



Architectuur Kaders voor Veilige Gegevensuitwisseling

op basis van Enabler Topic TE 010

Doel van dit document

- Dit architectuur document beschrijft de conclusies van enabler topic TE010 “Kaders voor veilige gegevensuitwisseling”
- Dit topic is uitgewerkt en goedgekeurd in de CoP SA
- Dit topic is vastgesteld in de ALV MFF van 07-03-2024

Samenvatting TE010

In dit document wordt onderzocht of e-mail een geschikt kanaal is voor gegevensuitwisselingen en of er een alternatief gepositioneerd moet worden.

Met de vaststelling van dit document is akkoord gegaan met de implementatie en inzet van een Berichtenbox.

4 Gekozen oplossing

4.1 Bestaande oplossingsrichtingen voor gegevensuitwisselingen

Samengevat zijn er momenteel in de sector twee officieel² 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 volledigheidscodes	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 conclusie 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

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.

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 volledigheidscntroles	Hoog ⁵
Ondersteuning hoge aantallen	Laag
Kosten	
Implementatiekosten	Laag ⁶

4.2.2 Afwegingskader

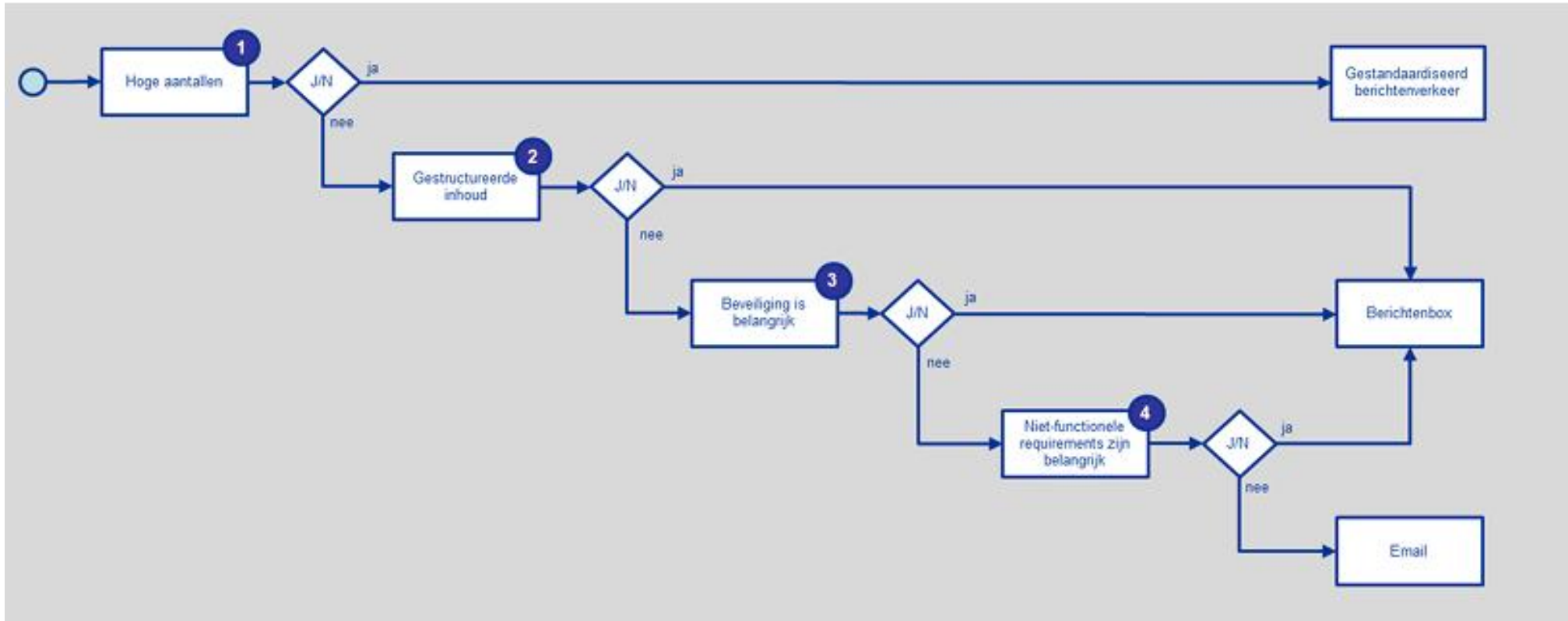
De vraag is dan wel wanneer er gekozen zou moeten worden voor de Berichtenbox en wanneer gestandaardiseerd of e-mail juist te verkiezen is.

Het volgende afwegingskader is hierbij een leidraad⁷ 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 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).

Afwegingskader gegevensuitwisseling

Dit afwegingskader zal toegepast worden in alle toekomstige topics die betrekking hebben op gegevensuitwisseling.



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 flexibiliteit (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 worden:

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

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