

Issue	TC002	Aparte certificaten voor testen
--------------	--------------	--

Status:	Vastgesteld door ALV		
Versienummer:	1.0	Versiedatum:	8 juli 2009
Documentnaam:	TC002 Aparte certificaten voor testen v1.0		

Behandeld door de Technische Commissie

Geaccepteerd door de Issue Commissie Klant op: 25 juni 2009

Geaccepteerd door de Issue Commissie Klant op:
--

Raakt aan:	Kleinverbruik	Grootverbruik	Wholesale
Elektriciteit	X	X	
Gas	X	X	

Impact op keten	Ja/nee
berichten	X
processen	
systemen	X
overigen	

Vastgesteld door NEDU op	8 juli 2009
Invoering in markt met	de nieuwe berichtstructuren

Contact	
Technische Commissie	TC@edsn.nl

TC002: Aparte certificaten voor testen

Situatieschets:

Het testen van applicaties en berichtenverkeer vergt altijd veel inspanning omdat aan weerszijden van de communicatielijn testomgevingen en productie omgevingen op verschillende wijze worden gebruikt en van elkaar gescheiden worden aangestuurd. Ook het (eenvoudig her-) gebruiken van testdata levert problemen op:

- Er is geopperd om voor testdoeleinden andere EAN Codes aan de marktpartijen toe te kennen. Deze EAN Codes zouden dan ook in de OU van de door Diginotar uitgegeven certificaten terecht komen. Deze optie is als niet werkbaar gekenmerkt, vooral omdat in de implementaties bij betrokken marktpartijen veel logica afhangt van de echte (productie-)EAN Codes;
- Er is een risico dat berichten, bedoeld voor een testomgeving, per ongeluk in de productieomgeving terecht zouden kunnen komen. Dit ook omdat in de oorspronkelijke opzet voor zowel productie- als testomgeving gebruik gemaakt wordt van door Diginotar uitgegeven certificaten. Om dit op te vangen is de mogelijkheid van het implementeren van een test-vlaggetje in de berichten header besproken. (Testvlaggetje 'aan' zou dan betekenen dat berichten niet in de productieomgeving geaccepteerd zouden mogen worden).

Vraag:

Kunnen er voor testen eenvoudige 'scheidingsmaatregelen' worden geïmplementeerd?

Overwegingen

Omdat voor testen handig kan zijn om tijdelijk ook certificaten toe te kennen en men de omgevingen ook fysiek wil scheiden wordt voorgesteld om voor testen aparte certificaten in te voeren. Deze certificaten worden NIET toegelaten op de productie omgevingen. Het hergebruik van productiedata in testomgevingen wordt hierdoor minder bedreigend.

Oplossing:

Een simpele oplossing is om voor de testomgeving gebruik te maken van door ESDN uitgegeven certificaten.

De Certificate Authority (CA) zal dan ESDN zelf worden. Berichten, die zijn signed met deze certificaten, worden onder geen beding in de productieomgeving toegelaten, doordat de test-certificaten niet gekend zijn in de productie omgeving (en ook omgekeerd). Indien er verschillende verbindingen gebruikt worden voor test- en productieomgevingen wordt ook op transportniveau (TLS) de verschillende certificaten toegepast. Voordelen op een rij:

TC002: Aparte certificaten voor testen

- EAN Codes kunnen voor test- en productieomgevingen gelijk blijven, dus implementatielogica bij marktpartijen blijft ongewijzigd, waardoor extra inspanningen en kosten achterwege blijven;
- Geen risico dat testberichten per ongeluk in de productieomgeving belanden, dus (geprogrammeerd) gebruik van het test-vlaggetje in de header kan achterwege blijven;
- Uitgifte van testcertificaten wordt door EDSN zelf gedaan (hetgeen zonder al te veel kosten kan worden ingericht), dus kan sneller en zeker goedkoper dan via Diginotar;
- Testen met de EDSN certificaten kan aanvangen voordat de officiële route via Diginotar is gelopen voor de productiecertificaten.

Toelichting

Deze test-certificaten zijn qua inhoud identiek aan de DigiNotar-certificaten, m.u.v. de uitgever van het certificaat. Bijkomend voordeel is dat de uitgifte sneller verloopt dan bij DigiNotar.

EDSN beschikt over een tool waarmee certificaten kunnen worden gegenereerd. Om certificaten te kunnen genereren, is er een CA (Certificaat Autoriteit) opgetuigd, waarbij er twee root-certificaten aanwezig zijn, een hoofd-root-certificaat en een test-root-certificaat. Het test-root-certificaat "hangt" onder het hoofd-root-certificaat. De test-certificaten worden gekoppeld aan het test-root-certificaat. Om een test-certificaat te kunnen genereren is er in de tool een template ontwikkeld, waarmee de standaard gegevens, die in ieder certificaat aanwezig moeten zijn, reeds worden gevuld. Aansluitend worden de partij-specifieke gegevens ingevuld om het aangevraagde certificaat compleet te maken.

Het test-certificaat met bijbehorende sleutel wordt in de tool opgeslagen. Om deze gegevens naar een partij te kunnen sturen, dient het certificaat te worden geëxporteerd naar een 'p12'-bestand, die vervolgens samen met de twee root-certificaten en een passphrase (tijdelijk password) naar de desbetreffende marktpartij worden opgestuurd.

Deze export heeft het volgende formaat: "PKCS #12 with certificate chain". Dat wil zeggen dat het bestand naast het aangevraagde certificaat ook de twee root-certificaten bevat.

De bestandsnaam van de export heeft de volgende format: "EDSN<eejjmmdd><volgnr:nnnn>.p12".

Om alle gegevens in te kunnen voeren, is de volgende informatie nodig van een marktpartij:

1. Hoofd-EAN13 (gebruikt ter identificatie van de organisatie);
2. Naam marktpartij (volgens KvK-uitreksel);
3. Provincie (volgens KvK-uitreksel);
4. Plaats (volgens KvK-uitreksel);
5. Email-adres contactpersoon;
6. FQDN: url of een IP-adres.

TC002: Aparte certificaten voor testen

Het invoeren van gegevens, het genereren van de benodigde bestanden, het completeren van een te verzenden ZIP-bestand met daarin alle benodigde gegevens en het versturen naar de aanvrager kan binnen een uur worden afgehandeld.

Invoeringsstrategie:

Implementatie als standaard voordat intensieve testtrajecten starten in het kader van de uitrol van nieuwe processen en berichten.

Versieoverzicht:

- 0.1 eerste versie vanuit reeds aan IC-Klant aangeboden stuk van bespreking in TC op 15 mei 2009;
- 0.2 toelichting over werking bij EDSN toegevoegd;
- 1.0 na vaststelling door de ALV NEDU op 8 juli 2009.