TLP: WIT

TE010

Kaders voor veilige gegevensuitwisseling

Impact topic	
Segment	☒Grootverbruik ☒Kleinverbruik
Product	☒Elektriciteit ☒GAS
Partijen	☒LNB-G ☒LNB-E ☒RNB ☒Leverancier ☒BRP ☒BSP ☒MV ☒GDS-eigenaar ☒Datagebruiker ☐Andere: ……..
Wet- en Regelgeving	☐Elektriciteits- en Gaswet (Energiewet) ☐Informatiecode, Meetcode en Netcode (Ministeriële regeling) ☐Markt en sub-processen (MSP) (Afsprakenboekje)
Centrale Impact	☐Berichten ☒Ketenprocessen
Privacy	☐Privacy
Release	☐Release afhankelijk ☒Release onafhankelijk

Nummer	TE010	**Opsteller(s):**
Datum	03-07-2024	Bram van Straalen
Versie	1.0	
Status	Definitief	

Inhoudsopgave

1 Colofon

1.1 Versiebeheer

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste versie met H2 Probleemomschrijving en H3 Overwegingen ter review door het topicteam.	Bram van Straalen	07-02-2024
0.2	Concept	Tweede versie met bijgewerkte H3 Overwegingen ter review door het topicteam.	Bram van Straalen	13-03-2024
0.3	Concept	Derde versie met bijgewerkte H3 en H4 ter review door het topicteam.	Bram van Straalen	29-03-2024
0.4	Concept	Vierde versie met verwerking laatste opmerkingen ter review door het topicteam.	Bram van Straalen	09-04-2024
0.6	Concept	Versie voor peer review.	Bram van Straalen	22-04-2024
0.7	Concept	Versie met verwerking peer review ter controle door peer reviewers.	Bram van Straalen	27-05-2024
0.8	Concept	Versie ter goedkeuring.	Bram van Straalen	10-06-2024
1.0	Definitief	Vastgesteld in de ALV MFF d.d. 03-07-2024.	Bram van Straalen	03-07-2024

1.2 Distributie

Gremium	Verstuurd (versie/datum)									
	0.1	0.2	0.3	0.4	0.6	0.7	0.8	1.0		
Topicteam	07-02-2024	13-03-2024	29-03-2024	09-04-2024	22-04-2024	27-05-2024	10-06-2024			
Achterban (peer review)					22-04-2024	27-05-2024				
BOSO							10-06-2024			
PFSG										

1.3 Begrippenlijst

Begrip	Uitleg
AVG	De Algemene Verordening Gegevensbescherming.
BIO	De **Baseline Informatiebeveiliging Overheid** (BIO) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid.
BBN	BasisBeveiligingsNiveau.
CPR	ContactPersonenRegister.
IC208	Het issue ***IC2808 Optimalisatie data-uitwisseling marktpartijen*** is in 2018 als onderdeel van het Programma Dataveiligheid geïmplementeerd.
IC209	Het issue ***IC209 - Verwerken klantsleutels*** is in 2018 als onderdeel van het Programma Dataveiligheid geïmplementeerd.
IC210	Het issue ***IC210 - Aanlevering contracten CER t.b.v. Fase 3*** opvragingen is in 2018 als onderdeel van het Programma Dataveiligheid geïmplementeerd.
NEDU	De Vereniging Nederlandse Energie Data Uitwisseling (NEDU) is op 01-04-2022 opgehouden te bestaan en opgevolgd door MFFBAS.
PIE	Partners in Energie. Hiermee wordt een reeds door EDSN en de Regionale Netbeheerders geïmplementeerde Berichtenbox inclusief aanvullende functionaliteiten, bedoeld (bij EDSN staat deze Berichtenbox bekend onder de term ticketingsysteem).
TC039	Het issue ***TC039 Veilige ad hoc gegevensuitwisseling*** dat door de Technische Commissie van de NEDU is uitgewerkt tot een versie 0.7 die nooit is vastgesteld, maar aanleiding is geworden voor de Regionale Netbeheerders om een berichtenbox te implementeren (deze berichtenbox heet PIE).

2 Probleemdefinitie

Onderdeel	Omschrijving
Het probleem / de ontwikkeling / de wet- of regelgeving betreft:	Binnen de systeemprocessen in de energiesector is sprake van gegevensuitwisselingen om deze marktprocessen in de energiesector te ondersteunen. Voor veelvoorkomende gegevensuitwisselingen maakt de energiesector gebruik van gestandaardiseerd berichtenverkeer. Gestandaardiseerd berichtenverkeer betekent het gebruik van **gestandaardiseerde berichten via gestandaardiseerde kanalen**, zoals SOAP Webservices en REST API's. Deze gestandaardiseerde berichten ondersteunen vanuit hun aard hoogwaardige faciliteiten, zoals beveiligingsmaatregelen (denk aan versleuteling) en syntaxvalidaties. Daarnaast is er binnen de systeemprocessen in de energiesector ook sprake van gegevensuitwisselingen waarvoor er vanwege lage aantallen en/of het ongestructureerde karakter van de gegevensuitwisseling geen business case is om deze via gestandaardiseerd berichtenverkeer te ondersteunen. Een veel gebruikt alternatief voor deze gegevensuitwisselingen is daarom **e-mail** dat bij diverse gegevensuitwisselingen binnen systeemprocessen geïmplementeerd is. Met de invoering van de AVG (Algemene Verordening Gegevensbescherming) en het traject Dataveiligheid (IC208, IC209 en IC210) is in de sector het bewustzijn aangaande het veilig uitwisselen van privacygevoelige en bedrijfsgevoelige gegevens toegenomen. Daarom is in 2018 gestart met de uitwerking van het issue *TC039 Veilige adhoc gegevensuitwisseling* (de voorloper van dit topicdocument) dat echter nooit is afgerond en vastgesteld. Wel zijn de regionale netbeheerders en EDSN naar aanleiding van TC039 gestart met de implementatie van een berichtenbox/portaal (Partners in Energie genoemd) ter vervanging van e-mailcommunicatie. PIE is op dit moment echter niet geschikt als vervanging van e-mails tussen alle marktrollen, maar enkel voor communicatie tussen marktrollen en de regionale netbeheerders. Feitelijk is er dus nog steeds sprake van e-mailuitwisselingen tussen diverse marktrollen binnen de systeemprocessen. De vraag is of dit problematisch is vanuit datawetgeving en evt. aanvullende regelgeving, eisen en wensen en of er daarom een alternatieve gegevensuitwisseling gepositioneerd moet worden voor gegevensuitwisselingen met een lage frequentie en/of een ongestructureerd karakter.
En raakt:	Alle marktrollen die gegevensuitwisselingen zonder formeel berichtenverkeer met andere marktrollen hebben.

Onderdeel	Omschrijving
Als gevolg waarvan:	Er onderzocht moet worden of e-mail een geschikt kanaal is voor gegevensuitwisselingen en of er een alternatief gepositioneerd moet worden.
Een goede oplossing moet:	Het voor laag frequente en/of ongestructureerde gegevensuitwisselingen tussen marktrollen mogelijk maken om deze op een **veilige** en **kostenefficiënte** wijze uit te voeren met inachtneming van overige generieke functionele en niet-functionele vereisten met betrekking tot deze gegevensuitwisselingen.
Of deze doelen worden behaald, kan worden gevalideerd door:	Een toets door security experts (met betrekking tot de veiligheid) en bij marktpartijen (met betrekking tot overige vereisten en de kostenefficiency).
Opdrachtgever te realiseren oplossing	MFFBAS
Probleemeigenaar	MFFBAS

3 Overwegingen

Dit hoofdstuk bevat diverse overwegingen rondom dit onderwerp die van belang zijn om mee te nemen bij de uitwerking van een oplossingsrichting voor dit topic. De verschillende overweging zijn gegroepeerd in verschillende paragrafen.

3.1 Soorten gegevensuitwisselingen

In deze paragraaf staan enkele overwegingen met belangrijke termen binnen de uitwisseling van gegevens tussen marktpartijen.

(1) **Gestructureerde gegevensuitwisseling** – De meeste gegevensuitwisselingen binnen de systeemprocessen kunnen gekenmerkt worden als "gestructueerd", wat betekent dat een gegevensuitwisseling een voorgedefinieerde set aan gegevenselementen bevat met hetzij een keuzelijst met voorgedefinieerde gegevens (bijvoorbeeld een verbruikssegment: grootverbruik of kleinverbruik), hetzij vrije invoervelden waarin een beperkte hoeveelheid informatie vastgelegd kan worden (bijvoorbeeld de hoeveelheid energie in kWh). Hierdoor kan de structuur van de betreffende gegevensuitwisseling vastgelegd worden met een vast aantal gegevenselementen (attributen) en is gestandaardiseerd berichtenverkeer mogelijk.

Conclusie: De term "Gestructureerde gegevensuitwisselingen" wordt in dit document gebruikt voor gegevensuitwisselingen met een voorgedefinieerde set aan gegevenselementen met hetzij een keuzelijst van vooraf voorgedefinieerde gegevens en/of korte vrije invoervelden.

(2) **Ongestructureerde gegevensuitwisseling** – Binnen systeemprocessen komen ongestructureerde gegevensuitwisselingen minder vaak voor dan gestructureerde gegevensuitwisselingen. Ongestructureerde gegevensuitwisselingen kunnen ook voorgedefinieerde sets aan gegevenselementen bevatten (net als gestructureerde gegevensuitwisselingen), maar die gaan vaak over meta-informatie in de gegevensuitwisseling (zoals de EAN-code van de aansluiting of de EAN-code van een marktpartij).
Het grote verschil is echter dat de daadwerkelijke inhoud van een ongestructureerde gegevensuitwisseling niet gestructureerd is, maar veelal bestaat een ongestructureerde inhoud (zoals een uitgebreide tekst om een klacht of reclamatie toe te lichten).

Conclusie: De term “Ongestructureerde gegevensuitwisselingen” wordt in dit document gebruikt voor gegevensuitwisselingen waarvan de essentiële inhoud grotendeels ongestructureerd van aard is; veelal is de inhoud uitgebreide tekst om een klacht of reclamatie toe te lichten.

(3) **Gestandaardiseerde gegevensuitwisseling** – De term “gestandaardiseerde” gegevensuitwisseling wordt in dit topicdocument gebruikt voor gegevensuitwisselingen die via standaard berichtformaten (zoals XML en CSV) worden uitgewisseld via standaard protocollen (zoals REST API, SOAP Webservice, AS4) en veelal via geïmplementeerde hubs (zoals MMC-Hub, NEXUS, PUD, MES, etc.).
De implementatie van gestandaardiseerd gegevensuitwisseling vergt een zorgvuldige vastlegging van de gegevensuitwisseling (in Business Services en Berichtdefinities), uitgebreide sectortesten en implementatie van integratiesoftware bij marktpartijen. Gestandaardiseerd berichtenverkeer wordt vooral geïmplementeerd bij gestructureerde gegevensuitwisselingen met hoge aantallen berichten, waarbij er een business case is om de gegevensuitwisseling met gestandaardiseerd berichtenverkeer te implementeren.

Conclusie: Gestandaardiseerd gegevensuitwisseling wordt vooral geïmplementeerd bij gestructureerde gegevensuitwisselingen met hoge aantallen berichten, waarbij er een business case is om de gegevensuitwisseling met gestandaardiseerd berichtenverkeer te implementeren.

(4) **Niet gestandaardiseerde gegevensuitwisseling**– De term “niet gestandaardiseerde” gegevensuitwisseling wordt in dit topicdocument voor gegevensuitwisselingen die niet geïmplementeerd zijn volgens de definitie van “gestandaardiseerde gegevensuitwisseling”. In de praktijk gebeurt dit nu op twee manieren: via e-mail of via Partners in Energie (PIE).

Conclusie: Niet gestandaardiseerde gegevensuitwisseling vindt in de marktprocessen op twee manieren plaats: via e-mail en via Partners in Energie (PIE).

(5) Gegevensuitwisselingen via e-mail – Van oudsher wordt zowel binnen als buiten de energiesector e-mail ingezet als een laagdrempelig kanaal om ongestructureerde gegevens uit te wisselen (of vragen te stellen). Binnen de energiesector zijn diverse gegevensuitwisselingen via e-mail geïmplementeerd. Een van de voorbeelden hiervan is het verwerken van een late metermutatie waarbij de netbeheerder conform de ***Bijlage Correctieprocessen*** uit het ***MSP MFF Retailprocessen*** een e-mail kan sturen naar de leverancier.

Conclusie: In de afgelopen jaren zijn binnen de energiemarktprocessen diverse gegevensuitwisselingen geïmplementeerd, waarbij e-mail wordt ingezet als uitwisselkanaal voor ongestructureerde gegevensuitwisselingen.

3.2 TC039 Veilige ad hoc gegevensuitwisseling

In 2018 is het issue TC039 opgestart door de Technische Commissie van de NEDU. Dit issue is uiteindelijk nooit vastgesteld, maar de inhoud van dit issue is wel relevant voor dit topic. En feitelijk is dit topic de afronding van TC039.

(6) **Centrale berichtenbox** – Bij de invoering van het Actieplan Dataveiligheid en de invoering van de AVG is binnen de Technische Commissie (voorloper van de huidige CoP Secure Architecture) gestart met de uitwerking van het issue ***TC039 Veilige ad hoc gegevensuitwisseling*** met de vraagstelling of het wel veilig is om persoonsgegevens via e-mail uit te wisselen. In de laatste versie 0.7 van dit issue adviseren te opstellers om te kiezen voor een gegevensuitwisseling met **hoog** veiligheidsniveau en adviseren de implementatie van een **centrale berichtenbox** met de volgende argumentatie: "*Deze biedt voldoende veiligheid, mits goed ingericht, zoals gebruikmaking van goede identity en access management, en is relatief gemakkelijk in het gebruik. Het laten inrichten van decentrale berichtenboxen wordt als te onwerkbaar ervaren, omdat dan afhankelijk van de interacterende partijen steeds een andere decentrale berichtenbox dient te worden aangesproken en de administratieve last voor het gebruikersbeheer voor de sector (bij alle boxen) onevenredig hoog wordt.*"

Conclusie: De NEDU Technische Commissie heeft in 2018 voorgesteld om ter vervanging van e-mail een centrale berichtenbox te implementeren waardoor een hoog beveiligingsniveau wordt bereikt.

(7) **Partners in Energie (PIE)** – Nadat het issue ***TC039 Veilige ad hoc gegevensuitwisseling*** deels is uitgewerkt tot een versie 0.7, zijn de regionale netbeheerders gestart met de implementatie van een centrale berichtenbox, het zogenaamde platform Partners in Energie om de diverse gegevensuitwisselingen met de regionale netbeheerders die middels e-mail plaatsvinden, te vervangen door PIE. Middels dit platform kunnen marktpartijen, na ingelogd te zijn op PIE, via een invulscherm tickets indienen bij de regionale netbeheerders. Via dit portaal krijgen ze ook antwoord van de regionale netbeheerders. Het platform PIE is nu echter enkel geïmplementeerd ter ondersteuning gegevensuitwisseling met de regionale netbeheerders. Een deel van disputenproces met betrekking tot meetgegevens van kleinverbruikaansluitingen wordt al ondersteund middels PIE, maar

ook het non-conformiteitenproces tussen meetverantwoordeljiken en regionale netbeheerders. Verder geldt dat nog niet alle marktpartijen zijn aangesloten op PIE.

Conclusie: De regionale netbeheerders hebben binnen het platform PIE een ticketingsysteem als een berichtenbox geïmplementeerd ter ondersteuning van ongestructureerde gegevensuitwisseling met hen. Nog niet alle marktpartijen hebben zich echter aangesloten op PIE en PIE ondersteunt enkel gegevensuitwisselingen met de regionale netbeheerders, maar bijvoorbeeld niet gegevensuitwisselingen tussen twee verschillende leveranciers of tussen een balanceringsverantwoordelijke en een meetverantwoordelijke.

(8) **Gebruik berichtenbox van de regionale netbeheerders** – Bij de uitwerking van TC039 werd duidelijk dat de regionale netbeheerders aan de slag gingen om een centrale berichtenbox te implementeren en dat gestart werd met de uitwisseling van gegevens met de regionale netbeheerders. TC039 stelde daarom voor om deze centrale berichtenbox op een later moment ook in te zetten voor alle ad hoc interactie tussen partijen waarbij (persoonsgevoelige) gegevens worden uitgewisseld. In afwachting daarop is TC039 nooit officieel vastgesteld.

Conclusie: Het eindvoorstel in TC039 was om de door de regionale netbeheerders te realiseren centrale berichtenbox op een later moment ook in te zetten voor een veilige uitwisseling tussen andere marktpartijen.

3.3 Veilige gegevensuitwisseling

In deze paragraaf worden enkele overwegingen gewijd aan wet- en regelgeving met betrekking tot de vereiste maatregelen die genomen moeten worden om de uitwisseling van gegevens veilig te laten plaatsvinden. Verder wordt ingegaan op de afwegingen die gemaakt zijn in TC039.

(9) **Elektriciteitswet Art. 79** – De Elektriciteitswet benoemt in Hoofdstuk 6, § 1. Informatieverstrekking een aantal zaken waaraan een netbeheerder zich moet houden. Art. 79 lid 1 zegt het volgende met betrekking tot de zorgplicht van de netbeheerder voor vertrouwelijke gegevens: “Een netbeheerder die bij de uitvoering van zijn taak de beschikking krijgt over gegevens waarvan hij het **vertrouwelijke karakter** kent of redelijkerwijs moet vermoeden, **draagt er zorg voor** dat die gegevens niet ter beschikking komen of kunnen komen van derden, tenzij enig wettelijk voorschrift anders bepaalt.”

Conclusie: De netbeheerder moet onder de Elektriciteitswet zorgen dat vertrouwelijke gegevens niet ter beschikking komen van derden.

(10) **Energiewet Art. 4.21 Passende maatregelen** – De concept Energiewet zegt in Art. 4.21 onder het kopje "gegevensbescherming en gegevensbeveiliging" dat de gegevensuitwisselingsentiteit **passende en evenredige technische en organisatorische maatregelen** om de **risico's te beheersen** met betrekking tot onder andere **het faciliteren van de uitwisseling van gegevens ten behoeve van de processen**, bedoeld in Art. 4.1, tweede lid. In Art. 4.1 lid 2 worden feitelijk alle systeemprocessen bedoeld.

Conclusie: De energiesector moet passende en evenredige technische en organisatorische maatregelen nemen om risico's te beheersen bij de uitwisseling van gegevens in marktprocessen.

(11) **Risicoafweging** – Voor het bepalen van de passende maatregelen is derhalve een **risicoafweging** noodzakelijk. De Baseline Informatiebeveiliging Overheid (BIO) kiest bij de risicoanalyse voor drie basisbeveiligingsniveaus (BBN), waarbij BBN1 de basisbeveiliging is en BBN3 de hoogste beveiliging voor de meest vertrouwelijke informatie. BBN2 zit daar tussenin.[1] In de Bijlage 2 van de BIO wordt voor de overheid uitgewerkt wat deze drie niveaus behelzen. Deze BIO is niet direct toepasbaar op de energiesector, maar kan wel als inspiratie dienen.

Conclusie: De BIO van de overheid is een inspiratie voor het gebruik in de energiesector.

(12) **STRIDE threat modeling** – Het zogenaamde STRIDE-model is in de jaren negentig van de vorige eeuw door Microsoft ontwikkeld om kwetsbaarheden in applicaties in kaart te brengen. Dit model is deels geschikt om ook kwetsbaarheden in gegevensuitwisselingen in kaart te brengen en te categoriseren.
Spoofing identity = het je voor doen als een ander persoon/bedrijf (authenticatie);
Tampering with data = het zonder toestemming wijzigen van gegevens (integriteit);
Repudiation threats = het wijzigen zonder sporen na te laten (non-repudiation);
Information Disclosure = gevoelige gegevens komen op straat te liggen (vertrouwelijkheid);
Denial of Service = vermindering toegang tot een bepaalde dienst (beschikbaarheid);

[1] BIO, versie 1.04zv, 17-06-2020

Elevation of Privilege = ongeautoriseerde toegang tot gegevens (autorisatie).

Conclusie: De zes verschillende bedreigingen binnen het STRIDE-model zijn een passende kapstok om bedreigingen van gegevensuitwisselingen in kaart te brengen, alhoewel ze misschien niet alle zes even relevant zijn voor dit topic.

(13) **Beoordeling vanuit TC039** – In versie 0.7 van TC039 is het gebruik van normale e-mail met betrekking tot het uitwisselen van persoonsgegevens geclassificeerd met een beveiligingsniveau “laag”, omdat het e-mailkanaal en in de inhoud van de e-mails niet beveiligd zijn. In TC039 is vervolgens beoordeeld of er mogelijkheden zijn om e-mail te beveiligen waardoor het beveiligingsniveau omhoog gaat. Bijvoorbeeld door het gebruik van encryptie van de e-mails en/of het beveiligen van de e-mailverbindingen met TLS. Dit vereist echter extra inspanningen van de IT-organisaties en/of de gebruikers waardoor het gemak van e-mail wegvalt. De eindconclusie in TC039 was daarom de implementatie van een centrale berichtenbox (zie ook paragraaf 3.2 overweging (6), (7) en (8). Sinds de uitwerking van TC039 is mate van beveiliging van e-mail niet verbeterd.

Conclusie: In TC039 werd normale e-mail als onveilig geclassificeerd voor de uitwisseling van gevoelige (persoons)gegevens. Wel zijn er mogelijkheden om e-mail te beveiligen, maar die zijn moeilijk uitvoerbaar vanwege het decentrale karakter van de verschillende e-mailboxen. De risico’s van e-mail zijn samenvattend nog steeds te groot geacht om gevoelige (persoons)gegevens via e-mail uit te wisselen.

3.4 Vereisten gegevensuitwisseling zonder gestandaardiseerd berichtenverkeer

Naast het veiligheidsaspect is het goed om ook te kijken naar andere kenmerken bij gegevensuitwisselingen met als doel om de vraag te stellen in hoeverre e-mail geschikt is voor gegevensuitwisseling in de marktprocessen. In deze paragraaf worden daarom enkele aspecten genoemd die relevant (kunnen) zijn bij gegevensuitwisselingen en wordt de vraag gesteld in hoeverre e-mail hier invulling aan kan geven.

(14) Ongestructureerde gegevens – Voor de gegevensuitwisselingen van ongestructureerde informatie, zoals het stellen van vragen, is e-mail zeer geschikt. In het dagelijks gebruik, wordt e-mail daar immers voor gebruikt. En ook de beantwoording van een e-mail is eenvoudig. Daarnaast is het mogelijk om bijlages in allerlei formaten mee te sturen.

Conclusie: E-mail is goed geschikt om ongestructureerde gegevens uit te wisselen met een toevoeging van diverse soorten bijlagen.

(15) **Zakelijk gebruik e-mail (afdelingse-mail) –** Met e-mailprogramma's is het verder ook mogelijk om een afdelingse-mailadres te genereren waar medewerkers van die afdeling toegang toe hebben. Hierdoor hoeven geen persoonlijke e-mailadressen gebruikt te worden, maar kunnen marktpartijen met elkaar communiceren via afdelingse-mailadressen.
Wel zullen deze e-mailadressen opgezocht moeten worden, waarvoor het ContactpersonenRegister (CPR) ingericht is. Een automatische koppeling tussen e-mailprogramma's en het CPR bestaat niet. In de praktijk kunnen die e-mailadressen natuurlijk wel in de e-mailprogramma's vastgelegd kunnen worden, maar dat moet dan wel per marktpartij gedaan worden.

Conclusie: E-mail is goed geschikt voor zakelijk gebruik waar medewerkers van het e-mailadres van een afdeling gebruiken en met meerdere medewerkers gebruik te maken van dit e-mailadres.

Conclusie: De te gebruiken e-mailadressen liggen veelal vast in het CPR. Vanuit e-mailprogramma's is geen automatische koppeling met het CPR, zodat er handmatige acties nodig zijn om het juiste e-mailadres op te zoeken.

(16) **Laagdrempeligheid en flexibiliteit –** Een van de argumenten om gebruik te maken van niet gestandaardiseerd berichtenverkeer, is laagdrempeligheid en flexibiliteit. Bij de keuze om een gegevensuitwisseling niet via gestandaardiseerd berichtenverkeer plaats te laten vinden, speelt een laagdrempelige toegang voor alle marktpartijen een grote rol. Of de marktpartij nu groot is of klein. E-mail is bij uitstek laagdrempelig en het inrichten van een nieuwe gegevensuitwisseling via e-mail is snel in te richten (flexibiliteit), omdat e-mail bij alle marktpartijen en door alle medewerkers gebruikt wordt.

Conclusie: E-mail is een zeer laagdrempelig en flexibel kanaal voor de uitwisseling van gegevens. Een nieuwe gegevensuitwisseling is hierdoor snel te implementeren bij alle betrokken marktrollen.

(17) **Kostenefficiënt –** Een van de argumenten om gebruik te maken van niet gestandaardiseerd berichtenverkeer, is kostenefficiency. Bij de keuze om een gegevensuitwisseling niet via gestandaardiseerd berichtenverkeer plaats te laten vinden, speelt kostenefficiency voor alle marktpartijen een grote rol. De gegevensuitwisselingen zijn veelal niet hoog frequent waardoor een kostenefficiënt kanaal nodig is voor het proces. E-mail is bij uitstek kostenefficiënt,

omdat e-mail bij alle marktpartijen en door alle medewerkers gebruikt wordt en het geen additionele investeringen vergt om een nieuwe gegevensuitwisseling te implementeren.

Conclusie: E-mail is een zeer kostenefficiënt kanaal voor de uitwisseling van gegevens.

(18) **Traceerbaarheid & bewijslast –** De traceerbaarheid van verzonden e-mails is beperkt. Het is als verzender wel mogelijk om een ontvangstbevestiging te vragen aan de ontvanger, maar die hoeft de ontvanger niet te versturen. Verder is er geen onafhankelijke logging van de verzending en de ontvangst van e-mails. De verzender kan in zijn e-mailprogramma kijken wanneer welke e-mail is verstuurd en of er antwoord op is binnengekomen, maar meer is er feitelijk niet. Dit in tegenstelling tot bijvoorbeeld gestandaardiseerd berichtenverkeer waarbij een centrale logging plaatsvindt bij een centrale postbus (zoals de MMC-Hub of de NEXUS-Hub) waarmee onafhankelijk inzichtelijk is wanneer een bericht verzonden is en of het bericht is afgeleverd bij de ontvanger. Dit is voor normaal dagelijks gebruik van e-mail niet relevant, maar de vraag is wel of het een vereiste is bij het gebruik bij marktprocessen, waarbij soms tijdslijnen zijn afgesproken over de afhandeling van vragen/verzoeken.

Conclusie: Een centrale of onafhankelijke traceerbaarheid ontbreekt bij e-mail met betrekking tot de verzending en de ontvangst van e-mails. Dit bemoeilijkt de traceerbaarheid van verzonden berichten en de tijdige beantwoording daarvan. Verder is er geen onafhankelijke bewijslast met betrekking tot de verzending en ontvangst.

(19) **Bewaren en verwijderen van gegevens –** Onderdeel van de AVG is de verwijdering van gegevens als de bewaartermijn verstreken is. Uiteraard kunnen in e-mailprogramma's oude e-mails verwijderd worden, maar dit is in de praktijk een handmatig proces, dat daarmee afhankelijk is van een gebruiker die tijdig oude e-mails weggooit. Automatische en tijdige verwijdering van oude e-mails waarvan de bewaartermijn verstreken is, is niet goed praktisch uit te voeren omdat de inhoud van de mails ongestructureerd is en niet automatisch kan worden bepaald of een mail verwijderd moet worden. De keerzijde is dat de berichten gedurende de periode dat een proces gaande is, moeten worden bewaard. Bij e-mail is het gevaar aanwezig dat berichten voortijdig verwijderd worden.

Conclusie: E-mail is geen praktisch hulpmiddel om op een efficiënte wijze de gegevens tijdig te verwijderen of juist te bewaren als dat moet.

(20) **Procesbewaking –** Het bewaken of een proces volledig is afgehandeld, en eventueel te zorgen dat en proces binnen de overeengekomen tijdlijnen (SLA of DVO) afgerond wordt, is vaak belangrijk. Via e-mail is deze functionaliteit lastig, zo niet onmogelijk te ondersteunen, omdat e-mails niet altijd opvolgend verstuurd worden en geautomatiseerde voortgangsbewaking interpretatie van de inhoud (of het soort bericht) vereist. Door het ongestructureerde karakter van e-mail is procesbewaking daardoor lastig, zo niet onmogelijk via e-mail.-

Conclusie: E-mail is onbruikbaar als middel om procesbewaking te ondersteunen.

(21) **Escaleren of tweedelijns ondersteuning –** Het kan voor de afhandeling van een proces nodig zijn om tweedelijns hulp in te schakelen of te escaleren bijvoorbeeld van een medewerker naar een teamleider. De laagdrempeligheid van e-mail maakt inschakelen van tweedelijnshulp of escaleren zeer eenvoudig, maar daarmee worden de eerder genoemde veiligheidsrisico's juist verder versterkt. Er bestaan binnen e-mail wel oplossingen voor, maar die zijn vaak lastig te implementeren.

Conclusie: De laagdrempeligheid van e-mail maakt inschakelen van tweedelijnshulp of escaleren zeer eenvoudig, maar daarmee worden de veiligheidsrisico's juist verder vergroot.

(22) **Volledigheidscontrole –** Voor een correcte uitvoering van het proces is het belangrijk dat de minimaal noodzakelijke informatie opgeleverd wordt bij een gegevensuitwisseling. Een volledigheidscontrole op de aangeleverde gegevens waarborgt niet dat de inhoud van de aangeleverde gegevens juist is, maar wel dat de “verplichte velden” aangeleverd worden. Hiermee is volledigheidscontrole een middel om te zorgen dat de aanleverende partij gedwongen wordt om minimaal een bepaalde set gegevens aan te leveren. Met e-mailformulieren is dit op zich in te regelen, maar die moeten dan wel bij alle marktpartijen geïmplementeerd worden.

Conclusie: Volledigheidscontrole is lastig via e-mail te implementeren. Het is op zich wel mogelijk, maar dan moeten alle marktpartijen dit decentraal implementeren.

4 Gekozen oplossing

4.1 Bestaande oplossingsrichtingen voor gegevensuitwisselingen

Samengevat zijn er momenteel in de sector twee officieel[2] gebruikte mogelijkheden om gegevensuitwisselingen tot stand te brengen (zie ook de overwegingen (3), (4), (5) en (6)):

1. Gestandaardiseerd berichtenverkeer;
2. E-mail.

Wegingsaspecten voor beoordeling gestandaardiseerd berichtenverkeer en e-mail
Voor een verdere beoordeling is het goed om de nu in de sector gebruikte officiële mogelijkheden voor gegevensuitwisseling met elkaar te vergelijken. De hierbij gebruikte wegingsaspecten zijn gebaseerd op:

1. De mate van ondersteuning **beveiligingsvereisten** (STRIDE) (zie overweging (12));
2. De mate van ondersteuning van **overige niet functionele vereisten** (zie paragraaf 3.4).

In de onderstaande tabel is weergegeven hoe goed deze verschillende oplossingsrichtingen scoren op verschillende wegingsaspecten:

- Hierbij geldt voor de beveiligingsrisico's dat "hoog" betekent dat de oplossingsrichting in potentie een hoge bescherming tegen dit risico biedt en "laag" een lage bescherming.
- Bij de overige aspecten zijn ook de kwalificaties "hoog", "midden" en "laag" gebruikt, maar kan een kwalificatie "hoog" een negatieve betekenis hebben, zoals bij implementatiekosten.
- Met de kleuren **groen**, **oranje** of **rood** is ten behoeve van de zichtbaarheid aangegeven in hoeverre een oplossingsrichting goed scoort op een aspect.

Hierbij geldt dat er bij gestandaardiseerd berichtenverkeer veel zaken standaard geregeld zijn of eenvoudig ingericht kunnen worden.

[2] Zoals eerder beschreven wordt PIE nu al ingezet voor gegevensuitwisselingen tussen aan de ene zijde de regionale netbeheerders en aan de andere zijde leveranciers, meetverantwoordelijken en balanceringsverantwoordelijken, maar dit is nooit binnen MFFBAS geformaliseerd.

Aspecten	Gestandaardiseerd	E-mail
Mate van ondersteuning beveiligingsvereisten (STRIDE)		
Spoofing	Hoog	Midden
Tampering with data	Hoog	Midden
Repudiation threats	Hoog	Midden
Information Disclosure	Hoog	Midden
Denial of Service	Hoog	Midden
Elevation of Privilege	Hoog	Midden
Mate van ondersteuning niet-functionele vereisten		
Bewaartermijn (verwijderen o.b.v. bewaartermijn)	Hoog	Laag
Procesbewaking (afhandelingsbewaking)	Hoog	Laag
Toegangscontrole tot de gegevens	Hoog	Midden[3]
Continuïteit (niet afhankelijk van één persoon)	Hoog	Midden[4]
Uitvoeren volledigheidscontroles	Hoog	Laag
Ondersteuning hoge aantallen	Hoog	Laag
Kosten		
Implementatiekosten	Hoog	Laag

[3] Bij gebruik van een afdelingse-mailadres met autorisaties.
[4] Bij gebruik van een afdelingse-mailadres.

4.2 Additionele oplossingsrichting voor gegevensuitwisselingen

4.2.1 Berichtenbox

Zoals naar voren is gekomen in de overwegingen (zie hoofdstuk 3) en de analyse van de bestaande oplossingsrichtingen voor gegevensuitwisselingen (zie paragraaf 4.1) zit er een gat tussen gestandaardiseerd berichtenverkeer en e-mail. Voor diverse gegevensuitwisselingen is gestandaardiseerd berichtenverkeer namelijk te zwaar (lees: te duur en niet kostenefficiënt), terwijl aan de andere kant e-mail onvoldoende beveiliging biedt en geen invulling kan geven aan andere vereisten.

De conclusies is dat de implementatie van een sectorbreed gebruikte Berichtenbox het gat kan invullen voor gegevensuitwisselingen waarvoor gestandaardiseerd berichtenverkeer te duur is (vanwege de lage aantallen berichten) en e-mail onvoldoende geschikt is om veiligheidsrisico's te mitigeren en/of onvoldoende invulling kan geven aan de overige vereisten.

In de onderstaande tabel is weergegeven hoe goed een Berichtenbox invulling kan geven aan de in paragraaf 4.1 genoemde wegingsaspecten:

- Hierbij geldt voor de beveiligingsrisico's dat "hoog" betekent dat de oplossingsrichting in potentie een hoge bescherming tegen dit risico biedt en "laag" een lage bescherming.
- Bij de overige aspecten zijn ook de kwalificaties "hoog", "midden" en "laag" gebruikt, maar kan een kwalificatie "hoog" een negatieve betekenis hebben, zoals bij implementatiekosten.
- Met de kleuren **groen**, **oranje** of **rood** is ten behoeve van de zichtbaarheid aangegeven in hoeverre een oplossingsrichting goed scoort op een aspect.

Aspecten	Berichtenbox
Mate van ondersteuning beveiligingsvereisten (STRIDE)	
Spoofing	**Hoog**
Tampering with data	**Hoog**
Repudiation threats	**Hoog**
Information Disclosure	**Hoog**
Denial of Service	**Hoog**
Elevation of Privilege	**Hoog**

Aspecten	Berichtenbox
Mate van ondersteuning niet-functionele vereisten	
Bewaartermijn (verwijderen o.b.v. bewaartermijn)	**Hoog**
Procesbewaking (afhandelingsbewaking)	**Midden** / **Hoog**
Toegangscontrole tot de gegevens	**Hoog**
Continuïteit (niet afhankelijk van één persoon)	**Hoog**
Uitvoeren volledigheidscontroles	**Hoog** [5]
Ondersteuning hoge aantallen	**Laag**
Kosten	
Implementatiekosten	**Laag** [6]

4.2.2 Afwegingskader

De vraag is dan wel wanneer er gekozen zou moeten worden voor de Berichtenbox en wanneer gestandaardiseerd of e-mail juist te verkiezen is.

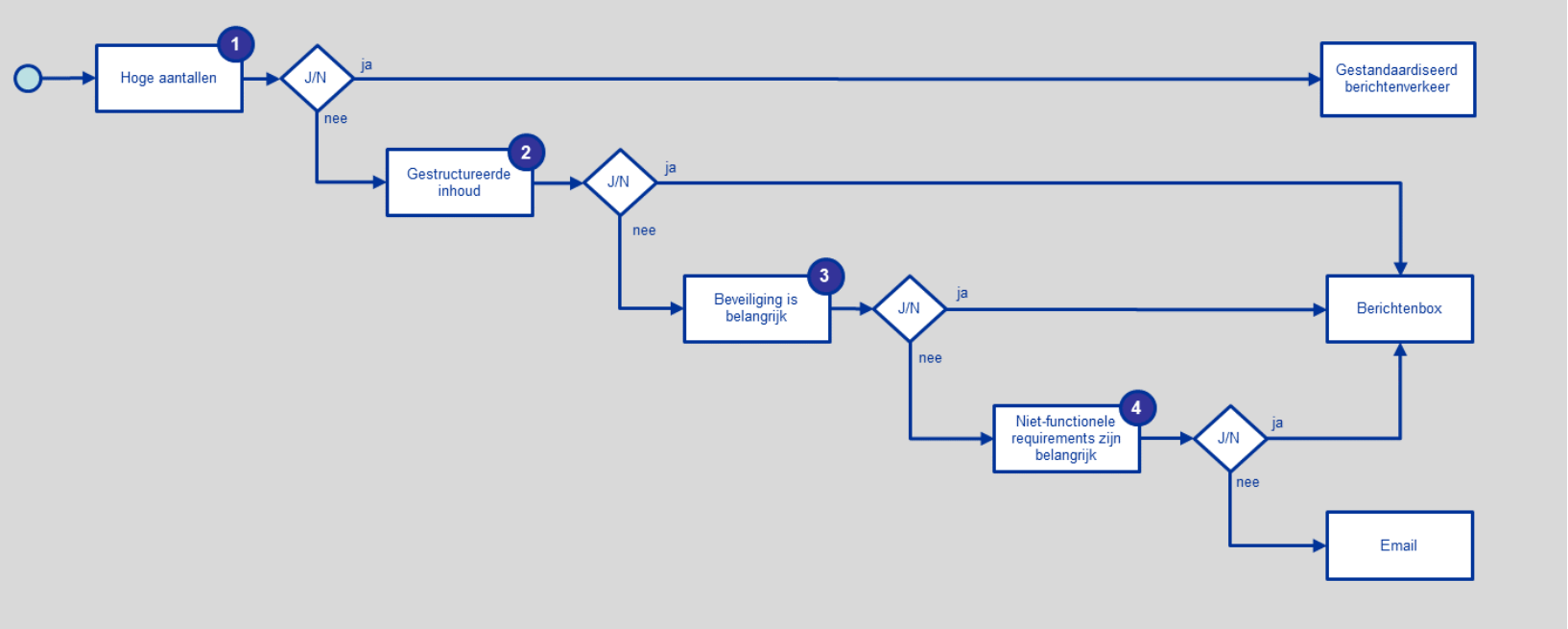
Het volgende afwegingskader is hierbij een leidraad[7] voor de architecten binnen MFFBAS om een keuze te maken uit de drie oplossingsrichtingen aan de hand van een viertal vragen:

1. **Hoge aantallen in relatie tot de afhandeltijd**. Gaat het bij de gegevensuitwisseling om hoge aantallen? Een aantal is hier niet te noemen, omdat dit de keuze te binair maakt. Het is aan de betrokken marktpartijen bij de toepassing van het afwegingskader om aan te geven of de aantallen dermate hoog zijn dat de gegevensuitwisseling via gestandaardiseerd berichtenverkeer afgehandeld moet worden. Dit omdat een handmatige afhandeling operationeel te duur is ten opzichte van een geautomatiseerde afhandeling Mogelijk is een impactanalyse met een ondersteunende business case

[5] Bij het gebruik van een formulier.
[6] Laag bij marktpartijen die gegevens uitwisselen via de Berichtenbox. Dit is exclusief de kosten die de beheerder van de berichtenbox heeft om deze te implementeren en te beheren.
[7] Dit afwegingskader is een leidraad en dat betekent dat er afgeweken kan worden als er gegronde redenen voor zijn die dan wel vastgelegd moeten worden bij het maken van de keuze.

noodzakelijk bij het maken van de keuze bij een bepaalde gegevensuitwisseling.

2. **Gestructureerde inhoud**. Is er bij de gegevensuitwisseling sprake van een gestructureerde inhoud. Omdat deze vraag niet altijd binair te beantwoorden is (soms zijn delen gestructureerd en delen niet en is er sprake van een glijdende schaal) is de stelregel dat er sprake is van een gestructureerde inhoud als tenminste 75% van de gegevenselementen gestructureerd is.
3. **Beveiliging is belangrijk**. De vraag is hier of het vanwege de aard van de gegevens STRIDE, belangrijk is om beveiligingsmaatregelen te treffen. De belangrijkheid is afhankelijk van de impact op beschikbaarheid, integriteit, vertrouwelijkheid en privacy. Mogelijk is een impactanalyse noodzakelijk bij het maken van de keuze bij een bepaalde gegevensuitwisseling.
4. **Niet-functionele vereisten**. De vraag is hier of het belangrijk is om invulling te kunnen geven aan een of meerdere niet-functionele vereisten(zie paragraaf 4.2.2).



4.3 Vereisten Berichtenbox

Om een Berichtenbox als additionele gegevensuitwisseling binnen MFFBAS te positioneren en deze Berichtenbox vervolgens ook succesvol in te zetten, zijn de volgende zaken van belang:

1. **Ondersteuning gegevensuitwisseling tussen alle marktrollen**. Het belangrijkste uitgangspunt voor een succesvolle implementatie van de Berichtenbox is dat deze gegevensuitwisseling tussen alle marktrollen (en daarmee alle marktpartijen) ondersteunt. Alleen dan kan de Berichtenbox gepositioneerd worden als een alternatief voor gestandaardiseerd berichtenverkeer en e-mail.
2. **Officiële status**. De Berichtenbox krijgt in de energiesector een officiële status als uitwisselkanaal van gegevens tussen alle marktrollen (en marktpartijen) binnen MFF, waardoor binnen de energiesector afspraken gemaakt kunnen worden om gegevensuitwisselingen te implementeren via de Berichtenbox.
3. **Implementatie en Beheer**. Aan de netbeheerders zal gevraagd worden om de Berichtenbox te implementeren en beheren.[8] De netbeheerders zullen de Berichtenbox moeten configureren ten behoeve van de inzet voor een specifieke gegevensuitwisseling. Aan deze Berichtenbox moeten op een eenvoudige wijze nieuwe gegevensstromen toegevoegd kunnen worden waardoor flexibliteit (gemakkelijk wijzigingen door te voeren) waardoor een korte time to market (snelle implementatie van nieuwe gegevensuitwisselingen) wordt bereikt.
4. **Commitment gebruik**. Als vanuit MFFBAS de keuze gemaakt wordt voor de inzet van de Berichtenbox als uitwisselkanaal, dan committeren alle betrokken marktrollen/marktdeelnemers om de Berichtenbox te gebruiken.
5. **Documentatie**. Gegevensuitwisselingen via gestandaardiseerd berichtenverkeer worden vastgelegd in procesbeschrijvingen (MSP) en Business Services, terwijl gegevensuitwisselingen via e-mail alleen in procesbeschrijvingen vastliggen (MSP). Ten behoeve van de inzichtelijkheid voor de marktpartijen welke gegevensuitwisselingen via de Berichtenbox plaatsvinden, is het advies om dit vast te leggen in sectordocumentatie (een soort Business Service light). Hierdoor is het duidelijk dat een bepaalde gegevensuitwisseling via de Berichtenbox plaatsvindt. Het is niet nodig om een uitgebreide beschrijving te maken, zoals gebruikelijk in Business Services.
6. **Vereisten Berichtenbox**. Aan de Berichtenbox worden tenminste de vereisten gesteld die genoemd staan in de paragrafen 3.3 en 3.4:
    a. Beveiligingsvereisten;
    b. Niet-functionele vereisten.
7. **Overige vereisten.** Aan een Berichtenbox zullen nog meer eisen gesteld moeten worden om deze goed te laten functioneren. Deze moeten later uitgewerkt worden in overleg met de beheerder van de Berichtenbox, maar in ieder geval kunnen non-limitatief de volgende aspecten genoemd

[8] Bij de inwerkingtreding van de Energiewet moet bepaald worden of dit beheer overgedragen wordt aan de Gegevensuiwisselingsentiteit.

worden:

a. Autorisatie
b. Authenticatie
c. Audittrail
d. Routering van berichten
e. Formulieren (templates)
f. Inzicht in voorraden
g. Inzicht in doorlooptijden van afhandeling.

5 Impact

Dit topic heeft geen impact op impact op de codes, een MSP, een MPM of een DPM.

6 Invoeringsstrategie

	Release onafhankelijk	Release afhankelijk
Na vaststelling MFF	X	
Sectorrelease		
Specifieke datum		

De invoeringsstrategie is als volgt:

1. Met de vaststelling van dit topicdocument gaat het MFF akkoord met de implementatie en de inzet van een Berichtenbox.
2. De netbeheerders gaan de Berichtenbox implementeren op basis van de in dit topicdocument benoemde vereisten en aanvullende, nog te verzamelen, vereisten.[9]
3. Bij te implementeren nieuwe gegevensuitwisselingen zal volgens het in paragraaf 4.2.2 genoemde afwegingskader bepaald worden of een gegevensuitwisseling middels de Berichtenbox geïmplementeerd gaat worden.
4. Het Berichtenteam zal bij nieuwe gegevensuitwisselingen die via de Berichtenbox verlopen, zorgen voor de formele vastlegging in een passend sectordocument[10].
5. Bestaande gegevensuitwisselingen die nu via PIE verlopen, worden indien relevant gemigreerd naar de Berichtenbox (zie voetnoot 9). Bestaande gegevensuitwisselingen die nu via e-mail verlopen worden geïnventariseerd en op basis van het in paragraaf 4.2.2 genoemde afwegingskader zal bepaald worden of deze gegevensuitwisseling gemigreerd zouden moeten worden naar de Berichtenbox. Een eventuele migratie zal separaat opgepakt worden.[11]

[9] Het is een technische keuze van de netbeheerders of dit een doorontwikkeling is van een bestaand platform of de ontwikkeling van een nieuw platform.
[10] Een soort Business Service Light.
[11] Het in ontwikkeling zijnde topic TE011 Tijdige modernisering informatie-uitwisseling lijkt het passende proces te bevatten voor deze migratie.

7 Te vervallen issues/topics

Het nooit afgeronde NEDU *TC039 Veilige ad hoc gegevensuitwisseling* komt te vervallen.

Bijlage A – Aanvullende informatie ten behoeve van codewijzigingsvoorstel

Vraag	Antwoord
1. Wat is de aanleiding voor de indiening van het codevoorstel en wat zijn de redenen die het voorstel noodzakelijk maken?	Niet van toepassing.
2. Wat zijn de doelstellingen die met het codevoorstel worden nagestreefd en op welke wijze draagt het codevoorstel bij aan het verwezenlijken van die doelstellingen?	Niet van toepassing.
3. Op welke wijze houdt het codevoorstel rekening met het belang van:	
a. het betrouwbaar, duurzaam, doelmatig en milieuhygiënisch verantwoord functioneren van de energievoorziening?	Niet van toepassing.
b. de bevordering van de ontwikkeling van het handelsverkeer op de energiemarkt?	Niet van toepassing.
c. de bevordering van het doelmatig handelen van afnemers?	Niet van toepassing.
d. een goede kwaliteit van de dienstverlening van netbeheerders?	Niet van toepassing.
e. een objectieve, transparante en niet discriminatoire handhaving van de energiebalans op een wijze die de kosten weerspiegelt?	Niet van toepassing.

Vraag	Antwoord
4. Welke alternatieven zijn mogelijk en welke afweging is gemaakt bij de keuze tussen de alternatieven?	Niet van toepassing.
5. Welke effecten heeft het codevoorstel voor netgebruikers, netbeheerders en andere belanghebbenden?	Niet van toepassing.
6. Is er samenhang met andere issuebeschrijvingen, (voorstellen voor) codes en Europese netcodes? En zo ja, welke?	Niet van toepassing.

Bijlage B – Vragenlijst ter beoordeling van de privacy impact

Vraag	Antwoord
Type project	
1. Is er sprake van het verwerken van persoonsgegevens?	Nee
2. Is het duidelijk wie verantwoordelijk is voor de verwerking van gegevens?	N.v.t.
3. Is het doel van de verwerking van persoonsgegevens voldoende SMART omschreven?	N.v.t.
De gegevens	
4. Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?	N.v.t.
5. Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt?)	N.v.t.
Verzamelen van gegevens	
6. Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?	N.v.t.
7. Is duidelijk of u de gegevens verzamelt op basis van opt-in (verzameling uitsluitend als de betrokkene daarvoor toestemming heeft gegeven) of op basis van opt-out (verzameling tenzij de betrokkene daartegen bezwaar heeft	N.v.t.

Vraag	Antwoord
gemaakt)?	
Gebruik van gegevens	
8. Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?	N.v.t.
Bewaren en vernietigen	
9. Is een bewaartermijn voor de gegevens vastgesteld?	N.v.t.
10. Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?	N.v.t.
11. Zo ja, worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen zijn en te gebruiken zijn?	N.v.t.

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?	N.v.t.
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?	N.v.t.
4. Verandert door het issue het belang van de betreffende gegevensuitwisseling of de mogelijke schade die kan ontstaan bij verkeerd gebruik van de gegevens	N.v.t.

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?	N.v.t.
2. Is er sprake van een wijziging in de bestaande berichtuitwisseling (bijvoorbeeld nieuwe/vervallen elementen/attributen)?	N.v.t.
3. Is er sprake van een significante wijziging in de aantallen / frequentie van de uit te wisselen berichten?	N.v.t.
4. Is er sprake van een significante wijziging in de omvang van de betreffende berichten (bijvoorbeeld m.b.t. grote aantallen aansluitingen)?	N.v.t.
5. Is er sprake van wijziging in de systematiek (wijze) van de gegevensuitwisseling (bijvoorbeeld van Push naar Pull)?	Ja, de introductie van een Berichtenbox als aanvulling op gestandaardiseerd berichtenverkeer en e-mail.

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.

Vraag	Antwoord
1. Wat is de benodigde security (BIV codering kan hierbij volstaan)?	N.v.t.
2. Wat is de verwachte frequentie van uitwisseling (aantallen per tijdseenheid)?	N.v.t.
3. Wat is de verwachte functionele omvang van de uit te wisselen berichten?	N.v.t.
4. Wat is de gewenste beschikbaarheid van de uitwisseldienst?	N.v.t.
5. Wat is de gewenste betrouwbaarheid van de gegevensuitwisseling?	N.v.t.
6. Zijn er (bijzondere) eisen aan de tijdigheid van uitwisseling?	N.v.t.