Barchman Wuytierslaan 6 T (033) 422 4680
3818 LH Amersfoort
www.nedu.nl

NEDU
Nederlandse Energie Data Uitwisseling

Issue TC027 Beveiligingscertificaten 2016

Status	Vastgesteld		
Versienummer	1.0	**Versiedatum**	28 oktober 2015
Documentnaam	TC027 Beveiligingscertificaat 2016 v1.0		

Behandeld door de Technische Commissie

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

Impact op keten	Ja/Nee
Codewijziging	**Nee**
Berichten	**Nee**
Ketenprocessen	**Nee**

Mogelijke impact marktrollen en EDSN	Ja/Nee
LV	**Ja**
PV	**Ja**
MV	**Ja**
RNB	**Ja**
LNB	**Ja**
EDSN	**Ja**

Vastgesteld door NEDU op	**28 oktober 2015**
Invoering in markt per	**1 juni 2016**

Contact	
Technische Commissie	TC@edsn.nl

Managementsamenvatting

Beveiliging van de communicatie in de ketenprocessen tussen de partijen verenigd in de NEDU is een constant punt van aandacht. Voor de beveiliging van het berichtenverkeer wordt gebruik gemaakt van beveiligingscertificaten. De energiesector volgt de overheid in de beveiligingsnorm, aangeduid met PKIoverheid. Regelmatig dienen de certificaten aangepast te worden aan de nieuwe normen. De TC adviseert, conform de afspraak in de ALV van 7 juni 2015, om uiterlijk per 1 juni 2016, nagenoeg samenvallend met de verplichte driejaarlijkse certificatenwissel, de beveiligingscertificaten aan te passen en gebruik te gaan maken van een private root certificaat van de PKIoverheid. In de beveiligingscertificaten wordt de EAN-code van de deelnemende partij in een ander veld geplaatst en wordt er een certificaat ingevoerd voor authenticatie/beveiligen van de verbinding en eventueel het bericht (signing). Indien nodig wordt een separaat certificaat gebruikt voor vertrouwelijkheid (beschermen van vertrouwelijkheid van gegevens door encryptie van de inhoud van het bericht).

Situatieschets

Voor het beveiligen van de berichtenuitwisseling in de sector wordt gebruik gemaakt van beveiligingscertificaten. De certificaten voor de beveiliging (versleuteling) van de verbinding (TLS) wordt door de bedrijven zelf geregeld, zie ook issue TC026. EDSN organiseert het uitgeven van de certificaten voor het berichtenverkeer, voor authenticatie (wie stuurt het bericht) en voor de beveiliging (versleutelen van de berichten). Certificaten moeten regelmatig worden vervangen en worden aangepast aan de eisen des tijds (de race van de beveiliging). Wij hebben dit bijhouden van de ontwikkelingen 'uit besteed' aan de overheid door onder de richtlijnen van de PKIoverheid te vallen. Daarmee moeten onze certificaten voldoen aan die richtlijnen. Sinds de invoering van de beveiligingscertificaten gebruiken we de EAN-code van de partijen als een kenmerk in het certificaat, dit kenmerk wordt door EDSN gebruikt voor de EAN-code controle (controle EAN-code in certificaat vs. EAN-code in bericht). We hebben deze EAN-code op een plaats gezet die bij de invoering logisch leek en die nu minder logisch en niet meer toegestaan is. Bij de invoering van de SHA2 certificaten, ruim twee jaar geleden, hebben we van Logius, de Policy Authority PKIoverheid (vallend onder het Ministerie van Binnenlandse zaken en Koninkrijksrelaties), uitstel gekregen voor de manier waarop we de EAN-code van een partij in het certificaat hebben geplaatst. Dit uitstel loopt halverwege 2016 af, waarna we, als we niks doen, geen bruikbare certificaten meer hebben en daarmee het berichtenverkeer in de sector blokkeert.

In het certificaat is het attribuut KeyUsage opgenomen dat aangeeft waar het certificaat voor gebruikt mag worden, het doel van het certificaat. Hierbij wordt onderscheid gemaakt tussen het controleren wie het bericht stuurt en het versleutelen van de berichten. In de structuur van de huidige SHA2 certificaten wordt in het attribuut KeyUsage digitalSignature aangegeven dat een certificaat voor beide doeleinden wordt gebruikt. Hierdoor kan met dit certificaat dus zowel getekend (signing) als versleuteld (encryptie) worden. Daarmee is de structuur van de huidige SHA2-certificaten niet in lijn met het PKIoverheid stelsel, een combinatiecertificaat voor zowel tekenen (signing) als versleutelen (encryptie) kent het PKIoverheid stelsel niet.

Vraag

Hoe kunnen we de certificaten aanpassen aan de nieuwe eisen en hoe voeren we dit in?

Overwegingen

PKIoverheid
De energiesector heeft in het verleden besloten dat beveiliging conform de richtlijnen van de overheid onder het stelsel van de PKIoverheid gewenst en voldoende is. PKI(Public Key Infrastructure)overheid is een stelsel voor betrouwbare elektronische communicatie binnen en met de Nederlandse overheid. Het stelsel PKIoverheid betreft infrastructuur, regelgeving en afspraken om digitale PKIoverheid certificaten te genereren, beheren, uit te geven en te gebruiken.
Zowel de Security Commissie als de Technische Commissie oordelen dat het voor de sector nog steeds van belang is onder de paraplu van de PKIoverheid te blijven. Het zelf organiseren en uitgeven van voldoende beveiligde certificaten is een voor de sector ongewenste en dure oplossing. De momenteel benodigde aanpassingen zijn geen reden voor het herzien van het eerder genomen besluit om de certificaten onder PKIoverheid uit te laten geven.

Private root
Sinds dit jaar bestaat onder de PKIoverheid de mogelijkheid om de certificaten uit te geven onder een zogenaamde private PKIoverheid-root. Dit zijn certificaten voor min of meer gesloten groepen, waar een iets milder invoerings- en handhavingsregiem geldt. Essentiele verschil tussen de private en de publieke root van PKIoverheid is het feit dat het root certificaat van de private PKIoverheid-root standaard niet wordt verspreid richting alle software / browser leveranciers. Deze kunnen een dergelijk certificaat daarmee ook niet automatisch afhandelen via hun toepassingen.
Logius adviseert de sector om over te gaan op een dergelijk root. De verwachting van Logius is dat de veranderingen in de certificaten de komende jaren steeds frequenter zullen zijn en bij de publieke root ook steeds stringenter moeten worden ingevoerd.
De Security Commissie oordeelt dat vanuit beveiliging optiek de private root en de publieke root gelijkwaardig zijn.

Certificaat voor combinatie verbinding en authenticatie
Zoals aangegeven specificeert het PKIoverheid stelsel verschillende typen certificaten voor verschillend gebruik (doel van het certificaat). De specificatie voor gebruik wordt vastgelegd in het attribuut KeyUsage in het certificaat. Het combineren van authenticatie van een bericht en het versleutelen van een bericht mag niet worden gecombineerd in één certificaat. Het combineren van een certificaat voor het opzetten van een beveiligde lijn en het ondertekenen van een bericht is wel in lijn met het PKIoverheid stelsel zodat een combinatiecertificaat voor zowel tekenen (signing) van het bericht als het beveiligen van de verbinding mogelijk is.
Zie de policy statements van Logius: https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-csp/programma-van-eisen/.
En tevens: https://www.logius.nl/fileadmin/logius/ns/diensten/pkioverheid/programma-van-eisen/08-2015/PvE_deel3e_v4.1.pdf: In servercertificaten MOETEN het digitalSignature, keyEncipherment en de keyAgreement bit zijn opgenomen en zijn aangemerkt als essentieel.

Oplossing

Geadviseerd wordt om:
- Over te gaan op de private root van de PKIoverheid;
- Binnen de PKIoverheid het veld Subject.serialNumber te gebruiken om de EAN-code van de marktpartij op te nemen;
- Over te gaan op een certificaat voor authenticatie van het bericht/beveiligen van de verbinding en een (apart) certificaat (met andere kenmerken) voor het versleutelen van de berichtinhoud (vertrouwelijkheid).

De detaillering voor de diverse velden/attributen van de certificaten zal worden opgenomen in projectdocumentatie.

Impact

Overgang naar een private root van de PKIoverheid houdt in dat alle partijen, naast het wisselen van het eigen private certificaat en het publieke certificaat van de tegenpartij, tevens de Root-CA in hun systeemregister moeten toevoegen om de certificaten te kunnen verwerken.

Gebruik van het veld Subject.serialNumber voor de EAN-code van de marktpartij houdt in dat die partijen die er gebruik van maken de eigen software moeten aanpassen, om in een ander veld het betreffende kenmerk te vinden. Omdat EDSN dit kenmerk gebruikt voor de EAN-code controle (controle EAN-code in certificaat vs. EAN-code in bericht) heeft deze wijziging impact op de centrale systemen. Tevens heeft deze wijziging impact op markpartijen die deze controle hebben ingebouwd waarbij aangetekend moet worden dat een aantal marktpartijen deze EAN-code controle niet hebben ingebouwd omdat het berichten betreft die zij vanuit de centrale systemen ontvangen met enkel EDSN als verzender.

Invoeringsstrategie

De TC adviseert, conform het besluit van de ALV, de nieuwe certificaten los van een functionele sectorrelease in te voeren. Omdat de huidige certificaten vanaf 1 juni 2016 hun geldigheid verliezen is invoering per uiterlijk 1 juni 2016 gewenst.

Te vervallen issues

Geen.

Versieoverzicht

0.1 2015-08-06: Eerste aanzet door Roelof Dijkstra;
0.2 2015-08-07: Managementsamenvatting en kleine wijzigingen nav overleg met Jan de Jong (EDSN);
0.3 2015-08-12: Review van Gerrit Fokkema en toevoegen bijlagen met detaillering velden/attributen van de certificaten;
0.6 2015-09-28: Aanvulling certificaten voor Applicability Statement 2 (Wholesale Gas) en aanvulling voor authenticiteit- en servercertificaat (combicertificaat);
0.7 2015-10-02: Aanpassingen nav bijeenkomst TC en overhevelen van de bijlagen naar de project documentatie;
1.0 2015-10-28: Vaststelling door de ALV NEDU.