

## Known issue PKCS#10 request en Portecle v1.2

**Versie** : 1.0  
**Status** : Definitief  
**Datum** : 16 oktober 2007

---

### Omschrijving issue

In de WDH pilot in Enschede is de volgende bevinding naar voren gekomen (Nr. 19). *Voor het genereren van een PKCS#10 request is een programma nodig. In de pilot zijn PKCS#10 requests aangemaakt met de tool Portecle. Om onduidelijke redenen lukt het niet om op basis hiervan een servercertificaat te maken. Het systeem van het UZI-register beschouwt de aanvraag als ongeldig. Op het oog lijkt er sprake van een correct PKCS#10 request.*

### Omgevingen waar het optreedt

Alle PKCS#10 requests die met Portecle v1.2 (5 november 2006) zijn aangemaakt, kunnen niet gebruikt worden voor aanvraag van een servercertificaat bij het UZI-register.

### Analyse

Uit nader onderzoek is gebleken dat een PKCS#10 request dat gegenereerd is met Portecle v1.2 niet voldoet aan de PKCS standaard. Dit is hieronder toegelicht.

In de PKCS#9 standaard v2.0 *Selected Object Classes and Attribute Types* staan de attributen beschreven die in een PKCS#10 certificate signing request mogen zitten. Onderstaand citaat laat zien dat bij het attribuut `countryOfCitizenship` 'PrintableString' staat als enig toegestaan coderingsformaat voor deze string. (Andere attributen mogen ook een UTF8 en/of IA5 gecodeerde string zijn.)

\*\*\*\*\*

#### 5.2.7 Country of citizenship

The `countryOfCitizenship` attribute specifies the (claimed) countries of citizenship for the subject it is associated with. It SHALL be a 2-letter acronym of a country in accordance with [4].

```
countryOfCitizenship ATTRIBUTE ::= {
    WITH SYNTAX PrintableString (SIZE(2) ^ CONSTRAINED BY {
-- Must be a two-letter country acronym in accordance with ISO/IEC 3166 --})
    EQUALITY MATCHING RULE caseIgnoreMatch
    ID pkcs-9-at-countryOfCitizenship
}
```

\*\*\*\*\*

Hierna is een PKCS#10 request dat gegenereerd is met Portecle v1.2 gedecodeerd met openssl (versie 0.9.8d 28 Sep 2006). Uit het volgende fragment blijkt dat Portecle het `country` attribuut codeert als UTF8.

```
openssl asn1parse -i -dump -in [PKCS#10 file]
```

```
*****  
73:d=5 hl=2 l= 3 prim: OBJECT :countryName  
78:d=5 hl=2 l= 2 prim: UTF8STRING  
0000 - 4e 4c NL  
*****
```

### Conclusie

De portecle tool v1.2 codeert het 'countryOfCitizenship' attribuut in het PKCS#10 request als een UTF8-string. Dit is niet conform de specificaties in de PKCS#9 standaard die alleen PrintableString toestaat. Bij een eerste controle (handtekening / RSA 1024 bits) ziet het PKCS#10 request er dus goed uit, maar dit is hoogstwaarschijnlijk de oorzaak dat het CA systeem de aanvraag afkeurt.

### Oplossingsrichting en workaround

De volgende workarounds zijn beschikbaar:

- Als workaround zijn de PKCS#10 requests voor de WDH pilot met OpenSSL aangemaakt.
- Soms hebben applicatie- of webservers eigen tools voor sleutelgeneratie en het aanmaken van een PKCS#10 request bijvoorbeeld Microsoft IIS. Op dit moment zijn er geen problemen bekend met deze tools.

Voor een structurele oplossing dienen leveranciers die in de toekomst Portecle willen gebruiken, contact op te nemen met de ontwikkelaars van Portecle om dit probleem te laten oplossen. Verder analyse door het UZI-register zal pas plaatsvinden als in een nieuwe versie van Portecle het genoemde coderingsprobleem is opgelost.

### Referenties

- <http://portecle.sourceforge.net/>
- <http://www.openssl.org/>
- <http://www.rsa.com/rsalabs/node.asp?id=2131> PKCS #9 v2.0: Selected Object Classes and Attribute Types