Barchman Wuytierslaan 6
3818 LH Amersfoort
www.nedu.nl

Issue SC002 Uitfaseren AS2

Status	Vastgesteld		
Versienummer	1.0	**Versiedatum**	18 januari 2017
Documentnaam	SC002 Uitfaseren AS2 v1.0.docx		

Behandeld door de Security Commissie

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

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

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

Vastgesteld door NEDU op	**14 december 2016**
Invoering in markt per	**vanaf voorjaar 2018**

Contact	

Management samenvatting

Situatieschets:

Momenteel wordt het AS2 protocol in de Nederlandse gasmarkt gebruikt voor het uitwisselen van informatie in de wholesale gas processen.

Met ingang van 1 mei 2016 is de Verordening (EU) 2015/703 in werking getreden. Op grond hiervan dient de op documenten gebaseerde gegevensuitwisseling m.b.t. transacties op internationale uitwisselpunten - de zogenaamde interconnectiepunten – plaats te vinden door middel van het AS4 protocol (vgl. art. 20 e.v.[1])

Gelet op artikel 23, tweede lid heeft GTS aan ACM toestemming gevraagd om het AS2-protocol te mogen blijven gebruiken. ACM heeft GTS toestemming gegeven om uiterlijk 3 mei 2018 over te gaan op AS4 (ACM/DE/2016/202529). Tot dan toe mag GTS het protocol AS2 voor het internationale berichtenverkeer gebruiken.

---

[1] *Artikel 20* Algemene bepalingen

1. In dit hoofdstuk wordt onder „wederpartijen" verstaan, netgebruikers die actief zijn in: a) interconnectiepunten; of b) zowel interconnectiepunten als virtuele handelspunten.
2. Aan de gegevensuitwisselingseisen overeenkomstig punt 2.2 van bijlage I bij Verordening (EG) nr. 715/2009, Verordening (EU) nr. 984/2013, Verordening (EU) nr. 312/2014, Verordening (EU) nr. 1227/2011 en de onderhavige verordening tussen transmissiesysteembeheerders en van transmissiesysteembeheerders naar hun wederpartijen wordt voldaan aan de hand van de in artikel 21 omschreven gemeenschappelijke oplossingen voor de uitwisseling van gegevens.

Artikel 21 Gemeenschappelijke oplossingen voor de uitwisseling van gegevens

1. Afhankelijk van de in artikel 20, lid 2, neergelegde gegevensuitwisselingseisen kunnen één of meer van de volgende types van gegevensuitwisseling worden gebruikt: a) op documenten gebaseerde gegevensuitwisseling:de gegevens worden in de vorm van een bestand en automatisch uitgewisseld tussen de respectieve IT-systemen; b) geïntegreerde gegevensuitwisseling:de gegevens worden uitgewisseld tussen twee applicaties die zich direct op de respectieve IT-systemen bevinden; c) interactieve gegevensuitwisseling:de gegevens worden op interactieve wijze uitgewisseld met behulp van een webapplicatie via een browser.
2. De gemeenschappelijke oplossingen voor de uitwisseling van gegevens omvatten het protocol, het gegevensformaat en het netwerk. Voor elk van de in lid 1 genoemde types van gegevensuitwisseling worden de volgende gemeenschappelijke oplossingen voor de uitwisseling van gegevens gebruikt: a) voor de op documenten gebaseerde gegevensuitwisseling: i) protocol: AS4; ii) gegevensformaat: Edig@s-XML of een equivalent gegevensformaat dat een identieke mate van interoperabiliteit waarborgt. Het ENTSOG publiceert een dergelijk equivalent gegevensformaat; b) voor de geïntegreerde gegevensuitwisseling: i) protocol: HTTP/S-SOAP; ii) gegevensformaat: Edig@s-XML of een equivalent gegevensformaat dat een identieke mate van interoperabiliteit waarborgt. Het ENTSOG publiceert een dergelijk equivalent gegevensformaat; c) voor de interactieve gegevensuitwisseling: protocol HTTP/S. Voor alle types van gegevensuitwisseling als omschreven onder a) tot en met c), is het netwerk het internet.
3. (…)

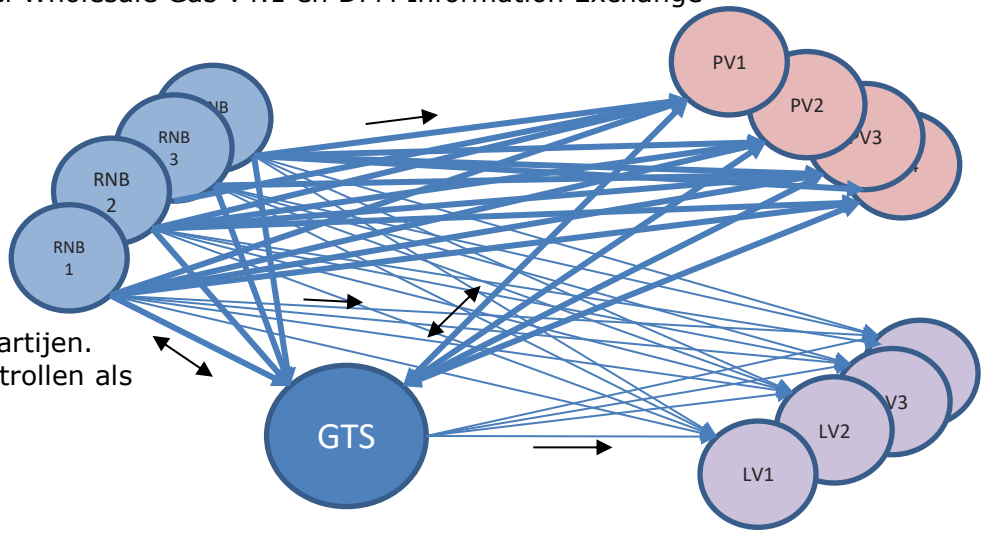
Artikel 23 Tenuitvoerlegging van de gemeenschappelijke oplossingen voor de uitwisseling van gegevens

1. Afhankelijk van de gegevensuitwisselingseisen overeenkomstig artikel 20, lid 2, stellen de transmissiesysteembeheerders alle in artikel 21 omschreven gemeenschappelijke oplossingen voor de uitwisseling van gegevens ter beschikking en gebruiken zij die.
2. Wanneer er op de datum van inwerkingtreding van deze verordening reeds oplossingen voor de uitwisseling van gegevens tussen een transmissiesysteembeheerder en de betrokken wederpartijen beschikbaar zijn en wanneer deze bestaande oplossingen voor de gegevensuitwisseling verenigbaar zijn met artikel 22 en met de gegevensuitwisselingseisen overeenkomstig artikel 20, lid 2, kunnen die bestaande oplossingen voor de uitwisseling van gegevens na raadpleging van de netgebruikers van kracht blijven mits deze worden goedgekeurd door de nationale regulerende instantie van de transmissiesysteembeheerder.

AS 2

AS2 wordt in de Nederlandse gasmarkt gebruikt sinds 2004 voor het uitwisselen van informatie in de wholesale gas processen, zoals de allocatie en reconciliatie gerelateerde berichten (zie MPM Market Model Wholesale Gas v4.1 en DPM Information Exchange

- Allocatie:
  - LALL
  - BALL
  - MINFO
  - CINFO
  - TINFO
  - OVEXIT
- Reconciliatie:
  - RNINFO
  - RSINFO
- Nominatie berichten



De uitwisseling is een zogenaamde peer-to-peer uitwisseling tussen partijen. De informatiestromen verlopen schematisch tussen de volgende marktrollen als in het nevenstaande plaatje weergegeven.

Het AS2 protocol wordt gebruikt met de volgende instellingen (bron EASEE-gas CBP 2007-003/01):

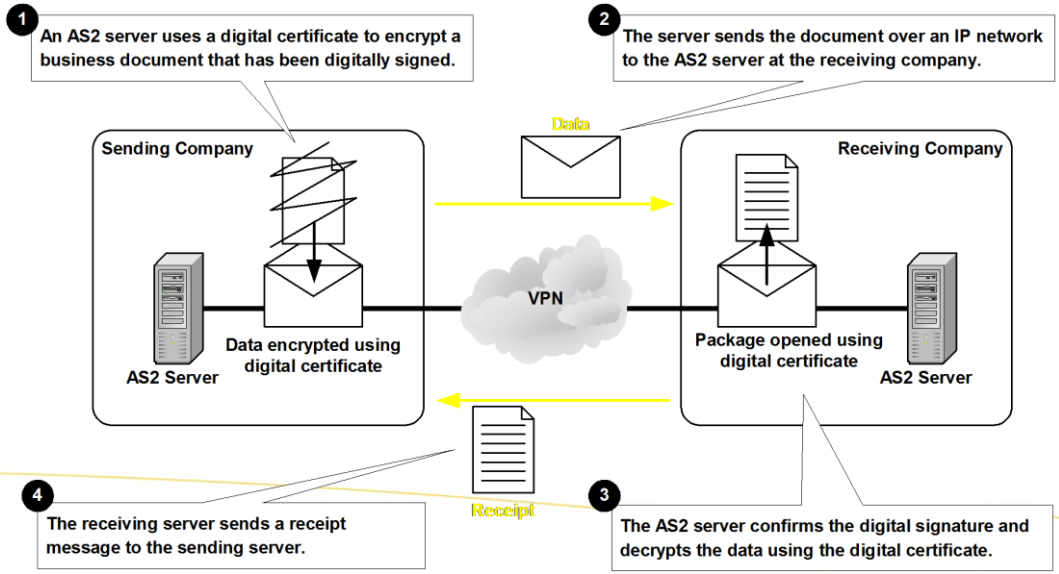
Configuration Parameters for the AS2 Protocol

Sending and receiving servers must be reachable via fixed public IP addresses

Encryption:	3DES
Signing:	SHA1
Compression:	On
Message Disposition Notification (MDN):	Signed (Mandatory) Synchronous (Highly Recommended)
AS2 System Identifiers:	AS2-From/AS2-To same as ZEW code list in Edig@s catalogue
TCP Port Number:	Http – default port 80 Https – default port 443

Het concept van het AS2 protocol is hiernaast in een plaatje weergegeven.

De lijnverbinding (Https) wordt sinds kort beveiligd met TLS1.2, i.c.m. een SHA2 beveiligingscertificaat.



Vraag:

Kan het AS2 protocol beveiligingstechnisch nog langer worden gebruikt voor de uitwisseling van de genoemde berichten in de Nederlandse markt?

(Risico) Overwegingen

Hoewel de huidige toepassing van AS2 binnen de markt (inclusief mitigerende maatregelen) momenteel geen acuut technisch beveiligingsrisico met zich meebrengt, is vanwege de verouderde technologie er een (snel) toenemende kans dat de beschikbare encryptie zal worden gekraakt.
Nagegaan is wat het standpunt van het NCSC in deze problematiek is (de Security Commissie za zich sterk laten leiden door de adviezen van deze nationale beveiligingsinstantie). Het NCSC geeft geen directe adviezen m.b.t. tot AS(X). In het document "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)" wordt wel een oordeel gegeven over de gebruikte encryptiemethodieken.
Binnen AS2 wordt de encryptie standaard 3DES gebruikt, hiervoor is er een betere methode beschikbaar (AES), maar 3DES voldoet (voorlopig) nog wel aan de stand van de techniek.
Daarnaast verloopt het signing algoritme binnen het AS2 protocol volgens SHA1, dat niet meer voldoet aan de stand van de techniek. Er bestaat derhalve een toenemende kans dat de beschikbare encryptie zal worden gekraakt en dat er op dat moment wel een technisch beveiligingsrisico is. Er worden voor de digitale ondertekening wel SHA2 certificaten gebruikt.
Tevens is getoetst wat de consequenties voor de marktprocessen zijn:

> De zwakheid van AS2 heeft consequenties voor het dreigingsscenario "Unauthorized monitoring and/or modification of communications". De inschatting van de Commissie is dat de kans van optreden hiervan op dit moment nog laag is. De komende jaren zal de effectiviteit van de controls (encryptie) met AS2 naar het zich laat aanzien sterk verminderen waardoor de kans van optreden aanzienlijk groter wordt. Dit zal leiden tot een verhoogd risico voor de marktprocessen die gebruik maken van het AS2 protocol voor uitwisseling van de berichten, zoals Nominaties, Allocaties en Reconciliaties.
> Vooruitlopende op de nog definitief op te stellen risico-analyses op de ketenprocessen met behulp van Qdrant methodiek is de Commissie op grond van de huidige (mogelijk beperkte) inzichten van mening dat dit risico op redelijke termijn dient te worden gemitigeerd (let wel dat deze uitspraak over de risico's voor de business processen pas gefundeerd kan worden gedaan als op basis van de methodiek alles is ingevuld, hetgeen momenteel nog in uitwerkingsfase verkeert[2]).

Het streven in de sector moet zijn om de beveiliging van de informatieuitwisseling zoveel mogelijk aan de laatst mogelijke security eisen te laten voldoen en de als onveilige aangemerkte protocollen uit te faseren.

---

[2] De aanpak van een dergelijke risico analyse bestaat een aantal stappen :

1. Een beeld krijgen van de technische achtergrond en daaraan gerelateerde technische risico's m.b.t. het issue;
2. Bepalen op welke risicoscenario's uit de dreigingenanalyse het issue betrekking heeft en wat de invloed van het issue op deze risicoscenario's is;
3. Als de optredingskans van een scenario hoger wordt, bepalen op welke objecten uit de Qdrant deze risicoscenario's betrekking hebben;
4. Bepalen welke BIV coderingen van toepassing zijn en of de maatregelen, die hierop betrekking hebben, nog afdoende zijn;
5. Eventueel maatregelen treffen (die ook weer verwerkt worden in de controles van de dreigingenanalyse).

Oplossing:

In lijn met het aangehaalde ACM-besluit is de conclusie dat de security risico's ten aanzien van het gebruik van AS2 de komende jaren dermate zullen toenemen en dat dit aanleiding is om dit protocol binnen een termijn van enkele jaren uit te faseren.

Impact:

Uitfaseren van AS2 betekent overgang op een andere, nog nader te bepalen standaard. Dit zal impact hebben op alle betreffende marktpartijen om hun systemen tijdig in te richten.

Invoeringsstrategie:

De SC adviseert om SC002 (uitfaseren AS2) in te voeren overeenkomstig de in TC034 beschreven invoeringsstrategie.

Te vervallen issues:

N.v.t.

Versieoverzicht:

0.1 Eerste aanzet door Gerrit Fokkema en Marcel Kerkhof, 07-07-2016;
0.2 Na review commentaar SC;
0.3 Na kwetsbaarhedenanalyse Sander Dortland, 19-08-2016;
0.4 Na review commentaar Martijn Hamberg, 28-11-2016;
0.5 Na review commentaar SC voorafgaand aan goedkeuring SC, 06-12-2016;
0.9 Ter vaststelling aangeboden aan ALV NEDU, 07-12-2016;
1.0 Na vaststelling, samen met TC034, in de ALV van 14-12-2016.