Baarnsche Dijk 4 D
3741 LR Baarn
www.edsn.nl
T (035) 54 80 180
F (035) 54 80 184

NEDU
Nederlandse Energie Data Uitwisseling

Issue TC018 Beveiliging berichtenverkeer via centrale P4

Status	Vastgesteld door ALV		
Versienummer	1.0	**Versiedatum**	06 juli 2011
Documentnaam	TC018 Beveiliging berichtenverkeer via centrale P4		

Behandeld door de Technische Commissie			
	IC Klant	**IC Wholesale–E**	**IC Wholesale-G**
Datum akkoord	**9 juni 2011**		

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

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

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

Vastgesteld door NEDU op 6 juli
Invoering met centrale protal P4

Contact	
Technische Commissie	TC@edsn.nl

Management samenvatting

EDSN zal een centraal P4 portaal bieden waar alle relevante marktpartijen (leveranciers (LV), regionale gasnetbeheerders (RNB-G) en overige dienstenaanbieders (ODA)) hun verzoeken tot leveren van meetdata (en op een later moment stuur- en schakelopdrachten) uit slimme meters kunnen indienen. Communicatie tussen Leveranciers, ODA's, RNB-G en EDSN geschiedt via een beveiligde verbinding (1) waarmee gewaarborgd wordt dat alleen bij EDSN bekende en toegelaten partijen deze verzoeken kunnen indienen. Een van de aspecten van een dergelijke beveiligde verbinding is dat de identiteit van de afzender geverifieerd kan worden. Hiertoe wordt gebruik gemaakt van een certificaat dat de identiteit van de afzender aantoont. Het transport van berichten over deze verbinding is niet 'af te luisteren' door onbevoegden.

Het centrale P4 portaal, dat EDSN in opdracht van de gezamenlijke netbeheerders zal gaan faciliteren, kent momenteel twee varianten:

A. 'Dunne' of eenvoudige variant: na identiteitscontrole van de afzender worden verzoeken en meetdata onbewerkt doorgezonden (2) naar de juiste RNB.
B. 'Dikke' of functioneel uitgebreidere variant: na identiteitscontrole van de afzender worden ook enkele functionele validaties toegepast op de inhoud van de berichten. Deze controles worden uitgevoerd met behulp van de inhoud van het C-AR. Alleen verzoekregels die deze inhoudelijke controle passeren worden doorgezonden (2) aan de juiste RNB ter verwerking.

De verwachting is dat na verloop van tijd (alle netbeheerders nemen deel in het C-AR) scenario B de standaard wordt.

Ook verbinding (2) in deze beide scenario's is een beveiligde verbinding. De beveiligingsmaatregelen zijn identiek aan die van verbinding (1). Het enige verschil is dat voor verbinding (2) gebruik gemaakt wordt van het certificaat van EDSN, terwijl voor verbinding (1) gebruik gemaakt wordt van de certificaten van elk van de individuele partijen.

Aan de TC is gevraagd of er naast de inzet van de hier genoemde beveiligde verbindingen aanvullende maatregelen getroffen moeten worden om te verzekeren dat de inhoud van de verzoeken die via verbinding (1) aangeboden worden ongewijzigd wordt doorgegeven via verbinding (2). Een tweede aspect waar de mening van de TC voor gevraagd is betreft of er aanvullende maatregelen moeten worden getroffen om te voorkomen dat er 'halverwege' de keten (EDSN) ongeoorloofd berichten of verzoeken kunnen worden aangemaakt en verzonden naar een RNB.

De TC is van mening dat:

- Er geen aanvullende maatregelen nodig zijn om te waarborgen dat verzoeken van marktpartijen ongewijzigd worden afgeleverd bij RNB's. Dit mede gezien de doorontwikkeling naar genoemde variant B, waarbij defacto geen sprake meer is van ongewijzigd doorzenden van berichten.
- Beveiligingsprotocollen zijn eerst en vooral ontworpen en bedoeld voor het beveiligen van het transport van informatie. Het gaat dan om het toepassen van beveiligde verbindingen en technieken als signing en encryptie. Ze betreffen *niet* het beveiligen van functionaliteit

tussen twee transporten in, dus bij de marktpartijen in hun systemen (zoals bijv. *firewalls* en ander security-beleid van die partij). Voor het automatiseringssysteem van de centrale P4 portaal geldt dat daarop adequate beveiliging in de zin van toegangscontrole (alleen wijzigbaar en toegang door geautoriseerd personeel) de enige ultieme beveiliging vormt. Net zoals nu al geldt voor de EDSN systemen.

Situatieschets:

In de Werkgroep P4 van 5 januari 2011 is aan de orde gesteld in welke mate de introductie van een (centraal) portal P4 vraagt om extra maatregelen in de sfeer van "privacy en security". In de Werkgroep P4 hebben enkele partijen zich afgevraagd of het risico bestaat op inbreuk/malversaties door onbevoegden op de IT-middelen behorende tot de centrale P4.
Aanleiding is dat bij de introductie van een centraal P4 portaal de communicatie tussen de aanvrager (Leverancier, ODA) en de (decentrale) P4 van de RNB in twee delen wordt opgesplitst:

Deel 1: communicatie tussen de aanvrager en de centrale P4.
Hierbij wordt gebruik gemaakt van het beveiligings-certificaat van de aanvrager (LV of ODA).
Deel 2: communicatie tussen de centrale P4 portaal en decentrale P4 bij de RNB.
Hierbij wordt gebruik gemaakt van het beveiligingscertificaat van de centrale P4.

Vraag:

Dienen aanvullende maatregelen genomen te worden om te verzekeren (danwel hierop te controleren) dat het oorspronkelijke bericht zoals verzonden in deel 1 van de communicatie (zie boven) (inhoudelijk) niet veranderd is/wordt in het tweede deel van de communicatie?
Ook wordt gevraagd of *additionele signing* veiligheid kan verhogen.

Overwegingen

Beveiligingsprotocollen zijn eerst en vooral ontworpen en bedoeld voor het beveiligen van het transport van informatie. Het gaat dan om het toepassen van beveiligde verbindingen en technieken als signing en encryptie. Ze betreffen *niet* het beveiligen van functionaliteit tussen twee transporten in, dus bij de marktpartijen in hun systemen. Want dan gaat het om bijv. *firewalls* en ander security-beleid van die marktpartij. Voor de centrale P4portaal geldt dat daarop adequate beveiliging in de zin van toegangscontrole (alleen wijzigbaar door geautoriseerd personeel) de enige ultieme beveiliging vormt. Net zoals nu al geldt voor de EDSN systemen.

Analyse in het licht van de introductie van de centrale P4 portaal

De verbinding tussen enerzijds de LV of ODA en anderzijds de centrale P4 portaal is beveiligd door het gebruik van de *industrie standaard* SOAP in casu het toepassen van HTTPs en het gebruik van certificaten. De tweede verbinding, van het centrale P4 portaal met de CTS van de netbeheerders, gebruikt dezelfde *standaard* dus is exact even veilig (referentie: WS-I Basic Profile 1.1). De centrale P4 portaal en de CTS van de netbeheerders kennen elkaars certificaat en kunnen daardoor uitgaan van betrouwbare informatie.

Plaats van signing in de beveiliging van berichtenverkeer

Op hoofdlijnen zijn er twee categorieën van beveiliging van berichtenverkeer:

- tussen gekoppelde computers ("point to point"). Hierbij gebruikt men TLS/SSL al dan niet in combinatie met client-authenticatie. Binnen de NEDU volstaan we tot op heden met deze vorm van beveiliging.
- tussen ontvanger en verzender "end to end". Daarbij gebruikt men "ondertekenen" ofwel "*signing*" op basis van W3C XML Digital Signature. Bovenop het ondertekenen kan dan nog encryptie van de inhoud van het bericht worden toegepast. Deze tweede categorie wordt wel gebruikt voor de routering en beveiliging van informatie over tussenliggende systemen. Men gebruikt "signing" dus typisch voor ketens als de voorliggende implementatie van de P4-keten.

Het eerste probleem dat opdoemt is dat de Nederlandse marktpartijen worden geconfronteerd met de ontwikkelkosten en risico's voor deze ontwikkelingen.
Het tweede probleem dat opdoemt bij het toepassen van *signen,* zoals beschreven, is dat we de *many-to-many* complexiteit die we dachten op te lossen met de introductie van de centrale P4 portaal weer terug brengen. Belangrijke uitgangspunten (bestaansrecht) voor de intrioductie van de centrale P4 portaal waren:

1. vereenvoudiging / vermindering van het aantal connecties;
   en
2. vereenvoudiging / vermindering van het certificaatbeheer bij alle partijen.

Voor een daadwerkelijke controle of een 'gesigned' (door oorspronkelijke afzender) document onderweg niet is veranderd moet ook het certificaat waarmee 'gesigned' is aan de ontvangende kant (RNB) bekend zijn. Dat conflicteert met uitgangspunt 2.

Tot slot kan *signen* van het oorspronkelijke document (en dat onveranderd doorzenden aan de uiteindelijke bestemming) ook alleen in het inmiddels beschreven '(functioneel)dunne centrale P4 portaal' scenario. Bij elke functionele opwaardering van dun naar dik(ker) vervalt onmiddellijk de waarde van het gesigned zijn van het brondocument. In een 'dikkere' variant zou de centrale P4 portaal de ontvangen berichten gaan lezen, bijvoorbeeld de aanvragen hergroeperen (per netbeheerder of type) en vervolgens anders gegroepeerd door zenden aan de netbeheerder(s). De additionele signing heeft dan geen betekenis meer, omdat de berichten niet 'verder' komen dan de Portal P4 en dan in een andere vorm worden doorgezonden of zelfs al worden verwerkt en beantwoord.

Oplossing:

Het berichtenverkeer voor P4 is beveiligd middels het transporteren via een beveiligde verbinding en het toepassen van een betrouwbaar, afzender specifiek certificaat. Additionele signing is vooralsnog niet noodzakelijk. Het brengt extra investeringen en implementatierisico's met zich mee en heeft een nadelig effect op de complexiteit en daarmee op de *kosten efficiënte* exploitatie van de P4-processen.

Omdat de verbinding tussen het centrale P4 portaal naar de CTS van de netbeheerders ten minste zal voldoen aan dezelfde veiligheidsmaatregelen als NEDU stelt aan de verbinding tussen LV/ODA met de portal P4 is er geen noodzaak voor extra maatregelen.

Impact:

Geen

Invoeringsstrategie:

Het issue kan direct na vaststelling van kracht worden.

Te vervallen issues:

Geen

Versieoverzicht:

0.1 Eerste aanzet door Gerrit Rentier / Ed van der Pijl na globale bespreking in de TC van 14 januari 2011 en vervolgens bespreking in de TC op 11 februari 2011. Dit advies is gecommuniceerd aan De WG P4.
0.2 Managementsamenvatting toegevoegd op 3 mei 2011;
0.3 Kleine aanscherping en beperking tot centrale P4 in de TC vergadering van 13 mei 2011 en akkoord voor beoordeling IC-Klant;
0.4 Na beoordelingen unanieme goedkeuring door IC-Klant ter vaststelling door de ALV;
1.0 Na vaststelling in de ALV NEDU op 6 juli 2011.