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

NEDU
Nederlandse Energie Data Uitwisseling

Issue TC001 Security berichtenverkeer

Status:	Vastgesteld door ALV		
Versienummer:	2.0	**Versiedatum:**	13 november 2009
Documentnaam:	TC001 Security berichtenverkeer		

Behandeld door de Technische Commissie
Geaccepteerd door de Issue Commissie Klant op: 27 augustus 2009

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

Impact op keten	**Ja/nee**
berichten	**ja**
processen	**nee**
systemen	**ja**
overigen	

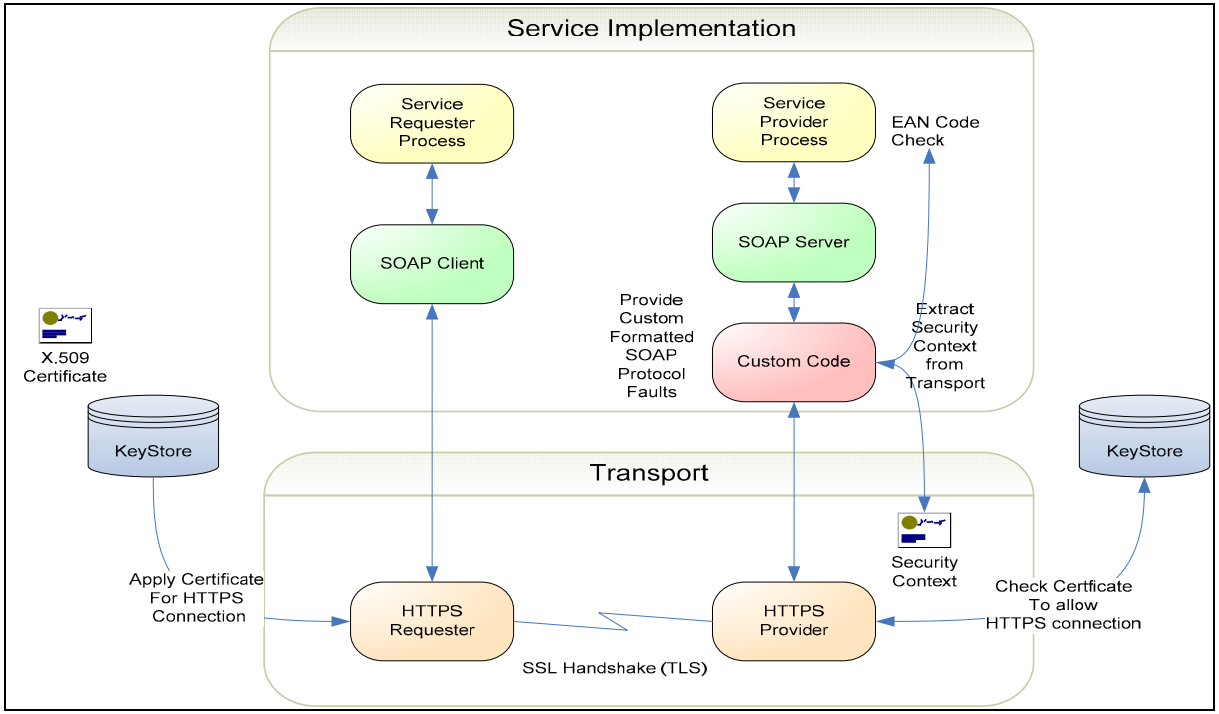
Vastgesteld door NEDU op	**11 november 2009**
Invoering in markt met de nieuwe bericht structuren	

Contact	
Technische Commissie	TC@edsn.nl

TC001: Security berichtenverkeer

Situatieschets:

In de huidige opzet van de nieuwe berichtenuitwisseling, die in het najaar 2008 door de Technische Commissie is gekozen, wordt door middel van de Diginotar (x.509) certificaten de verbinding (transportlaag) in hoge mate beveiligd. Na het opzetten van de beveiligde verbinding wordt voor de reguliere berichten geen extra beveiliging meer geregeld.
Effect is echter dat, om de juiste authenticatie en autorisatie te doen, de service-implementatie bij ontvangende partij uit het certificaat gegevens moet peuteren die alleen op verbindingsniveau beschikbaar zijn. Hiervoor is geen standaard software beschikbaar. Dit leidt bij partijen tot extra maatwerk-ontwikkeling en onderhoudswerk (zo leren ervaringen opgedaan met de P4).



Huidige werkwijze leidt tot extra maatwerk (custom code)

Vraag:

Kan er voor grootschalige implementatie van de nieuwe berichten structuren een standaard worden ingevoerd die leidt tot minder extra (programmeer)werk en kosten?

Overwegingen

De TC streeft er naar om zoveel mogelijk conform internationaal geaccepteerde (en dus in standaard tools geïmplementeerde) standaarden te werken opdat implementatie configureerbaar wordt zonder programmeerinspanningen.

Oplossing:

De Technische Commissie stelt voor om de beveiliging op het berichten verkeer voor invoering van de nieuwe berichten en processen aan te passen door de beveiliging op transport (met certificaat) en op bericht (met certificaat) te scheiden.
Hierdoor worden bij partijen extra programmeer inspanningen voorkomen en daarmee de ontwikkel en beheer inspanningen verlaagd.

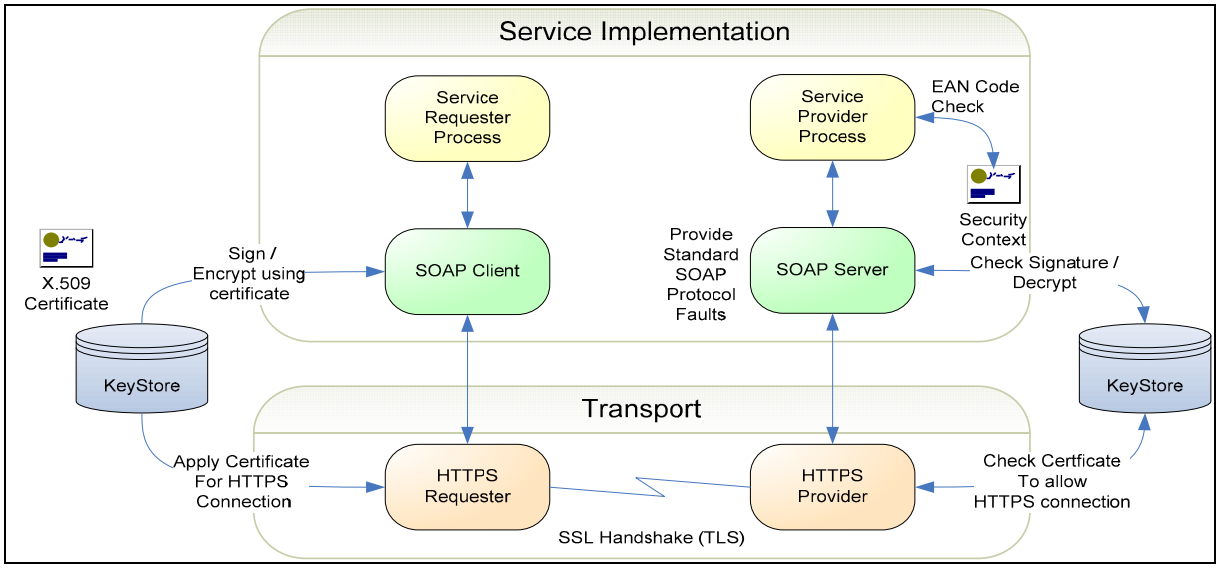
Er is een sterke voorkeur om de beveiliging in de transport laag te scheiden van die in de inhoud. Dit betekent dat we naast de transportlaag ook een certificaat gaan hanteren om de inhoud te beveiligen.

- Op transportniveau:
  - We blijven gebruik maken van het x.509 certificaat om een vertrouwde verbinding op te zetten (TLS handshake);
  - Deze implementatie wijzigt dus feitelijk niet, alleen de controle op EAN code uit de TLS security context op service-niveau wordt vervangen door een vergelijkbare controle tegen de security context op berichtniveau.
- Op berichtniveau:
  - Het(zelfde) x.509 certificaat voor signen of zelfs encryptie van de inhoud. Deze methode biedt voldoende beveiligingsmogelijkheden.
  - Op deze wijze is de gesignde inhoud bepalend voor de authenticatie en de autorisatie op berichtniveau. De oorspronkelijke EAN Code controle wordt dan op serviceniveau gedaan door de Organisational Unit (OU) uit de signature van het bericht te matchen met het 'SENDER_ID' uit de inhoud van hetzelfde bericht.

Het inrichten van de autorisatie (op functie en op data) is des ontvangers.

Bijkomend voordeel van de loskoppeling van verbinding- en berichtenbeveiliging is dat een bedrijfsonderdeel (in een uitwijkscenario) eventueel gebruik zou kunnen maken van de verbinding van een ander bedrijfsonderdeel; tenslotte is de verbinding vertrouwd en de berichten worden nog steeds namens de juiste marktpartij gesigned. Dit biedt meer flexibiliteit.
Samengevat:

1. Transport: SSL /TLS met x.509 certificaten op organisatie niveau;
2. Inhoud: signen met x.509 (organisatie of marktpartij). Dit certificaat is leidend voor de authenticatie en autorisatie (volgens eigen implementatie). De certificaten voor de Transport en Inhoud zijn onafhankelijk van elkaar.



Voorgestelde werkwijze: standaard SOAP server voldoet

De wijze waarop het certificaat in de Inhoud wordt opgenomen, conform de SOAP Message Security 1.1 (WS-Security), in een standaard onderdeel van de berichten staat gespecificeerd in de bijlage.

Meerdere niveaus berichtbeveiliging

We willen hooguit twee of drie niveaus van beveiliging van de berichten onderkennen:

1. Standaard niveau: alle reguliere berichten en ook de categorie "geen beveiliging nodig" zal onder de standaard vallen. Van deze berichten wordt alleen de SOAP Header gesigend met het x.509 certificaat van de aanvragende marktpartij. Encryptie wordt hier niet toegepast om de load op betrokken systemen binnen de perken te houden.
2. Hogere beveiliging voor privacy (of hoge impact imago schade) dan wel risico's op verstoring van de energielevering: deze gaan we signen met (de private key van) het x.509 certificaat van de aanvragende marktpartij en encrypten met (de public-key van) het x.509 certificaat van de ontvangende partij.

Invoeringsstrategie:

Invoering met de invoering van de nieuwe webservice/xml berichtenverkeer voorkomt onnodige ontwikkelinspanningen.

Versieoverzicht:

0.1 eerste versie vanuit reeds aan IC-Klant aangeboden stuk van bespreking in TC op 15 mei 2009;
0.2 na schriftelijke review ronde TC over ter beoordeling IC Klant op 19 juni 2009;
1.0 na vaststelling door de ALV NEDU op 8 juli 2009;
1.1 hoe het certificaat in de berichten mee te nemen, opgenomen in de bijlage, akkoord door de TC op 21 augustus 2009;
1.2 na acceptatie door de IC-Klant op 27 augustus 2009 en verduidelijking signen en encrypten op pag 4;
2.0 Na vaststelling door de ALV op 11 november 2009.

Bijllage

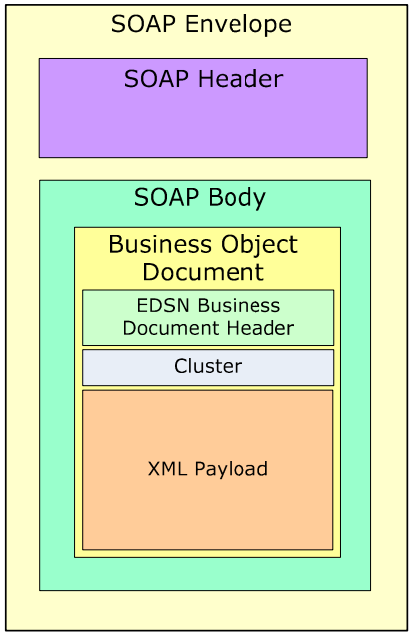
SOAP Message Security
De SOAP Message Security 1.1 (WS-Security) is een OASIS Standaard Specificatie, gedateerd op 1 februari 2006. Deze standaard specificatie biedt een framewerk voor beveiliging van het berichtenverkeer en wordt ondersteund door gangbare "middleware" tools. Deze specificatie sluit aan bij het streven van de TC om conform internationaal geaccepteerde en geïmplementeerde standaarden te werken.
Voor het toepassen van WS-Security, moet er een SOAP Header in de SOAP Envelope worden opgenomen. Deze SOAP Header omvat onder andere de WS-Security informatie.
OASIS schrijft de volgende structuur voor:

```
<Envelope>
  <Header>
    <Security>
    </Security>
  </Header>
  <Body>
  …
  </Body>
</Envelope>
```

Het bericht (Business Object Document) wordt opgenomen in de Body. Dit bericht heeft een eigen, functionele header, de EDSNBusinessDocumentHeader. Deze header staat los van de SOAP Header.

De OASIS Standaard Specificatie Message Security 1.1 (WS-Security) wordt integraal op genomen in de SOAP Header voor het NEDU berichtenverkeer.

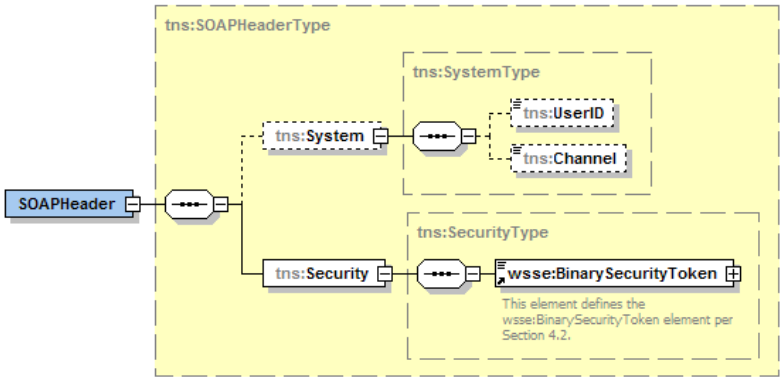
Weergave structuur in "containers":



Definitie SOAP Header
De WS-Security structuur in de SOAP Header is gebaseerd op WS-Security XML Schema's zoals die door OASIS worden uitgegeven.

De SOAP Header voor het NEDU berichtenverkeer valt in twee delen uiteen:

1. System deel, is optioneel en wordt alleen gebruikt voor het uitwisselen van technische informatie tussen E-MP en achterliggende EDSN business applicaties;
2. Security deel, gebaseerd op WS-Security, verplicht te gebruiken in uitwisseling tussen partijen.



In het element <wsse:BinarySecurityToken>, onderdeel van de WS Security 1.1 standaard, moet het x.509 certificaat voor beveiliging op berichtniveau opgenomen worden. De certificaten voor beveiliging op Transport niveau en op Bericht niveau zijn van dezelfde structuur (x.509) en zijn veelal dezelfde.
Aan de eis voor beveiliging op berichtniveau wordt voldaan door het element <wsse:BinarySecurityToken> als verplicht veld op te nemen.

Referenties
Het Security deel omvat de volgende OASIS XML Schema's:

- http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd;
- http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd;
- http://docs.oasis-open.org/wss/v1.1/oasis-wss-wssecurity-secext-1.1.xsd.

Alle documenten met betrekking tot de OASIS Standaard Specificatie Message Security 1.1 (WS-Security) zijn beschikbaar en kunnen geraadpleegd worden via de volgende URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.

Het document met de beschrijving van de OASIS Standaard Specificatie Message Security 1.1 (WS-Security) is als PDF beschikbaar, URL: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf.