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 TC026 Tweezijdige authenticatie van verbindingen

Status	Vastgesteld door de ALV		
Versienummer	1.0	**Versiedatum**	1 april 2015
Documentnaam	TC026 Tweezijdige authenticatie 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	**-**
PV	**-**
MV	**-**
RNB	**-**
LNB	**-**
EDSN	**-**

Vastgesteld door NEDU op	**1 april 2015**
Invoering in markt per	**nvt**

Contact	
Technische Commissie	TC@edsn.nl

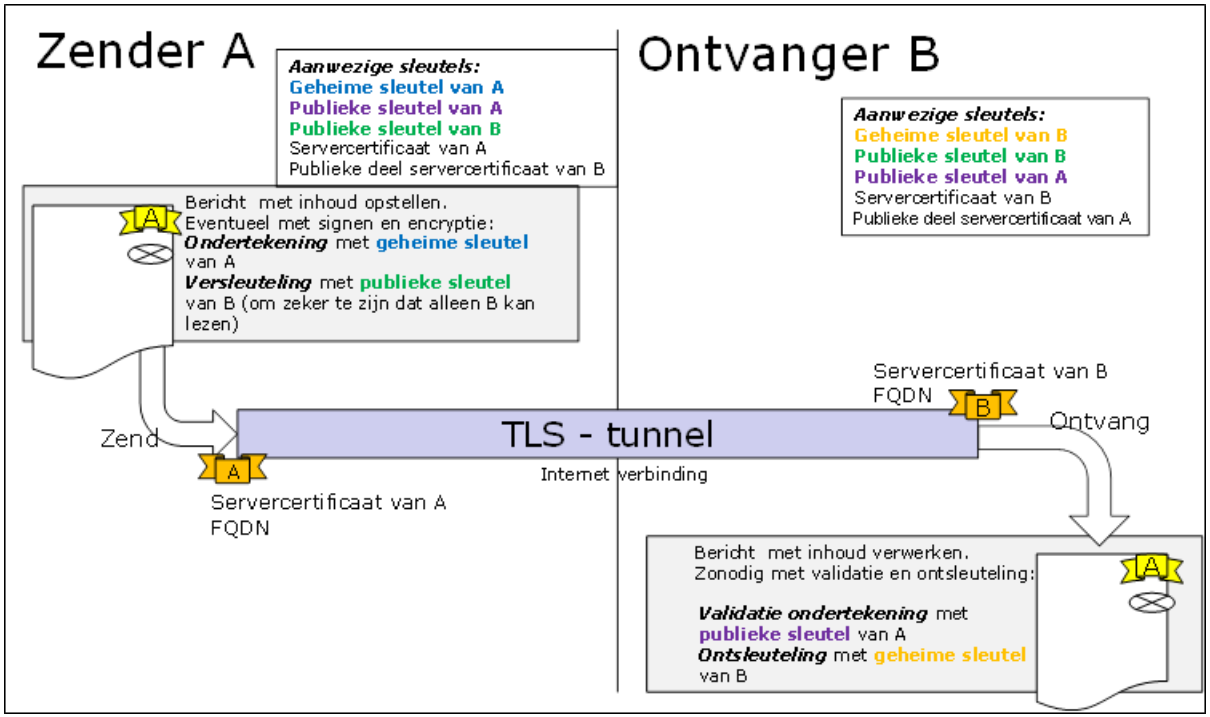
TC026: Tweezijdige authenticatie van verbindingen

Managementsamenvatting

Tweezijdige authenticatie m.b.v. servercertificaten op de verbinding

Beveiliging van de communicatie in de ketenprocessen tussen de partijen verenigd in de NEDU is een constant punt van aandacht. In issue TC024 is derhalve voorgesteld de beveiliging van de verbinding op een hoger plan te tillen door minimaal op TLS 1.2 te communiceren. Indien de vereiste wederzijdse herkenning niet op een andere manier (zoals via het bericht) kan worden geregeld is een optie om tweezijdige authenticatie op het niveau van transport (de netwerk laag) in te voeren.

Het berichtenverkeer van de markt wordt beschermd door beveiliging toe te passen op het niveau van transport en op het niveau van het bericht (de functionele inhoud). Op transportniveau wordt beveiligd volgens TLS standaarden. TLS (Transport Layer Security) is een protocol dat tot doel heeft om beveiligde en versleutelde verbindingen over het internet te verzorgen. TLS versleutelt alléén de verbinding en niet het bericht zelf dat over de beveiligde verbinding wordt verzonden. Om berichtversleuteling (signing en encryption) te bereiken kan gebruik gemaakt worden van de WS-security standaard of bijvoorbeeld AS2. Zie onderstaande afbeelding 1 voor een symbolische verduidelijking. In dit voorbeeld wordt gebruik gemaakt van zowel berichtversleuteling als van versleuteling op transportniveau (de TLS-tunnel).



Situatieschets:

Bij het opzetten van de verbinding tussen twee marktpartijen voor de uitwisseling van informatie wordt met TLS standaarden een versleuteling opgezet op basis van het gebruikte servercertificaat. Hierbij wordt een enkelzijdige authenticatie gebruikt, waarbij de aanvrager valideert dat hij de juiste (doel)server heeft bereikt, maar waarbij de server de aanvrager niet kan herkennen. Door gebruik te maken van enkelzijdige authenticatie wordt bereikt dat de verbinding tussen beide systemen wordt versleuteld (ter bescherming tegen een 'man-in-the-middle attack'). Bij tweezijdige authenticatie worden de certificaten van de systemen aan weerszijden van de verbinding gebruikt voor het opzetten van de beveiligde verbinding, waarbij de twee systemen elkaars identiteit vaststellen; de aanvrager weet met welke server gecommuniceerd wordt en de server weet met welke aanvrager gecommuniceerd wordt. Het is gebruikelijk om ook hierbij de verbinding te versleutelen.

Vraag:

Wat zijn de richtlijnen voor het inzetten van tweezijdige authenticatie op de transportlaag in de B2B verbindingen?

Overwegingen

Het verplichte gebruik van tweezijdige authenticatie op de transportlaag in de B2B verbindingen vergroot de beveiliging van de opgezette verbinding. Het wordt minder eenvoudig om een ongewenste verbinding op te zetten met de (doel)server. Het afluisteren of beïnvloeden van een verbinding door een derde partij wordt voorkomen.

Sommige verbindingen kennen al (afgedwongen) tweezijdige authenticatie, die afhangt van de eisen van de betreffende partijen (bilateraal geregeld).

Het transportgedeelte valt onder netwerkbeveiliging en het berichtgedeelte valt onder applicatiebeveiliging.
In veel gevallen is het gebruik van een beveiligde verbinding voldoende.
Om te verifiëren dat de juiste partijen met elkaar communiceren verdient het de voorkeur om de deze te linken aan de inhoud, ergo te koppelen aan het over de beveiligde verbinding verzonden bericht (het signen en eventueel encrypten met een (ander) certificaat van de inhoud van de over de verbinding gezonden informatie).
Alvorens dergelijke maatregelen te implementeren dient er een uit de BIV codering afgeleide maatregel zijn die dit expliciet vereist dan wel een zodanige situatie dat er geen afdoende alternatief is (dit kan optreden bij verouderde standaarden bijvoorbeeld). Alternatieven zijn bijvoorbeeld de authenticatie op berichtniveau te leggen, hashing op de berichten toe te passen of parallel extra berichten te sturen ('4 ogen simulatie'). Dus het toepassen van tweezijdige authenticatie op de verbinding zal beperkt blijven tot heel specifieke situaties.
Tweezijdige authenticatie op de verbinding vereist intensief certificaten beheer van alle betroffen (tegen)partijen. Verbindingspunten in het IT landschap van een partij worden veelal voor meerdere doelen/interacties gebruikt waardoor dit extra certificatenbeheer nodeloos complex is.

Oplossing:

Stel tweezijdige authenticatie op de transportlaag in B2B communicatie slechts in specifiek gevallen verplicht. Deze gevallen betreffen dan situaties dat de vereiste wederzijdse herkenning niet op een andere manier (zoals via het bericht) kan worden geregeld.
De tweezijdige authenticatie wordt gedaan met servercertificaten (tenminste x.509 SHA-2 certificaten).

Impact:

Tweezijdige authenticatie betekent dat partijen elkaars (publieke deel) van de servercertificaten moeten bezitten en kunnen herkennen. Dit impliceert organisatorisch en technisch een goed certificatenbeheer inrichten.

Invoeringsstrategie:

Daar waar de eisen vanuit de security (BIV classificatie) of bilaterale afspraken dit onder eerder genoemde overwegingen nodig maken.

Te vervallen issues:

Geen.

Versieoverzicht:

0.1 Eerste aanzet door Gerrit Fokkema op 11 november 2014;
0.2 Na eerste bespreking in de TC van 14 november;
0.3 Na bespreking in de TC van 12 december 2014 toevoegingen en besluit het issue aan te houden tot concrete behoefte vanuit BIV codering en maatregelen;
0.4 Na bespreking in de TC van 23 januari 2015 vrijgave als richtlijn;
0.5 Na bespreking en goedkeuring in de TC van 6 maart 2015;
1.0 Na vaststelling in de ALV van 1 april 2015.