TC036

BERICHTINHOUD BEVEILIGING TMR

Heeft het issue impact op..?	
Grootverbruik	
Kleinverbruik	**X**
Elektriciteit	**X**
Gas	**X**
RNB	
LNB	
LV	**X**
MV	
PV	
EDSN	**X**
Codes	
Berichten	
Ketenprocessen	
Privacy	
Is het issue release afhankelijk/onafhankelijk en welke invoeringsdatum heeft het issue.	
Release-afhankelijk	**VJ2018**
Release-onafhankelijk	**certificaatwissel vóór 22 december 2017**

Nummer TC036
Datum 24-05-2017
Versie 1.0
Status Vastgesteld

Opsteller(s) Gerrit Fokkema

Inhoudsopgave

COLOFON

VERSIEBEHEER

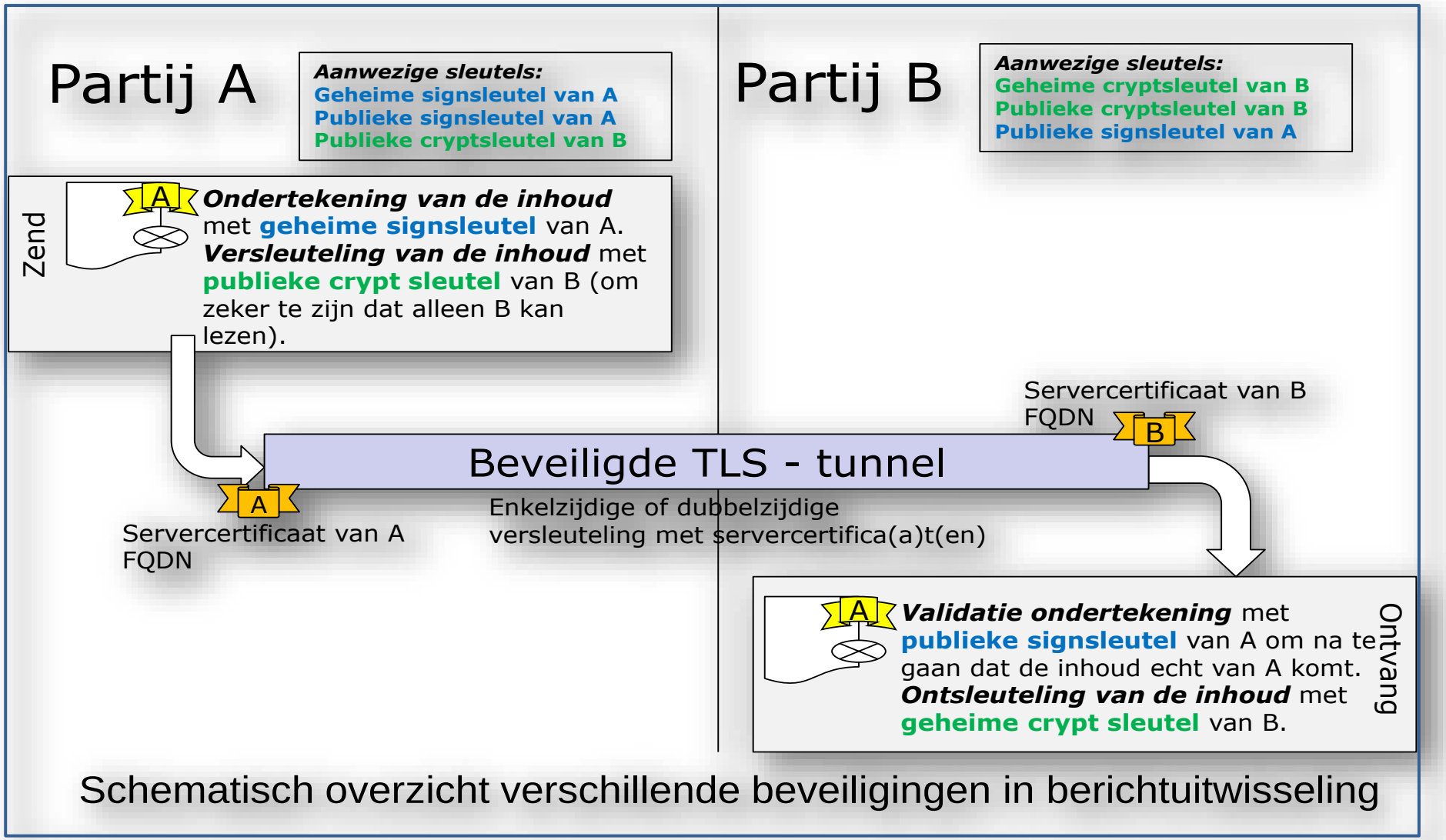
Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet, na bespreking in de TC van 31 maart 2017	Gerrit Fokkema	31-03-2017
0.2	Ter vaststelling	Enige aanscherpingen n.a.v. review door de TC en SC leden.	Gerrit Fokkema	07-04-2017
0.3	Ter vaststelling	Na opmerking van de SPC kleine aanscherping in tekst t.a.v. de certificaatwissel	Gerrit Fokkema	12-05-2017
1.0	Vastgesteld	Na vaststelling in de ALV NEDU vergadering van 24 mei 2017	Gerrit Fokkema	24-05-2017

DISTRIBUTIE

		Verstuurd (versie/datum)			
	0.1	**0.2**	**0.3**	**0.9**	**1.0**
Gremium	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj		dd-mm-jjjj
TC	31-03-2017	07-04-2017	12-05-2017		
SC	31-03-2017				
SPC		20-04-2017			
ALV NEDU				16-05-2017	
Allen					24-05-2017

PROBLEEMDEFINITIE

Onderdeel	Omschrijving
De ontwikkeling betreft:	De sector heeft gekozen voor PKIoverheid certificaten te gebruiken (TC027). Het Toegankelijk MeetdataRegister (TMR) beveiligt de informatie-uitwisseling met de marktpartijen op een aantal aspecten: - Door toepassing van PKI-Overheid servercertificaten wordt er een beveiligd communicatiekanaal opgezet (o.b.v. TLS 1.2); - Door toepassing van PKI-Overheid certificaten wordt d.m.v. signing de integriteit van de informatie in een bericht gewaarborgd. Signing vindt plaats met hetzelfde servercertificaat als voor het beveiliging van de communicatie/transport; - Door toepassing van certificaten (niet onder de PKIoverheid-root maar onder een KPN eigen private root) wordt d.m.v. encryptie van de inhoud van het bericht de vertrouwelijkheid van de informatie in een bericht gewaarborgd. Het huidige vertrouwelijkheidscertificaat van TMR vervalt per 22 december 2017. KPN ondersteunt als certificatenuitgever de softwarematige uitlevering van de vertrouwelijkheidscertificaten, ook die onder de KPN eigen private root, niet meer. Voor 22 december 2017 zal er een oplossing moeten zijn geïmplementeerd t.a.v. het vertrouwelijkheidscertificaten gebruik in TMR om de continuïteit van de informatie-uitwisseling te borgen.
En raakt:	De afnemers van de betreffende services van TMR: Leveranciers en EDSN.
Als gevolg waarvan:	Leveranciers niet meer gebruik kunnen maken van de TMR B2B webservices om meetdata te raadplegen.
Een goede oplossing moet:	De uitwisseling van de gegevens vanuit TMR voldoende veilig houden. TMR ook na 22 december 2017 beschikbaar houden via B2B kanaal tegen redelijke kosten voor betrokken partijen. Investeringen in TMR in balans houden met de fase van de life cycle waarin de applicatie zich bevindt.
Of deze doelen worden behaald, kan worden gevalideerd door:	Ongestoorde dienstverlening door TMR aan de Leveranciers.
Opdrachtgever te realiseren oplossing	NEDU
Probleemeigenaar	TC


Partij A
Aanwezige sleutels:
Geheime signsleutel van A
Publieke signsleutel van A
Publieke cryptsleutel van B
Partij B
Aanwezige sleutels:
Geheime cryptsleutel van B
Publieke cryptsleutel van B
Publieke signsleutel van A
Zend
A
Ondertekening van de inhoud met geheime signsleutel van A.
Versleuteling van de inhoud met publieke crypt sleutel van B (om zeker te zijn dat alleen B kan lezen).
Servercertificaat van B
FQDN
B
Beveiligde TLS - tunnel
A
Servercertificaat van A
FQDN
Enkelzijdige of dubbelzijdige versleuteling met servercertifica(a)t(en)
A
Validatie ondertekening met publieke signsleutel van A om na te gaan dat de inhoud echt van A komt.
Ontsleuteling van de inhoud met geheime crypt sleutel van B.
Ontvang
Schematisch overzicht verschillende beveiligingen in berichtuitwisseling

OVERWEGINGEN

De uitwisseling van berichten in de sector gebeurt met ‘server to server’ communicatie, die beveiligd is met de inzet van certificaten (op basis van TLS 1.2). Het beveiligingscertificaat waarvan gebruik wordt gemaakt betreft een zogenaamd servercertificaat, conform marktafspraak (TC027) onder de PKIoverheid-root.

Enkele applicaties gebruiken ook nog een certificaat voor het signen van de berichtinhoud, zoals de P4 berichten en de berichtuitwisseling van en naar TMR. Dit wordt meestal gedaan met hetzelfde servercertificaat als gebruikt voor de beveiliging van de verbinding.

Alleen TMR hanteert ook encryptie van de inhoud van de berichten onder gebruikmaking van een speciaal vertrouwelijkheidscertificaat voor encryptie. Deze certificaten moeten conform de eisen van het PKIoverheid-stelsel aan een aantal voorwaarden voldoen die leiden tot hoge additionele kosten. De separate vertrouwelijkheidscertificaten mogen niet, zoals de servercertificaten, softwarematig worden uitgeleverd. Hiertoe moet een zogenaamd Secure User Device (SUD), zoals een smartcard, HSM of beveiligde USB stick, .worden gebruikt. Aangezien het gaat om B2B berichten zullen alle betrokken partijen dan een SUD dienen in te zetten, wat resulteert in hardware-matige aanpassingen op de decentrale en centrale systemen om de certificaten te kunnen gebruiken.

De vertrouwelijkheidscertificaten, die in TMR worden gebruikt voor de encryptie van de berichtinhoud, zijn nog niet onder de PKIoverheid root gebracht en functioneren nog als tijdelijke overbruggingsmaatregel. Ze vallen op dit moment onder een private root van KPN. De ondersteuning van KPN voor deze tijdelijke constructie vervalt per 21 december 2017. Verlenging van deze tijdelijke constructie is niet mogelijk.

Als er niet tijdig actie wordt ondernomen zullen de TMR B2B webservices niet meer toegankelijk zijn per 22 december 2017.

De volgende alternatieven worden onderkend:

1. Introduceer HSM’s op TMR en bij alle marktpartijen, zoals KPN, als uitgever van de certificaten, en de PKIoverheid richtlijnen voorschrijven;
    - Smartcards of usb-sticks voldoen niet voor B2B webservices omdat dan voor elk bericht handmatig een validatiecode moet worden opgegeven;
    - Dit levert hoge kosten op in de sector (HSM’s zijn dure voorzieningen).
2. Verwijder de encryptie op de berichtinhoud van TMR, zodat de werking meer in lijn komt met de rest van de berichtenuitwisseling (en de uitwisseling van de meetdata);

- Dit vereistaanpassingen in de systemen en extra testen bij alle betrokken partijen.

3. Gebruik (tijdelijk) een niet-PKIoverheid vertrouwelijkheidscertificaat voor de encryptie;

    - Geen aanpassingen bij partijen, behoudens een ‘gewone’ certificaatwissel;
    - Keuze uit
        - Gebruik van een erkende certificaatuitgever(CA, als die te vinden is tegen acceptabele kosten);
        - EDSN genereert en distribueert de certificaten als tijdelijke overbrugging.

Risicoafwegingen

- De met TMR uit te wisselen gegevens betreffen vastgestelde meterstanden en verbruiken. Deze standen zijn al eerder uitgewisseld tussen de marktpartijen, met berichten die (alleen) zijn beveiligd door encryptie op de verbinding. Standen worden ook via de P4 uitgewisseld, waar ook geen sprake is van encryptie van de berichtinhoud. Dit leidt tot de stelling dat de encryptie van de meetdata uit TMR (op berichtinhoud) vanuit risicobeheersing niet strikt noodzakelijk is;
- De wijze waarop de encryptie van de inhoud van de berichten van TMR is ingericht is niet conform de standaardrichtlijnen, waardoor de beveiligingswaarde minder is;
- Er zijn geen vastgestelde eisen in de sector die aangeven dat de inhoud van de meetdataberichten (van TMR) dient te worden versleuteld (naast gebruik van beveiligde verbinding en de signing van de berichten);
- Het toevoegen van dure voorzieningen en aanpassingen om de encryptie van de inhoud van de berichten TMR aan de eisen van PKIoverheid te laten voldoen kent geen of onvoldoende grondslag;
- Door de encryptie van de inhoud van de berichten van TMR te verwijderen zijn de gegevens nog minstens zo goed beschermd als andere meetdata-uitwisselingen in de ketenprocessen.

TMR staat op de nominatie op niet al te lange termijn te worden uitgefaseerd in het kader van de optimalisatie van de meetketen, hetgeen hoge investeringen niet verantwoord maakt.

GEKOZEN OPLOSSING

De TC ziet geen redenen voor het handhaven van de bericht encryptie voor TMR en stelt voor die te verwijderen uit de B2B webservices van TMR.

Echter het vóór 22 december 2017 omschakelen naar de informatie uitwisseling zonder inhoudsencryptie vereist dat alle partijen deze overgang gelijktijdig doorvoeren. De termijnen om een dergelijke (kleine) sectorrelease te organiseren zijn erg kort.
De TC ziet de volgende implementatie scenario's:

a) de encryptie van de inhoud op de berichten van TMR weg te halen in of parallel aan de najaarsrelease 2017;
b) de encryptie van de inhoud op de berichten van TMR weg te halen in de voorjaarsrelease 2018. De betreffende TMR berichten worden in deze release vanwege de Dataveiligheid inhoudelijk aangepast;
c) de encryptie van de inhoud op de berichten van TMR weg te halen in de najaarsrelease 2018, tenzij dan duidelijk is dat TMR op zeer korte termijn zal worden uitgefaseerd.

Voor optie b) en c) zal het huidige vertrouwelijkheidscertificaat dienen te worden vervangen vóór 22 december 2017 conform optie 3 van de bovengenoemde alternatieven.

Een aantal leveranciers vertegenwoordigd in de TC geven aan dat optie a) voor hen haalbaar is gezien de geringe omvang van de ingreep. Echter een sectorbrede synchronisatie van de actie bij alle betreffende leveranciers blijft een uitdaging.
Een veilige route is deze benodigde aanpassing alsnog toe te voegen aan de voorjaarsrelease 2108, temeer daar betreffende berichten dan worden aangepast en getest. Derhalve wordt voorgesteld de encryptie op de berichtinhoud TMR in de voorjaarsrelease 2018 te verwijderen.

IMPACT

Door de encryptie uit te schakelen na 22 december 2017, per voorjaarsrelease 2018, is er nog wel een certificaatwissel voór 22 december 2017 benodigd. Deze zal als reguliere certificaatwissel worden uitgevoerd.

Geen impact op code of DPM.

INVOERINGSSTRATEGIE

	Release onafhankelijk	Release afhankelijk
Specifieke datum	Certificaatwissel vóór 22 december 2017	
Sectorrelease VJ 2018		Uitzetten van de berichtencryptie op TMR

TE VERVALLEN ISSUES

Nvt