

Known issue (cosmetic): dubbel ETSI QC compliance statement

Versie : 1.1
Status : Definitief / opgelost
Datum : 2 juni 2010

Omschrijving issue

In het kader van SHA-256 is UZI-register gemigreerd naar een vernieuwde infrastructuur die operationeel is vanaf 30 november 2009. Handtekeningcertificaten die na die datum zijn uitgegeven en voor 2 juni 2010 hebben een kleine afwijking in het certificaatprofiel: het zogenaamde *etsi-qc-compliance-statement* is dubbel opgenomen. Deze afwijking heeft geen invloed op de correcte werking van UZI-passen, handtekeningcertificaten en applicaties.

Omgevingen waar het optreedt

Handtekeningcertificaten die zijn uitgegeven na 30 november 2009.

Afwijking

Hieronder is aangegeven hoe het QCStatement ingevuld dient te zijn.

```
*****
0472 30 18: . . . . SEQUENCE {
0474 06 8: . . . . . OBJECT IDENTIFIER '1 3 6 1 5 5 7 1 3'
047E 04 C: . . . . . OCTET STRING, encapsulates {
0480 30 A: . . . . . SEQUENCE {
0482 30 8: . . . . . SEQUENCE {
0484 06 6: . . . . . . . . . . OBJECT IDENTIFIER '0 4 0 1862 1 1'
      : . . . . . . . . . . }
      : . . . . . . . . . . }
      : . . . . . . . . . . }
      : . . . . . . . . . . }
*****
```

De eerste OID (1 3 6 1 5 5 7 1 3) geeft aan dat het om het attribuut 'qcStatements' gaat. De waarde '0 4 0 1862 1 1' is het specifieke etsi-qc-compliance-statement en geeft aan dat een certificaat gekwalificeerd is en uitgegeven is door een CSP die voldoet aan het normenkader ETSI TS 101 456. Ter illustratie is dat hieronder weergegeven door een certificate viewer die deze OID herkent.

```
QualifiedCertificateStatements =
  QcCompliance (according to Annex I and II of the EU directive 1999/93/EC)
```

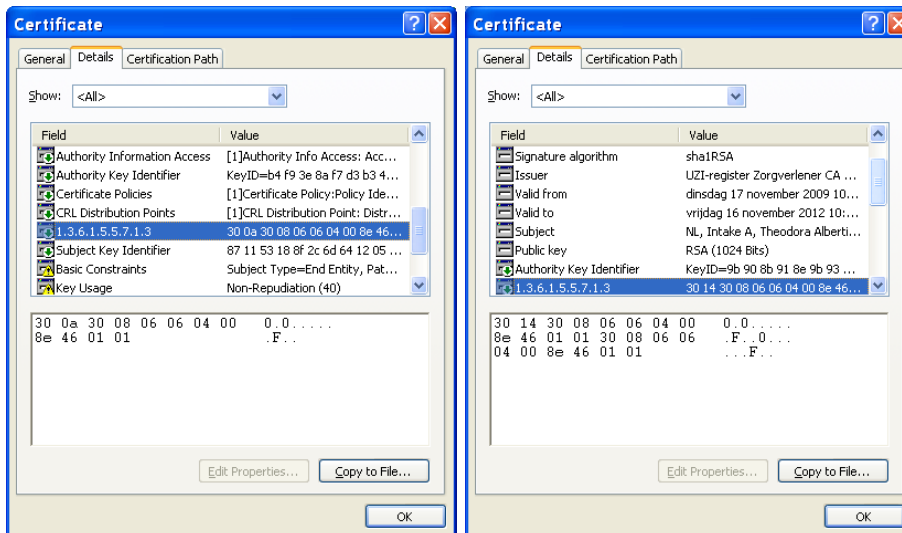
In de certificaten die uitgegeven zijn na 30 november 2009 is het etsi-qc-compliance-statement dubbel opgenomen zoals hieronder met highlight weergegeven:

```
*****
020C 30 22: . . . . SEQUENCE {
020E 06 8: . . . . . OBJECT IDENTIFIER '1 3 6 1 5 5 7 1 3'
0218 04 16: . . . . . OCTET STRING, encapsulates {
021A 30 14: . . . . . SEQUENCE {
021C 30 8: . . . . . SEQUENCE {
021E 06 6: . . . . . . . . . . OBJECT IDENTIFIER '0 4 0 1862 1 1'
      : . . . . . . . . . . }
0226 30 8: . . . . . SEQUENCE {
0228 06 6: . . . . . . . . . . OBJECT IDENTIFIER '0 4 0 1862 1 1'
      : . . . . . . . . . . }
      : . . . . . . . . . . }
      : . . . . . . . . . . }
      : . . . . . . . . . . }
*****
```

Hieronder is dat weergegeven door een certificate viewer die deze OID herkent.

```
QualifiedCertificateStatements =
  QcCompliance (according to Annex I and II of the EU directive 1999/93/EC)
  QcCompliance (according to Annex I and II of the EU directive 1999/93/EC)
```

De onderstaande figuur geeft weer hoe het attribuut in de Microsoft Certificate Viewer zichtbaar is. Omdat Microsoft de OID van de het attribuut 'qcStatements' niet kent, wordt de inhoud in beide gevallen hexadecimaal getoond.



Correct

Dubbel etsi-qc-compliance-statement

Analyse

Hoewel het afwijkt van het gespecificeerde certificaatprofiel is er geen risico van verstoring vanwege de volgende redenen:

1. Het attribuut 'qcStatements' biedt conform de *RFC 3039 Qualified Certificates Profile* ruimte voor meerdere afzonderlijke 'statements'. Hoewel redundant is het niet verboden om meerdere specifieke qcStatements op te nemen;
2. De technische codering (DER) van het certificaat en het qcStatements attribuut is correct;
3. De meeste applicaties interpreteren het (informatieve) attribuut niet zoals bijv. de microsoft certificate viewer;
4. Het 'qcStatements' attribuut is een 'non-critical' attribuut wat inhoudt dat applicaties die het attribuut niet 'begrijpen' het mogen negeren;
5. Binnen AORTA worden vooralsnog alleen authenticatie certificaten gebruikt.

Oplappingsrichting en workaround

Pashouders en vertrouwende partijen hoeven geen enkele maatregel te nemen aangezien de werking van de passen en handtekeningcertificaten niet in het geding is.

Certificaten die ondertekend zijn op 2 juni 2010 of later bevatten een correct qcStatement.