TC043

Invoering TLS 1.3

Heeft het issue impact op..?	
Grootverbruik	x
Kleinverbruik	x
Elektriciteit	x
Gas	x
RNB	x
LNB	x
LV	x
MV	x
PV	x
EDSN/TenneT	x
Codes	
Berichten	
Ketenprocessen	
Privacy	
Is het issue release afhankelijk/onafhankelijk en welke invoeringsdatum heeft het issue.	
Release-afhankelijk	
Release-onafhankelijk	x

Nummer TC043
Datum 11-11-2020
Versie 1.0
Status Vastgesteld ALV NEDU

Opsteller(s) Eline Spauwen (TC), gebaseerd op adviesrapport door Allard Blankensteijn en besprekingen WG TLS 1.3

Inhoudsopgave

Colofon 3
Versiebeheer 3
Distributie 3

1 Probleemdefinitie 4

2 Overwegingen 5
2.1 Achtergrond en aanleiding 5
2.1 Belangrijkste bevindingen rapportage 5

3 Gekozen oplossing 6
3.1 Stapsgewijze invoering TLS 1.3 6
3.2 Geen certifcaatwissel 7
3.3 Vooralsnog geen uitfasering van TLS 1.2 7

4 Impact 7

5 Invoeringsstrategie TLS 1.3 8

6 Te vervallen issues 8

Bijlage A – Aanvullende informatie ten behoeve van codewijzigingsvoorstel 9

Bijlage B – Vragenlijst ter beoordeling van de privacy impact 9

Bijlage C – Vragen ter beoordeling van de security impact 9

Bijlage D – Vragen ter beoordeling van de technische impact 10

Bijlage E – Vragen ter elicitatie van non-functionele eisen 10

Colofon

Versiebeheer

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet op basis van Adviesrapport 1.2, ter review en daarna schriftelijke goedkeuring door TC	Eline Spauwen	27-08-2020
0.2	Concept	Na bespreking in TC en in WG TLS 1.3 (7-9)	Eline Spauwen	8-9-2020
0.3	Ter goedkeuring WG	Na bespreking in WG (14-09)	Eline Spauwen	23-09-2020
0.4	Ter goedkeuring TC	Na bespreking in TC en SC; voorwaardelijk goedgekeurd, laatste schriftelijke ronde. Inhoudelijk gereed voor inplanning door SPC	Eline Spauwen / Gerrit Fokkema	13-10-2020
0.5	Ter vaststelling ALV	Na schriftelijke review / goedkeuring door TC versie voor aanbieding SPC en ALV	Eline Spauwen (opmerkingen Bram van Straalen en Wim de Olde verwerkt)	21-10-2020
1.0	Vastgesteld ALV NEDU		Eline Spauwen	11-11-2020

Distributie

Gremium	Verstuurd (versie/datum)									
	0.1	0.2	0.3	0.4	0.5	0.9	1.0			
WG TLS 1.3		**8-9-2020**	**23-09-2020**	**13-10-2020**	**21-10-2020**	**3-11-2020**	**11-11-2020**			
TC	x		x	x						
SC			x	x						
SPC				x	x					
ALV NEDU						x				
Allen							x			

1 Probleemdefinitie

Onderdeel	Omschrijving
Het probleem betreft:	De vereniging NEDU volgt overheidsrichtlijnen en -normen aangaande beveiligingstandaarden. De overheidsnorm is dat met betrekking tot de beveiliging van de elektronische communicatie tussen marktpartijen bij voorkeur gebruik gemaakt dient te worden van het TLS 1.3 protocol[1]. Op dit moment geldt in de sector de afspraak om TLS 1.2 te gebruiken, en een upgrade naar TLS 1.3 is dus verstandig.
En raakt:	Alle beheerders van centrale systemen en alle marktpartijen die voor de marktprocessen met hun systemen onderling dan wel met centrale systemen communiceren en alle system integrators die oplossingen realiseren binnen het landschap van de NEDU leden.
Als gevolg waarvan:	Op dit moment communicatie met de meest recente en beste versie van het TLS-protocol niet mogelijk is in de sector.
Een goede oplossing moet:	Zorgen dat er weinig problemen bij de invoering zijn en dat zoveel mogelijk communicatie zo snel als mogelijk via TLS 1.3 zal plaatsvinden.
Of deze doelen worden behaald, kan worden gevalideerd door:	Het uitvoeren van een geautomatiseerde securitytest (scripts), die aantoont dat het gewenste niveau van beveiliging volgens de opgestelde eisen is gerealiseerd. Dit dient zowel uitgevoerd te worden op de verbindingen met geautomatiseerde berichtenuitwisseling als op die welke een GUI gebruiken.
Opdrachtgever te realiseren oplossing	NEDU
Probleemeigenaar	NEDU TC

[1] **Fout! Verwijzingsbron niet gevonden.**

2 Overwegingen

2.1 Achtergrond en aanleiding

De Security Commissie (SC) heeft in 2019 de Technische Commissie (TC) geadviseerd om zo snel als mogelijk over te gaan op TLS 1.3. Als gevolg hiervan is eerst een Plan van Aanpak opgesteld en in september 2019 aangeboden aan de ALV, en door de ALV vastgesteld. Het beoogde eindresultaat van het Plan van Aanpak was een issue voor het beschrijven van de migratie naar TLS 1.3. Dit issue is gebaseerd op het resultaat van een verkennend onderzoek, wat als onderdeel van het Plan van Aanpak is uitgevoerd.

Met het beschikbaar komen van het beveiligingsprotocol TLS 1.3 voor communicatie wil de TC zo snel als mogelijk TLS 1.3 invoeren in de sector, om te voldoen aan algemeen geldende security-eisen en overheidsrichtlijnen. Omdat de NEDU verantwoordelijk is voor de afspraken over marktprocessen en de wijze waarop berichtenuitwisseling gerealiseerd wordt, heeft de TC in een adviesrapport eisen aangaande de invoering en inrichting van TLS 1.3 opgesteld.
In het adviesrapport, dat als bijlage van dit issue is opgenomen, is uitgebreide informatie te vinden over:

- de scope en context van de invoering TLS 1.3 (alle gegevensuitwisseling binnen ketenprocessen, die onder de scope van de NEDU vallen);
- eisen en wensen aan de inrichting van TLS 1.3
- gap analyse o.a. op basis van readiness-analyse van centrale systemen en de respons op de inventarisatie readiness TLS 1.3 bij NEDU-leden;
- relevantie van lessons learned bij invoering TLS 1.2;
- overwogen scenario's van invoering.

Doordat alle marktpartijen communiceren met de centrale systemen, spelen standaarden die volgens NEDU afspraken hier worden ingevoerd een bepalende rol in de wijze waarop communicatie plaatsvindt. Hierdoor staan de centrale systemen conform NEDU afspraak op dit moment alleen communicatie op basis van TLS 1.2 toe (op basis van TC024 Overgang op TLS 1.2 v2.0 dd 14-12-2015).

2.1 Belangrijkste bevindingen rapportage

1. Veiligheid van TLS 1.2
   Anders dan bij de overgang naar TLS 1.2, is (nog) het niet zo dat bij de overgang naar TLS 1.3 het nu gebruikte TLS 1.2 als ondeugdelijk wordt beschouwd (zie hiervoor referentie). Hier wordt de aanduiding "Goed" gegeven aan zowel TLS 1.2 als TLS 1.3. Er wordt wel gesteld dat de meest recente versie van een protocol meer bescherming biedt dan een oudere.

2. Planning beschikbaarheid TLS 1.3
   Een groot aantal aanbieders van componenten die door NEDU-leden worden gebruikt ondersteunt nog geen TLS 1.3 en van vele is er ook geen roadmap met tijdpad bekend wanneer zij dit wel zullen doen.

Dit betekent dat de termijn waarin het mogelijk zal zijn om zowel het centrale landschap als de decentrale marktpartijen over te laten gaan op TLS 1.3 ongewis is. De verwachting is dat deze termijn één a twee jaar zal zijn.

3. Ondersteuning TLS 1.3 en TLS 1.2 tegelijkertijd.
   Het is mogelijk om op een endpoint zowel TLS 1.3 als TLS 1.2 (via fallback) te configureren. Het TLS-protocol voorziet erin dat altijd bij het maken van een verbinding bepaald wordt via welke versie van TLS kan worden gebruikt om de verbinding te maken.

3 Gekozen oplossing

3.1 Stapsgewijze invoering TLS 1.3

De conclusie van het uitgevoerde onderzoek is: op dit moment is een complete overgang op TLS 1.3 en daarmee afstappen van TLS 1.2 nog niet af te spreken, omdat het voor te veel door marktpartijen gebruikte software- en hardwarecomponenten nog niet duidelijk is wanneer TLS 1.3 daadwerkelijk beschikbaar zal zijn.

De “overgang” van TLS 1.2 naar TLS 1.3 wordt daarom gestart middels een duaal scenario, dat start zonder “harde” einddatum van de duale periode (het gebruik van TLS 1.2). In deze aanpak wordt eerst een ‘zachte’ - op basis van readiness per systeem – invoering van TLS 1.3 gestart. Dit wordt mogelijk indien eerst de centrale systemen op een geschikt moment primair TLS 1.3 ondersteunen, met een terugvalmogelijkheid op TLS 1.2, zodat alle communicatie, zowel via TLS 1.2 als TLS 1.3 wordt ondersteund.

In dit scenario voeren de centrale systemen op een natuurlijk moment voor dat systeem TLS 1.3 in, terwijl zij tevens de mogelijkheid blijven ondersteunen om op basis van TLS 1.2 met hen te communiceren. Dit betekent dat de marktpartijen de overgang naar TLS 1.3 binnen de duale periode kunnen inplannen zodra TLS 1.3 ondersteuning door hun toeleveranciers van softwarecomponenten beschikbaar komt.

Detailafspraken:

- We starten een duale periode waarin communicatie op basis van zowel TLS 1.2 als TLS 1.3 is toegestaan.
- Deze duale periode heeft vooralsnog geen voorgestelde einddatum.
- De TC zal elk half jaar (laten) evalueren wat de status van de beschikbaarheid van TLS 1.3 is. Deze inventarisatie gebeurt op basis van de reeds opgestelde lijst componenten en pakketten gebruikt door marktpartijen.
- Zodra het mogelijk is, zal de TC een einddatum voor de duale periode afroepen en laten vaststellen door de ALV NEDU.
- Deze einddatum zal tenminste een jaar na afroep liggen.

- Daarnaast zal de TC elk half jaar door de beheerders van de centrale systemen laten monitoren hoeveel marktpartijen al communiceren met TLS 1.3.
- Het niet uitfaseren van TLS 1.2 levert qua beveiliging vooralsnog geen probleem op, omdat met de juiste parametersetting TLS 1.2 vooralsnog adequate beveiliging biedt. Deze parametersetting wordt afgedwongen door de centrale systemen.
- Ook de veiligheid van TLS 1.2 zal worden gemonitord door de SC en TC. Als daar aanleiding voor is zal TLS 1.2 versneld (moeten) worden uitgefaseerd en zal de duale periode versneld worden afgerond.

3.2 Geen certifcaatwissel

Tevens is gekozen om bij deze invoering van TLS 1.3 de methode waarmee certificaatverificatie wordt uitgevoerd ongewijzigd te laten. Hierdoor is voor de invoering van TLS 1.3 geen certificaatwissel vereist, hetgeen de invoering minder complex en foutgevoelig maakt.

3.3 Vooralsnog geen uitfasering van TLS 1.2

De TC zal op basis van de halfjaarlijkse evaluaties zodra het mogelijk en verantwoord is een advies uitbrengen met een einddatum voor het gebruik van TLS 1.2 binnen de sector. Indien dat het geval is, zal een nieuw issue met de strategie en de afspraken opgesteld worden.

4 Impact

Tijdens de op te starten duale fase (zonder een nu al voorgestelde einddatum) geldt het volgende:

Marktpartijen:

- Communicatie op basis van TLS 1.2 met de centrale systemen blijft mogelijk;
- Marktpartijen kunnen communicatie met een centraal systeem via TLS 1.3 invoeren zodra het betreffende centrale systeem TLS 1.3 ondersteunt.

Centrale systemen:

- Zodra voor een centraal systeem TLS 1.3 beschikbaar is, wordt dit getest en geïmplementeerd in de betreffende interfaces van het centrale systeem. Dit kan plaatsvinden in het reguliere life cycle management van die systemen.

Communicatie:
In de reguliere onderhoudscommunicatie van centrale systemen zal aan beheerders gemeld worden dat er nieuwe configuraties van TLS 1.3 aan worden gezet.

De TC zal naar aanleiding van haar halfjaarlijkse evaluatie tevens aan de ALV rapporteren welke centrale systemen al TLS 1.3 ondersteunen.
Let op! Het risico blijft bestaan dat TLS 1.2 als onveilig wordt bevonden, waarna een ‘hals-over-kop’ invoering van TLS 1.3 nodig zal zijn. Derhalve is van belang

dat marktpartijen in hun betreffende communicatie-onderdelen zo snel mogelijk TLS 1.3 invoeren.

5 Invoeringsstrategie TLS 1.3

	Release onafhankelijk	Release afhankelijk
Na vaststelling ALV NEDU	x	
Sectorrelease		
Specifieke datum		

De invoeringsstrategie wordt toegelicht in combinatie met de impact i in hoofdstuk 4.

6 Te vervallen issues

TC024 Overgang op TLS 1.2 v2.0 dd 14-12-2015

Bijlage A – Aanvullende informatie ten behoeve van codewijzigingsvoorstel

N.v.t., geen codewijzigingsvoorstel

Bijlage B – Vragenlijst ter beoordeling van de privacy impact

N.v.t., geen nieuwe of inhoudelijk gewijzigde uitwisseling (persoons)gegevens

Bijlage C – Vragen ter beoordeling van de security impact

Onderstaand staan een aantal vragen die beogen te bepalen of er een nadere analyse nodig is op de bestaande beveiligingsmaatregelen om te borgen dat nog aan de eisen voor dataveiligheid wordt voldaan.

Vraag	Antwoord
1. Betreft het een aanpassing op een bestaand marktproces of een geheel nieuw marktproces?	Nee
2. Zijn er in het proces maatregelen opgenomen die misbruik van het proces voorkomen of bemoeilijken?	N.v.t.
Bij aanpassingen op een bestaand proces	
3. Verandert de wijze van gegevensuitwisseling?	Ja, een nieuw (veiliger) protocol voor internetverkeer wordt geïntroduceerd, maar niet in het kader van een aanpassing op een bestaand proces.
4. Verandert door het issue het belang van de betreffende gegevensuitwisseling of de mogelijke schade die kan ontstaan bij verkeerd gebruik van de gegevens	Nee

Bijlage D – Vragen ter beoordeling van de technische impact

Onderstaand een aantal vragen om te bepalen of er reden is om vanuit de Technische Commissie een aantal standaarden of technieken te evalueren om te borgen dat de processen ongestoord kunnen blijven werken.

Vraag	Antwoord met korte toelichting
Als in het proces, waar het issue betrekking op heeft, gebruik wordt gemaakt van uitwisseling van berichten tussen marktpartijen	
1. Is er sprake van een nieuwe berichtuitwisseling?	Nee
2. Is er sprake van een wijziging in de bestaande berichtuitwisseling (bijvoorbeeld nieuwe/vervallen elementen/attributen)?	Ja, een nieuw (veiliger) protocol voor internetverkeer wordt geïntroduceerd, maar geen inhoudelijke wijzigingen in bestaande processen / gegevensuitwisseling.
3. Is er sprake van een significante wijziging in de aantallen / frequentie van de uit te wisselen berichten?	Nee
4. Is er sprake van een significante wijziging in de omvang van de betreffende berichten (bijvoorbeeld m.b.t. grote aantallen aansluitingen)?	Nee
5. Is er sprake van wijziging in de systematiek (wijze) van de gegevensuitwisseling (bijvoorbeeld van Push naar Pull)?	Nee

Bijlage E – Vragen ter elicitatie van non-functionele eisen

Onderstaand staan een aantal vragen die beogen een inschatting te geven van de eisen die worden gesteld aan een werkende oplossing zoals die in het issue wordt voorgesteld. Deze eisen zijn van belang voor het juist inrichten en laten werken van de gekozen oplossing.

N.v.t., het betreft geen te classificeren proces / gegevensuitwisseling.