_000007 givenName_TEST (advocaat)	advocaat	Revoked with reason 'CA compromise'
surName_TEST_000008	OVB QES	QES surName_TEST_000008 givenName_TEST (advocaat)	advocaat	Revoked with reason 'Affiliation changed'
surName_TEST_000011	OBFG QES	QES surName_TEST_000011 givenName_TEST (avocat)	Avocat	Revoked with reason 'Certificate hold'
surName_TEST_000012	OBFG QES	QES surName_TEST_000012 givenName_TEST (avocat)	Avocat	Revoked with reason 'Privileges withdrawn'

Certificate Policy ID : 1.3.6.1.4.1.47718.2.1.2.2.1.10				
Surname (also the filename)	**Type**	**Common Name**	**Title**	**Status of the certificate**
surName_TEST_000013	OVB AUT	AUT surName_TEST_000013 givenName_TEST (advocaat)	advocaat	Valid certificate
surName_TEST_000014	OBFG AUT	AUT surName_TEST_000014 givenName_TEST (staff member)	staff member	Expired
surName_TEST_000015	OVB AUT	AUT surName_TEST_000015 givenName_TEST (advocaat)	advocaat	Revoked with reason 'Unspecified'
surName_TEST_000016	OVB AUT	AUT surName_TEST_000016 givenName_TEST (advocaat)	advocaat	Revoked with reason 'Key compromise'
surName_TEST_000017	OBFG AUT	AUT surName_TEST_000017 givenName_TEST (avocat)	avocat	Revoked with reason 'Superseded'
surName_TEST_000018	OBFG AUT	AUT surName_TEST_000018 givenName_TEST (avocat)	avocat	Revoked with reason 'Cessation of operation'

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