Ministerie van Volksgezondheid, Welzijn en Sport

Rapportage onderzoek naar de gevolgen van een verplichting tot E2E-beveiliging

Versie: 1.0 (Definitief)

30 juni 2023

Kenmerk: 2023-0338/[redacted]

pwc

Persoonlijk en vertrouwelijk

Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
T.a.v. [redacted]

30 juni 2023

Onze Referentie: 2023-0338[redacted]

Uw Referentie: 201865007.700.003

Betreft: Rapportage onderzoek naar de gevolgen van een verplichting tot E2E-beveiliging

Geachte [redacted]

Met veel plezier bieden wij onze rapportage aan die invulling geeft aan uw opdracht uitgevoerd conform onze opdrachtbevestiging met referentie 201865007.700.003. Het resultaat is onderhavige eindrapportage die weergeeft wat er nodig is om E2E-beveiliging voor alle (toekomstige) gegevensuitwisselingen onder de Wegiz te implementeren. Hierbij wordt aangegeven welke knelpunten er zijn, met aandacht voor de verschillende uitwisselingssystemen, en hoe deze geadresseerd kunnen worden.

Ons advies is om een minder stringent “pas-toe-of-leg-uit” beleid, toe te passen op nieuw te ontwikkelen methodes om gegevens uit te wisselen. Een risicobepaling vooraf, om te bepalen of E2E-versleuteling of E2E-authenticatie van toegevoegde waarde is, kan een adequate toevoeging zijn. In het rapport kunt u de onderbouwing voor dit advies terugvinden.

Mocht u naar aanleiding van dit document vragen of opmerkingen hebben, dan kunt u contact opnemen met ondergetekende, [redacted] of [redacted]

Hoogachtend,
PricewaterhouseCoopers Advisory N.V.

[redacted]

PricewaterhouseCoopers Advisory N.V., Thomas R. Malthusstraat 5, 1066 JR Amsterdam, P.O. Box 9616, 1006 GC Amsterdam, the Netherlands
T: +31 (0) 88 792 00 20, F: +31 (0) 88 792 96 40, www.pwc.nl

Inhoudsopgave

Afkortingen

AMB	Ambulance
AMBS	Ambulancesysteem
AZN	Ambulancezorg Nederland
BegZ	Besluit elektronische gegevensverwerking door zorgaanbieders.
BgGGZ	Basisgegevensset Geestelijke Gezondheidszorg
BgLZ	Basisgegevensset Langdurige Zorg
BgZ	Basisgegevensset zorg
CI	Certificerende Instellingen
CNIO	Chief Nursing Information Officer
DIZ	Duurzaam informatiestelsel van de zorg
DVZA	Dienstverlener zorgaanbieder
ECD	Elektronisch Cliëntendossier
EGIZ	Nen-programma elektronische gegevensuitwisseling in de zorg
EPD	Elektrisch Patiënten Dossier
FMS	Federatie van Medisch Specialisten
HA	Huisartsen
HAP	Huisartsenpost
HIS-en	Huisartseninformatiesystemen
HL7	Health Level 7
IB zorg	Informatieberaad Zorg
ICA-gegevens	Intoleranties, Contra-indicaties en Allergieën
IGJ	Inspectie Gezondheidszorg en Jeugd
IHE	Integrating Healthcare Enterprise
InEen	Vereniging van organisaties voor eerstelijnszorg
KIK-V	Keteninformatie Kwaliteit Verpleeghuiszorg
LHV	Landelijke Huisartsen Vereniging
LNAZ	Landelijke Netwerk Acute Zorg
LSDV	Landelijk Systeem Digitale Vooraankondiging
LSP	Landelijk Schakelpunt
MKA	Meldkamer Ambulance
MSZ	Medisch specialistische zorg
Msz-instelling	Medisch specialistische zorg instellingen
NEN	Nederlandse Normalisatie-instituut
NedHIS	Koepelorganisatie van HIS-gebruikersverenigingen.
NFU	Nederlandse federatie Universitaire ziekenhuizen
NHG	Nederlandse Huisartsen Genootschap
Nictiz	Nationaal ICT-instituut in de zorg – Nederlands kenniscentrum voor landelijke toepassing van ICT in de zorg.
NLDigital	Collectief van bedrijven die de digitale transformatie mogelijk maken.
NVSHA	Nederlandse beroepsvereniging van spoedeisende hulp artsen
NVvR	Nederlandse Vereniging voor Radiologen
NVZ	Nederlandse Vereniging van Ziekenhuizen
NZa	Nederlandse Zorgautoriteit

OZIS-infrastructuren	Open Zorg Informatie Systemen infrastructuren
PACS	Picture Archiving and Communication System – uitwisselingssysteem radiologisch beeldmateriaal
PFN	Patiënt federatie Nederland
PGO	Persoonlijke Gezondheidsomgeving
RAV	Regionale Ambulancevoorzieningen
SEH	Spoedeisende hulp
TSV	Taskforce Samen Vooruit à samenwerking van een grote groep ICT-leveranciers met als doel om technologische versnelling voor gegevensuitwisseling in de zorg mogelijk te maken (steun van NLdigital, VWS, VNO-NCW, MKB-Nederland).
V&V	Verpleegkundigen en verzorgenden
V&VN	Verpleegkundigen en verzorgenden Nederland (beroepsvereniging)
VIPP OPEN	Versnellingsprogramma informatie-uitwisseling patiënt
VNA	Vendor neutral archive – technologie die medisch beeldmateriaal opslaat in een standaard format en interface.
VRHT	Het versturen van het recept door de huisarts aan de terhandsteller (apotheek)
VVT	Verpleegkundigen, Verzorgingshuizen en Thuiszorg
VZVZ	Vereniging van zorgaanbieders voor zorgcommunicatie à beheert de ontwikkeling en uitvoering van afsprakenstelsels.
Wegiz	Wet elektronisch gegevensuitwisseling zorg
Zibs	Zorginformatiebouwstenen
ZKN	Zelfstandige klinieken Nederland

1. Management Samenvatting

De Wet elektronische gegevensuitwisseling in de zorg (Wegiz) zet het belang van een effectieve gegevensuitwisseling op de kaart door ervoor te zorgen dat zorgverleners beschikken over accurate patiëntgegevens op het juiste moment, op de juiste plaats. Informatiebeveiliging is hierbij van groot belang en een mogelijke toevoeging hierop zou E2E-beveiliging kunnen zijn. Dit rapport geeft in hoofdlijnen weer wat er nodig is om E2E-beveiliging voor gegevensuitwisselingen onder de Wegiz te implementeren, waarbij er aangegeven wordt welke knelpunten er zijn, wat de voorwaarden zijn om deze knelpunten op te lossen en biedt het een advies over E2E-beveiliging. Deze analyse is uitgevoerd op vijf gegevensuitwisselingen waaruit algemene lessen zijn getrokken die van toepassing zijn op het grotere geheel.

Een verplichting tot E2E-beveiliging kan resulteren in een hogere mate van informatiebeveiliging omdat er een additionele laag van beveiligingsmaatregelen wordt toegepast. Een onderscheid moet gemaakt worden tussen E2E-versleuteling en E2E-authenticatie. Beide dienen andere doelen met andere kansen en beperkingen. Door E2E-versleuteling toe te passen krijgen alleen de verzendende en ontvangende partij inzicht in de gedeelde gegevens. Met E2E-authenticatie krijg je zekerheid over de authenticiteit van de opvragende en verzendende persoon die toegang krijgt tot de juiste gegevens. Voor E2E-versleuteling zijn er, afhankelijk van het type gegevensuitwisseling, grote infrastructurele aanpassingen of complete vernieuwingen nodig. Dit zal ook organisatorische gevolgen met zich meebrengen, want de versleuteling moet ook georganiseerd en geïmplementeerd worden. Deze veranderingen brengen daarbij een financiële impact die ook zal doorwerken in het beheer van de nieuwe maatregelen. Voor E2E-authenticatie gelden min of meer dezelfde uitdagingen als hiervoor beschreven. Alhoewel het technologisch haalbaarder is zal voor authenticatie de praktische uitvoerbaarheid een groter knelpunt zijn, vanwege de gebruikersimpact. Deze moeten zichzelf op een andere en wellicht complexere manier authenticeren zo mogelijk met als gevolg administratieve lasten voor zorgverleners.

Een additionele factor die E2E-beveiliging kan bemoeilijken is de gefragmenteerde kennis op het gebied van informatiebeveiliging. Hierdoor zal er voor de implementatie van E2E-beveiliging een grote mate van afhankelijkheid zijn van de leverancier(s) omdat niet alle zorgaanbieders in staat zijn dit vraagstuk zelf op te pakken. Basishygiëne op het gebied van informatiebeveiliging is daarbij voorwaardelijk voor E2E-beveiliging. Ook zullen de NEN-normenkaders en het MedMij afsprakenstelsel aangepast moeten worden aan deze verplichting.

Een regelrechte verplichting om E2E-beveiliging te implementeren lijkt een te grote stap voor veel gegevensuitwisselingen. Het is daarbij van belang om de afweging te maken of de toegenomen mate aan informatiebeveiliging van de gedeelde gegevens met de vereisten van E2E-beveiliging in deze context opwegen tegen de gevolgen. Deze gevolgen zijn niet uniform over de gegevensuitwisselingen heen, maar zijn in het geval van uitwisseling via een derde partij zoals het LSP of LS-DV significant.

Ook voor gegevensuitwisselingen die vergevorderd zijn in het elektronisch uitwisselen van gegevens kan deze verplichting veel impact hebben. Daarentegen kan het voor gegevensuitwisselingen die vroeger in het proces zitten van toegevoegde waarde zijn. Hierbij zal de impact minder zijn, zoals bij het geval van directe gegevensuitwisseling tussen zorgsystemen.

Ondanks de complexiteit van E2E-versleuteling en E2E-authenticatie zitten er wel degelijk voordelen aan. Zo kan een verplichting tot E2E-beveiliging resulteren in een hogere mate van informatiebeveiliging door de additionele laag aan beveiligingsmaatregelen. Een minder stringent “pas-toe-of-leg-uit” beleid, dat van toepassing is op nieuw te ontwikkelen methodes om gegevens uit te wisselen kan wellicht een optimalere insteek zijn. Een risicobepaling vooraf, om te bepalen of E2E-versleuteling of E2E-authenticatie van toegevoegde waarde is, kan een adequate toevoeging zijn.

2. Inleiding

De kwaliteit van de Nederlandse zorg behoort tot de internationale top. De zorg is bovendien volop in beweging. Krapte op de arbeidsmarkt vraagt om een nieuwe benadering hoe wij ons werk doen, de stijgende zorgkosten dwingen ons om na te denken over nieuwe (regionale) samenwerkingsvormen en door medische technologische vernieuwing realiseren wij steeds meer kwaliteit van leven waardoor wij ook anders tegen de gezondheidszorg aankijken dan twintig jaar geleden. Achter al deze bewegingen zit als belangrijke bouwsteen data; data waar wij onze informatie mee verkrijgen en uiteindelijk ons kennis oplevert. Die kennis is de motor achter alle zorgvernieuwing, of het nu gaat om passende zorg of om de verplaatsing van zorg naar de thuisomgeving. Het Integraal Zorgakkoord (hierna: IZA) en de komst van de Wet elektronische gegevensuitwisseling in de zorg (hierna: Wegiz) zetten het belang van een goede gegevensuitwisseling extra op de kaart. Het ministerie van Volksgezondheid, Welzijn en Sport (hierna: VWS) werkt aan de verwezenlijking van de Wegiz. De Wegiz maakt het mogelijk om bij Algemene Maatregelen van Bestuur gegevensuitwisselingen aan te wijzen die in het vervolg gestandaardiseerd, elektronisch worden uitgewisseld. Hiermee komen patiëntengegevens sneller beschikbaar voor overdracht en is de kans op fouten tijdens zorgverlening kleiner.

Tijdens het debat over de Wegiz, is het amendement van de leden Hijink en Van den Berg over end-to-end beveiliging (hierna: E2E-beveiliging) in de zorg door de Tweede Kamer aangenomen. Dit amendement stelt dat gegevensuitwisseling onder de Wegiz "*op het volledige traject tussen zender en ontvanger*" beveiligd moeten zijn. In de toelichting bij dit amendement wordt verder uitgewerkt dat E2E-beveiliging zowel E2E-versleuteling als E2E-authenticatie omvat. In de zorg moeten wij kunnen vertrouwen op data die beschikbaar, integer en vertrouwelijk zijn. Beveiliging borgt deze kwaliteitsaspecten. Als gegevens niet veilig uitgewisseld kunnen worden dan ondermijnt dat de mogelijkheid om de zorg toekomstbestendig en passend te maken.

2.1. Doelstelling

Dit onderzoek is erop gericht meer inzicht te krijgen in de technische en organisatorische gevolgen van het eventueel doorvoeren van een verplichting tot E2E-beveiliging voor alle (toekomstige) gegevensuitwisselingen die onder de Wegiz vallen. Wij hebben hierbij de technische, organisatorische en financiële gevolgen inzichtelijk gemaakt op zowel het niveau van de uitwisseling tussen enkele zorgaanbieders (zorgaanbieder naar zorgaanbieder) als op het niveau van de uitwisseling in een zorgketen als geheel. De inzichten in de gevolgen zijn opgedaan op basis van onderzoek naar enkele representatieve zorgketens.

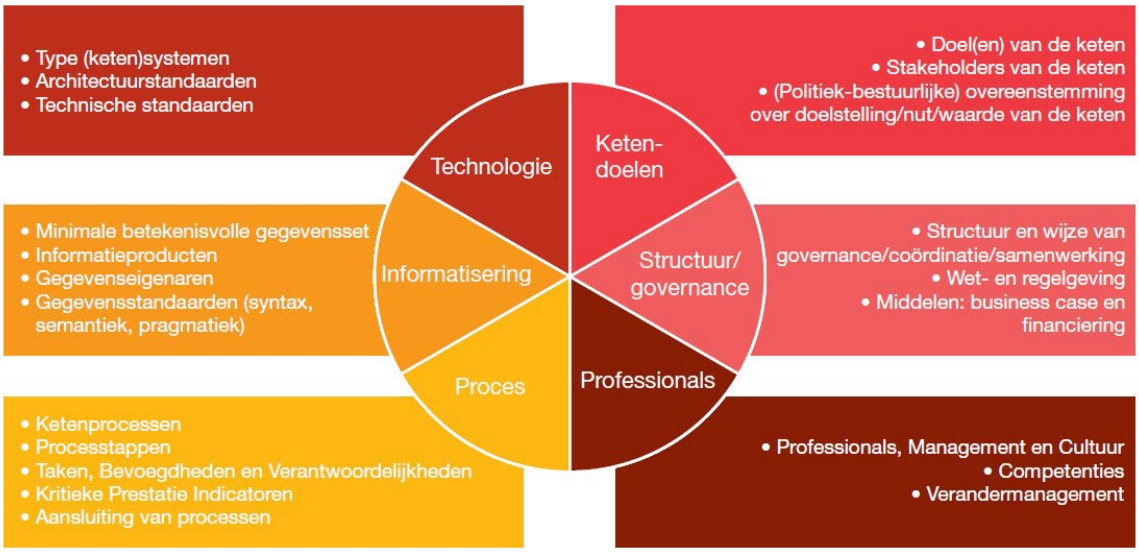
Daarnaast geef dit rapport weer wat er op hoofdlijnen nodig is om E2E-beveiliging voor alle (toekomstige) gegevensuitwisselingen onder de Wegiz te implementeren, waarbij er aangegeven wordt welke knelpunten er zijn, met aandacht voor de verschillende uitwisselingssystemen, en op hoofdlijnen wat er nodig is om deze knelpunten op te lossen. Tevens geeft de rapportage ook een advies over het implementeren van E2E-beveiliging en voorwaarden waaronder dit kan plaatsvinden.

Dit rapport geeft inzichten op basis van de analyse van enkele specifiek benoemde ketens zoals geprioriteerd in het meerjarenagenda Wegiz en het IZA:

- Medicatieoverdracht.
- Overdracht Basisgegevensset Zorg (BgZ) tussen MSZ-instellingen.
- Uitwisseling van beeld en verslag tussen MSZ-instellingen (beeldbeschikbaarheid).
- Verpleegkundige overdracht (eOverdracht).
- Een selectie van de gegevensuitwisselingen uit de Richtlijn Gegevensuitwisseling Acute zorg.

2.2. Methoden en technieken van onderzoek

Om de doelstelling te bereiken is de analyse gestructureerd met ons “Transformatiemodel effectieve ketens” (hierna: Transformatiemodel). Het Transformatiemodel van PwC biedt een praktisch referentiemodel voor alle onderwerpen die relevant zijn voor effectieve ketens waarin meerdere organisaties samenwerken. De relevante onderwerpen worden uitgedrukt in 6 aandachtsgebieden. Met andere woorden: voor een effectieve inrichting van een keten dient aan elk van deze aandachtsgebieden passende aandacht besteed te zijn. Elk van die zes aandachtsgebieden heeft zijn eigen subonderdelen en complexiteit. Daarnaast hangen ze onderling sterk samen. Het onderstaande figuur geeft de 6 aandachtsgebieden weer, en geeft tevens aan uit welke subonderdelen elk aandachtsgebied bestaat:



Figuur 1 Overzicht onderwerpen Transformatiemodel.

Dit model is in deze opdracht als een referentiemodel gebruikt om ervoor te zorgen dat alle relevante onderwerpen onderzocht worden. Het gebruik van het Transformatiemodel en de uitwerking in aandachtsgebieden borgden ook dat de analyse van elke gegevensuitwisseling in meer detail uitgevoerd wordt. De analyse werd vormgegeven langs de volgende onderzoeksvragen:

- **Hoe ziet de huidige situatie er uit?**
- **Wat is er *minimaal* nodig voor E2E-beveiliging, nu en in de toekomst?**
- **Wat zijn mogelijke scenario’s voor E2E-beveiliging?**
- **Wat zijn benodigdheden voor en knelpunten van E2E-beveiliging?**

Voor de vijf geprioriteerde gegevensuitwisselingen hebben wij deze onderzoeksvragen onderzocht door middel van documentstudie en interviews met stakeholders in het veld. Deze gegevensuitwisselingen worden als casuïstiek beschouwd, waaruit specifieke lessen en gevolgen zijn getrokken. Voor dit onderzoek is ervoor gekozen om de analyse te beperken tot deze vijf zodat het onderzoek uitvoerbaar blijft binnen de gestelde periode en er goed invulling gegeven kan worden aan de onderzoeksvragen. Het is dus uitdrukkelijk niet de doelstelling van het onderzoek om volledig te zijn in haar analyse over alle gegevensuitwisselingen. Om deze inzichten te valideren is er per gegevensuitwisseling een klankbordgroep ingericht, waarbij de eerdere gesprekspartners de mogelijkheid hadden om feedback te leveren op de uitwerkingen.

De specifieke benodigdheden en geïdentificeerde knelpunten werden vervolgens samengebracht tot algehele lessen aan de hand van de aandachtsgebieden uit het Transformatiemodel. Deze bevindingen zijn vervolgens gebruikt om antwoord te kunnen geven op de vraag “Welke algehele inzichten brengt dit op E2E-beveiliging, versleuteling en authenticatie?” Daarbij zijn de afsprakenstelsels (zoals MedMij) en NEN-normen die een directe relatie hebben met deze

uitwisselingen ook meegenomen in dit onderzoek. Wij zien dit onderzoek als een belangrijk fundament voor het transformatieproces naar zorg die toekomstgericht is.

2.3. Leeswijzer

Dit rapport begint met het definiëren van E2E-beveiliging. Hierbij wordt er gekeken naar E2E-authenticatie en -versleuteling. Dit hoofdstuk licht daarnaast de twee technische inrichtings-scenario's toe die zijn ontwikkeld. De scenario's geven twee manieren weer waarop E2E-beveiliging bereikt kan worden vanuit een technisch perspectief. Hierbij wordt in het eerste scenario een strikte interpretatie van E2E-versleuteling aangehouden en in het tweede scenario een meer flexibele interpretatie van E2E-versleuteling.

De daaropvolgende hoofdstukken geven op hoofdlijnen aan wat de gevolgen zijn van een verplichting tot E2E-beveiliging, waarbij een onderscheid wordt gemaakt tussen de twee scenario's. Hierbij wordt er gekeken naar de randvoorwaarden en de technische, organisatorische en financiële gevolgen, volgens het Transformatiemodel.

Het daaropvolgende hoofdstuk richt zich op de relevante NEN-normen en afsprakenstelsels. De scope van dit onderzoek is breder getrokken door de NEN-normen en afsprakenstelsels erbij te betrekken. Het belang hiervan werd benadrukt tijdens de interviews. De laatste twee hoofdstukken van dit rapport richten zich op de algemene lessen en adviezen van dit onderzoek.

2.4. Voorwaarden

Wij stellen het rapport op voor u als opdrachtgever, in overeenstemming met de gegeven opdrachtbevestiging. Wij accepteren richting geen enkele andere partij aansprakelijkheid of zorgplicht anders dan u als opdrachtgever op basis van de inhoud van ons rapport.

In het geval u een verzoek ontvangt op grond van de Wet open overheid (hierna: 'Woo verzoek') ter zake van schriftelijke uitingen van PwC, zult u ons hierover onverwijld (in ieder geval voorafgaand aan de te nemen beslissing op het Woo verzoek en derhalve voorafgaand aan eventuele openbaarmaking) schriftelijk informeren. In dat kader zult u ons alle beschikbare achtergrondinformatie met betrekking tot het Woo verzoek verstrekken. Daarbij zult u ons in de gelegenheid stellen om onze visie te geven op het Woo verzoek, vooruitlopend op de door u te nemen beslissing op het Woo verzoek.

Wij baseren onze werkzaamheden op informatie die u ons geeft. Wij nemen aan dat deze informatie juist, volledig en niet misleidend is. Wij voeren geen accountantscontrole uit op de informatie en beoordelen ook niet of deze volledig en juist is volgens internationale audit- of reviewstandaarden.

2.5. Definitie E2E-beveiliging

Om een gedegen onderzoek naar E2E-beveiliging uit te voeren is er overeenstemming nodig over wat de precieze definitie van deze term is.

2.5.1. E2E-beveiliging

Dit betreft alle organisatorische, technologische en procesmatige beveiligingsmaatregelen bij de partijen die betrokken zijn bij de gegevensuitwisseling, zoals zorgaanbieders, leveranciers, uitwisselingssystemen en patiënten. Hierbij kan bijvoorbeeld de NEN 7510 als basis worden gebruikt waarin onder andere maatregelen omtrent continuïteit, toegangsbeveiliging, cryptografie en softwareontwikkeling beschreven zijn. Voor de scope van deze opdracht is bepaald dat alleen E2E-versleuteling en E2E-authenticatie onder de definitie van E2E-beveiliging vallen. In paragraaf 2.5.2 en 2.5.5 duiden wij beide verder. Hierbij moet aangegeven worden dat de volgende onderwerpen ook van belang zijn, maar dat die vanwege de scope van het onderzoek buiten beschouwing gelaten zijn. Deze onderwerpen zijn maatregelen om de integriteit en onweerlegbaarheid van het bericht te valideren.

2.5.2. E2E-versleuteling

Dit betreft alle maatregelen die specifiek gericht zijn op het versleutelen van de gegevens die uitgewisseld worden tussen de zorgaanbieders en faciliterende partijen. E2E-versleuteling gaat derhalve over de cryptografische doelstellingen op vertrouwelijkheid en deels authenticatie. Het

laatste zal in 2.5.5 uitgewerkt worden. Alleen bevoegde functionarissen kunnen (na authenticatie) kennisnemen van gevoelige gegevens. Voor E2E-versleuteling moeten de gegevens op twee manieren versleuteld worden:

Versleuteling van data-at-rest: dit betreft de gegevens die op het opslagmedium opgeslagen zijn. Deze behoren versleuteld te worden conform industrie standaarden zoals AES-256. Dit kan het hele medium betreffen of de specifieke gegevens.

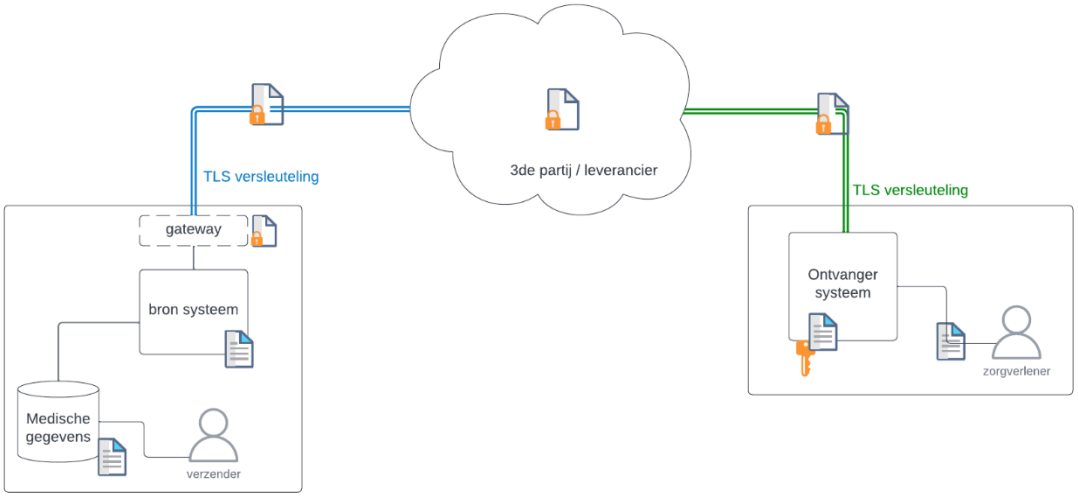
Versleuteling van data-in-transit: dit betreft de gegevens die verzonden worden naar een andere partij. Deze gegevens moeten versleuteld worden met berichtversleuteling en/of kanaalversleuteling. Bij berichtversleuteling worden de gegevens per bericht versleuteld, met symmetrische versleuteling (AES-256) of asymmetrische versleuteling (zoals PGP). Bij kanaalversleuteling worden niet de berichten zelf, maar het kanaal waarover gecommuniceerd wordt, versleuteld met Transport Layer Security (TLS) conform industrie standaarden.

Voor de implementatie van E2E-versleuteling moet aan meerdere generieke maatregelen gedacht worden zoals onder andere keymanagement en certificaatmanagement. Voor dit onderzoek hebben wij twee scenario's uitgewerkt waarbij wij in beide scenario's ervoor hebben gekozen om het systeem als "end" te definiëren en niet de gebruiker. Hiervoor is gekozen om het onderscheid te kunnen duiden tussen de impact van E2E-authenticatie en E2E-versleuteling. Rond versleuteling gaan wij dus uit van "point to point versleuteling" waarbij de systemen als eindpunt dienen. Het gevolg van dit besluit is dat het ontvangende en verzendende systeem ook de daadwerkelijke gegevens in mogen zien. In de E2E-authenticatie definitie wordt het verschil tussen "end" als gebruiker en systeem verder geduid.

Voor dit onderzoek schetsen wij twee scenario's voor de implementatie van E2E-versleuteling. Hierbij hanteren wij een strikte interpretatie van E2E-versleuteling, waarbij geen enkele gegevens ingezien mogen worden, en een flexibele interpretatie van E2E-versleuteling, waarbij de metadata ingezien mag worden. Een uitgebreide definitie is beschreven in paragraaf 2.5.3 en 2.5.4. Wij maken dit onderscheid om aan te tonen dat het van belang is om een duidelijke implementatierichtlijn te hebben. Beide scenario's behalen E2E-versleuteling, maar vereisen andere maatregelen en hebben daarbij ook andere gevolgen. In de analyse op de gegevensuitwisseling nemen wij dan ook beide scenario's mee.

2.5.3. Scenario 1: Een strikte interpretatie van E2E-versleuteling

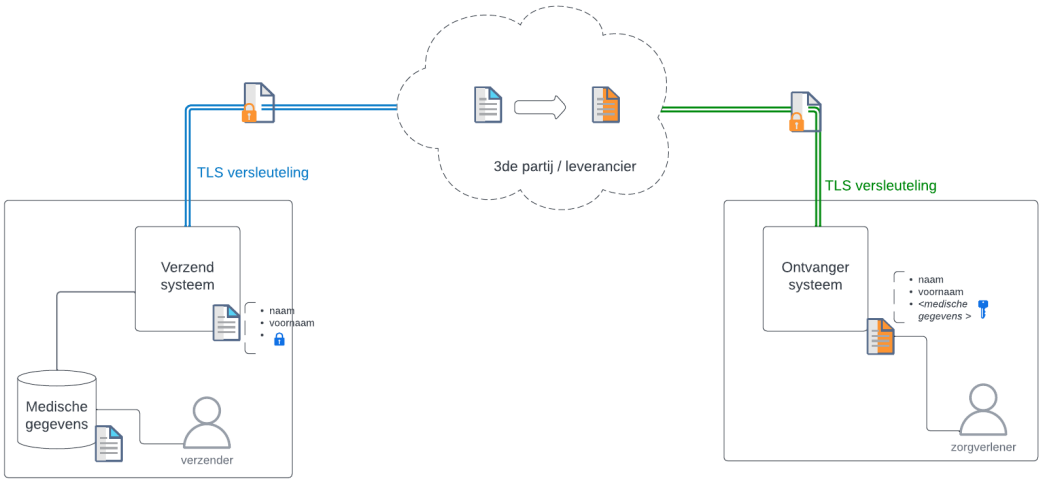
De strikte interpretatie van E2E-versleuteling vereist dat de gegevensuitwisseling van het verzendende systeem tot aan het ontvangende systeem versleuteld is, wat betekent dat eventuele tussenpartijen het bericht niet in kunnen zien. Binnen dit scenario zijn versleutelingsmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen het versturende en ontvangende systeem inzicht hebben in de informatie die wordt uitgewisseld.



Figuur 2: schematische weergave van strikte interpretatie van E2E-versleuteling

2.5.4. Scenario 2: Een flexibelere interpretatie van E2E-versleuteling

De flexibelere interpretatie van E2E-versleuteling vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er in plaats van versleuteling van het volledige bericht (berichtversleuteling) zoals bij Scenario 1, versleuteling binnen het bericht plaatsvindt (element versleuteling) waardoor de gevoelige (medische) informatie binnen het bericht versleuteld zijn. Daarnaast wordt kanaalversleuteling toegepast. Op de gegevenselementen kunnen dus ook nog bepaalde bewerkingen of mappings uitgevoerd worden, gezien de derde partij de metadata kan uitlezen. Hierdoor kan de derde partij het bericht eventueel in het juiste formaat en vorm zetten om vervolgens door te zenden naar de ontvanger.



Figuur 3: Schematische weergave van flexibele interpretatie van E2E-versleuteling

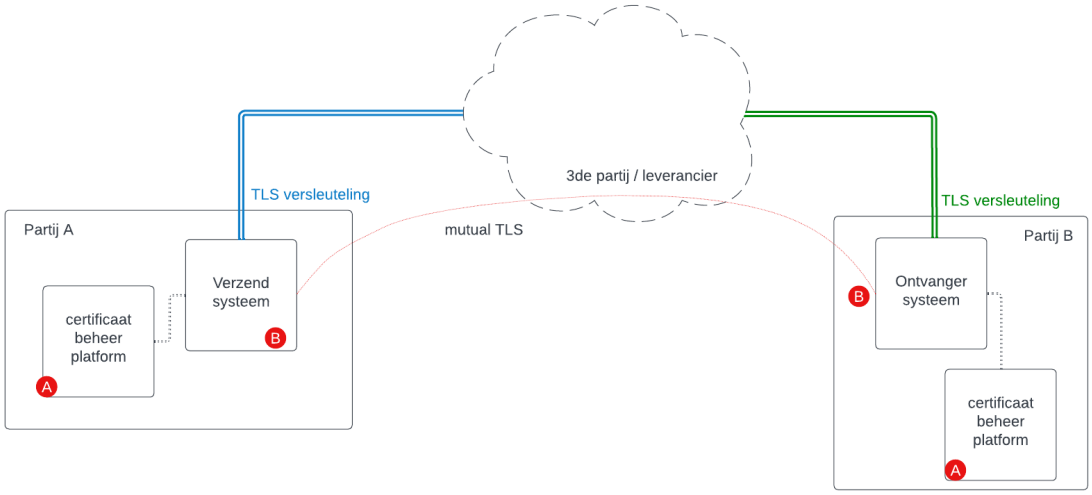
2.5.5. E2E-authenticatie

Authenticatie is het proces van het verifiëren van de identiteit van een entiteit, zoals een gebruiker of apparaat, om ongeautoriseerde toegang te voorkomen. Hierbij kan gebruikgemaakt worden van methoden zoals wachtwoorden, biometrie, twee-factor-authenticatie, certificaten en tokens. Sterke authenticatie methodes zijn essentieel voor de beveiliging van systemen en gegevens. E2E-authenticatie betreft dus de maatregelen om de identiteit van de ontvanger en verstuurder van berichten te authenticeren.

Voor de implementatie van E2E-authenticatie moet aan maatregelen gedacht worden zoals een identity and accessmanagment (IAM) systeem, authenticatiemechanisme, en logging en monitoring. E2E-authenticatie kan dus op verscheidene manieren bewerkstelligd worden. Voor dit onderzoek is de nadruk gelegd op de analyse van de authenticatie methodes bij de diverse partijen. Hierbij moeten er een keuze gemaakt worden over wat er als het end gedefinieerd is. Binnen het E2E-authenticatie vraagstuk kunnen wij twee aparte concepten onderscheiden: a) het authenticeren van de systemen die instaan voor het verzenden en ontvangen van gegevens, alsook b) de eindgebruiker die zich authenticeert.

2.5.5.1. Systeem authenticatie

Systeem authenticatie is gericht op twee eindsystemen die informatie uitwisselen en waarbij beide – meestal aan de hand van certificaten (mutualTLS) – elkaar kunnen identificeren en authenticeren, en daarmee elkaar vertrouwen.



Figuur 4: Schematische weergave van authenticatie op systeemniveau

Belangrijk hier is dat het verzendsysteem en ontvangersysteem (aan de hand van certificaten) certificaten moeten beheren (A) die van elkaar afkomstig zijn. Verzendsysteem en ontvangersysteem (B) zijn in dit geval de enige actoren die bekend zijn binnen de transactie, de noties van een eindgebruiker zijn hier niet van toepassing. Dit is als uitgangspunt genomen voor de definitie op E2E-versleuteling. Daarentegen nemen wij voor E2E-authenticatie de eindgebruiker als end welke hierna verder uitgeschreven.

2.5.5.2. Eindgebruiker authenticatie.

Een eindgebruiker die zich uniek kan identificeren en authenticeren is een belangrijk concept binnen E2E-authenticatie, deze zorgt er namelijk voor dat berichten en gegevens afgeschermd worden op een veel fijnmaziger niveau dan wanneer wij systemen laten authenticeren.

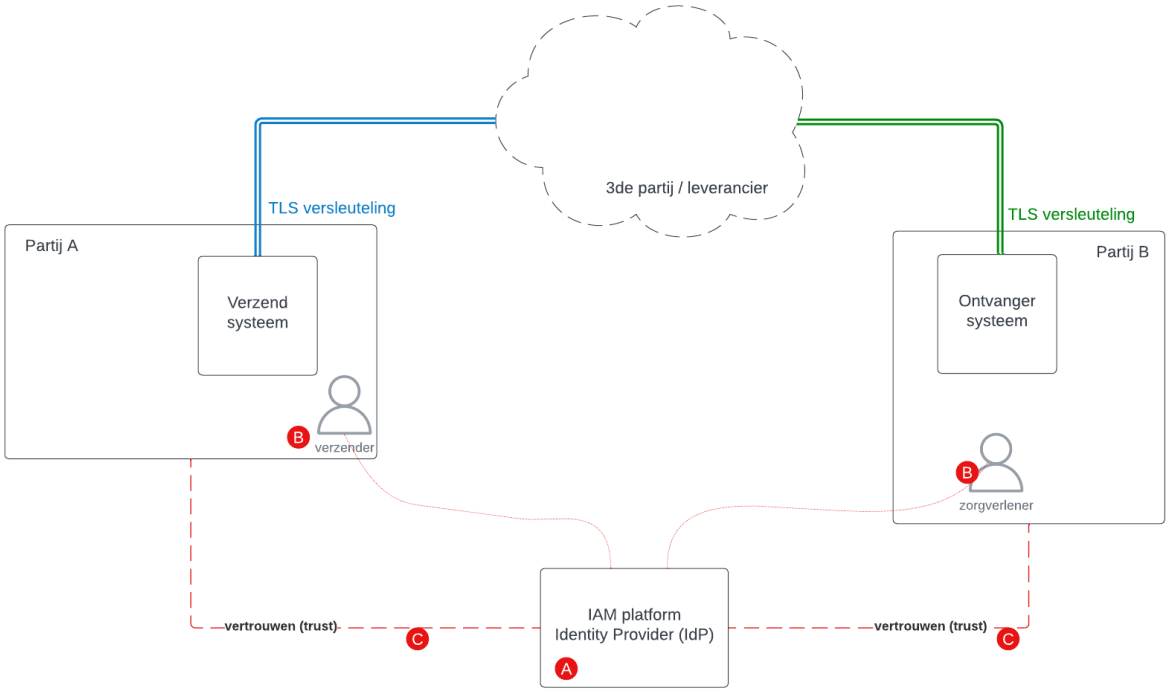
Wanneer wij spreken over eindgebruiker authenticatie zijn er verschillende technische architectuurmodellen mogelijk, waar centraal authenticatie kan plaatsvinden op een eventueel derde systeem (1), bij de verzender zelf (2) of op een systeem waarbij beide platformen een vertrouwensmodel hebben en kunnen federeren (3). Buiten deze drie modellen bestaat er uiteraard nog veel variatie in specifieke scenario's, voor ons onderzoek hebben wij ons echter enkel geconcentreerd op deze drie.

2.5.5.2.1. Centrale authenticatie

Een centraal systeem impliceert hier een platform dat aangestuurd wordt door een hoge electronic Identification, Authentication and Trust Services (hierna: eIDAS) betrouwbaarheid waarbij een natuurlijke persoon zich kan identificeren. Al dan niet met de correcte rol en functie als zorgverlener

of aanbieder. Typische voorbeelden zijn landelijk (door de overheid) aangestuurde platformen die de identiteit kunnen linken aan een natuurlijk persoon.

Dit kan ook beschouwd worden als gefedereerde authenticatie, al is het belangrijkste verschil dat deze authenticatie gebaseerd is op een derde partij die vertrouwd wordt, waarbij wij in ons gefedereerde model verwijzen naar de IAM-systemen van zowel verzender als ontvanger.



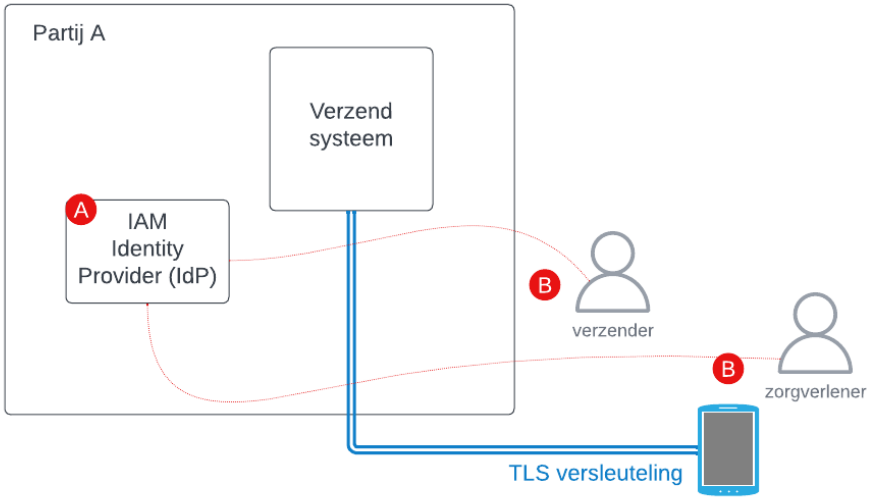
Figuur 5: Schematische weergave van centrale authenticatie

De verzender en ontvanger (B) authenticeren zichzelf beiden op een extern (derde partij) systeem (A) waar beide gebruikers geregistreerd en geverifieerd zijn. Dit systeem heeft een vertrouwensrelatie (C) met zowel verzender als ontvanger. Door deze architectuur ontzorgt het centrale platform de beide partijen in het beheren van deze gebruikers.

2.5.5.2.2. Verzender authenticatie

In dit scenario moet de persoon die het bericht wil opvragen zichzelf authenticeren bij de centrale bron (A) – het verzend systeem – van de medische gegevens.

Hier is het van belang dat de ontvanger en de verzender (B) beide bekend zijn in het systeem en dat de data rechtstreeks naar de eindgebruiker geconsumeerd kan worden (door middel van een persoonlijk toestel).



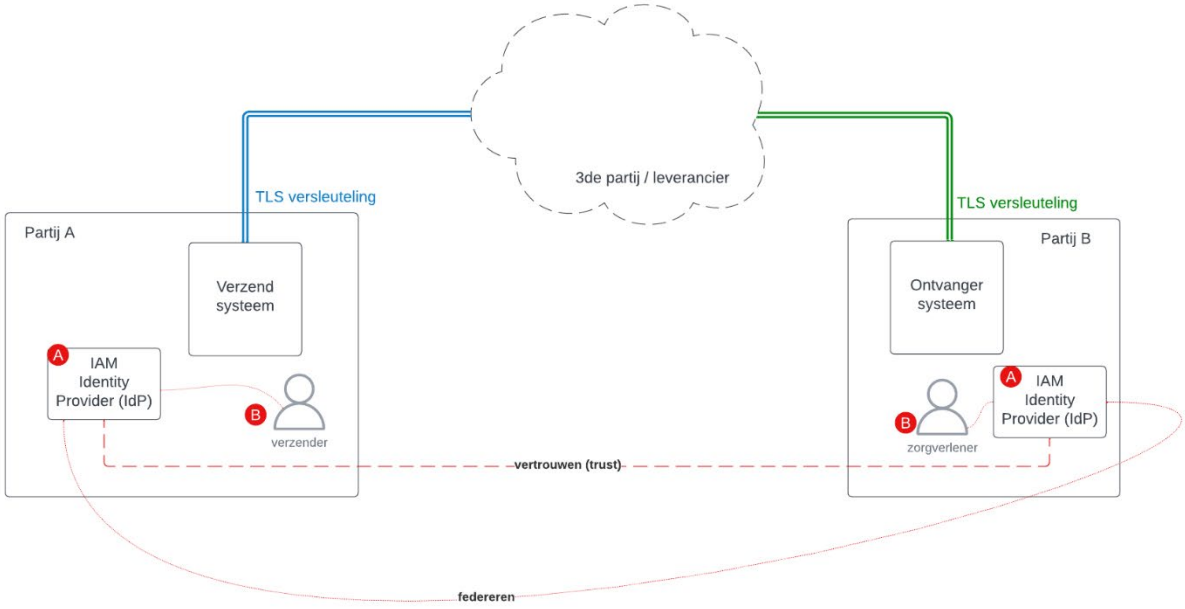
Figuur 6: Schematische weergave centrale van verzender authenticatie

In dit scenario kan een hoge mate van E2E-beveiliging gegarandeerd worden gezien het bericht met zekerheid enkel gelezen zal worden door de eindgebruiker die de bedoelde ontvanger is. Het gevolg is hier wel dat er langs de zijde van de verzender/aanbieder een meer complex beheermodel zal zijn gezien de verantwoordelijkheid voor autorisaties en authenticatie.

2.5.5.2.3. Gefedereerde authenticatie

Bij een gefedereerd model zullen de verzender en ontvanger (B), beide bekend zijn binnen hun eigen systeem, maar Partij A en B hebben een vertrouwensrelatie gelegd tussen de systemen (A) om elkaars identificatie en authenticatie te vertrouwen.

Door middel van een claim kan dan de zorgverlener – eventueel rechtstreeks – de data ophalen van het bronsysteem – de verzender.



Figuur 7: Schematische weergave centrale van gefedereerde authenticatie

In dit scenario moet er door beide partijen een goed beheerd IAM systeem onderhouden worden dat de nodige complexiteit meebrengt voor beide partijen.

Voor alle drie de methodes is het belangrijkste uitgangspunt daarbij dat er onderling vertrouwen tussen de IAM-oplossingen dient te zijn en dat de methode voor authenticatie eIDAS betrouwbaarheidsniveau op hoog geclassificeerd moet zijn. Dit laatste in verband met de gevoeligheid van de gegevens die uitgewisseld worden. Een voorbeeld van een authenticatiemiddel met een hoog betrouwbaarheidsniveau is de UZI-pas.

2.5.6. Kaderstelling door definities

In dit onderzoek is er ook een aantal keuzes gemaakt over wat E2E-versleuteling en E2E-authenticatie is. Door bijvoorbeeld de optie open te laten tot element versleuteling en door te kiezen voor een systeem als “end” en niet een gebruiker als “end”. Hiermee hebben wij het onderzoek kunnen kaderen, maar er zijn vele interpretaties mogelijk. Mocht een verplichting van E2E-versleuteling of authenticatie er komen, dan zal er duidelijkheid geschept moeten worden en zullen verdere keuzes gemaakt moeten worden over de definities en implementaties.

3. Relevantie E2E-versleuteling en E2E-authenticatie

Het doel van dit onderzoek is om de gevolgen van de verplichting van E2E-beveiliging, -versleuteling en authenticatie vast te stellen. Hierbij is een verplichting van E2E-versleuteling en E2E-authenticatie nog geen gegeven. In de huidige wet staat versleuteling niet omschreven. Hierin staat: “op het volledige traject tussen zender en ontvanger zijn beveiligd” waarin E2E-versleuteling en E2E-authenticatie niet gespecificeerd worden. Het is wel goed om stil te staan bij de intentie van deze maatregelen. Het is relevant en biedt een toename in informatiebeveiliging.

De gezondheidszorgsector ondergaat namelijk technologische innovatie en digitalisering, waarbij nieuwe apparatuur en behandelingsprocedures binnen de sector in een exponentieel tempo worden ontwikkeld. Ook is de gevoeligheid van medische gegevens vaak hoog en in de specifieke gevallen van de vijf geprioriteerde gegevensuitwisselingen is dat zeker het geval. Deze gevoeligheid, medische vooruitgang en het belang voor de samenleving als geheel, maakt het een aantrekkelijk doelwit voor verschillende cyberdreigingsactoren.

Daarnaast staat de sector voor meerdere uitdagingen en veranderingen, waaronder een toename van DDoS- en ransomwareaanvallen bij leveranciers, evenals bedreigingen zoals business-email compromise, spoofing en phishing. Ook neemt het gebruik van externe leveranciers en cloudvoorzieningen toe waardoor steeds meer partijen toegang krijgen tot gegevens en er een grotere kans is tot lekken van deze gegevens.

Op basis van onze threat intelligence zien wij dat dreigingsactoren variëren in motivatie, van financieel gewin tot spionage, inlichtingenverzameling en diefstal van intellectueel eigendom. E2E-versleuteling en E2E-authenticatie kan een additionele bescherming zijn tegen spionage en inlichtingenverzameling. Door E2E-versleuteling worden gegevens versleuteld op meerdere manieren waardoor ze minder inzichtelijk worden voor diverse partijen. Hoe minder partijen de gegevens in kunnen zien, hoe minder groot de kans is dat ze gelekt worden. Door E2E-authenticatie is er meer vertrouwen in de identiteit van de opvragende partij over de gehele keten. In het verlengde daarvan zou ongeautoriseerde toegang tot gegevens minder vaak kunnen voorkomen.

Daarnaast wordt er nieuwe wet- en regelgeving geïntroduceerd in de gezondheidszorgsector. In het kader van het Integraal Zorgakkoord wordt er gestreefd naar naleving van de NIS2-richtlijn tegen 2025. Deze richtlijn introduceert een zorgplicht met technische en organisatorische maatregelen, evenals een meldplicht. Ook zal de beveiliging van toeleveringsketens aangepakt moeten worden. E2E-encryptie en E2E-versleuteling kunnen hier onderdeel van zijn.

De gezondheidszorgsector is een sector waar de samenleving meer dan ooit afhankelijk van is. Met zoveel belangen op het spel in een sector die fundamenteel is voor onze samenleving, is het van vitaal belang dat organisaties robuuste en veilige omgevingen en apparatuur creëren en behouden. Daarnaast is het belangrijk dat als het toch een keer misgaat, dat niet meteen alle gegevens gelekt worden en de impact tot een minimum wordt beperkt. E2E-beveiliging en E2E-versleuteling kunnen hier een bijdrage aan leveren. Een verplichting tot deze maatregelen is niet zonder technische, organisatorische, en financiële gevolgen. Deze worden verder uitgewerkt in hoofdstuk 4 en 5 en behoren afgewogen te worden tegen de voordelen.

4. Algemene inzichten verplichting E2E-Versleuteling

Als onderdeel van dit onderzoek is een vijftal geprioriteerde gegevensuitwisselingen geanalyseerd om een beter beeld te krijgen van de huidige situatie, de invloed van een verplichting tot E2E-versleuteling op deze huidige situatie, de technische, organisatorische en financiële gevolgen van een dergelijke verplichting en benodigde randvoorwaarden. Deze specifieke analyses zijn terug te vinden in “Hoofdstuk 9 Bijlagen”.

Onafhankelijk van op welke gegevensuitwisselingen het van toepassing is, zijn er algemene inzichten, met betrekking tot technische, organisatorische en financiële gevolgen te halen uit het verplicht stellen van E2E-versleuteling. Zo kunnen de verschillende methoden voor gegevensuitwisseling die binnen de verschillende geprioriteerde gegevensuitwisselingen worden toegepast gecategoriseerd worden in een aantal overkoepelende methoden voor gegevensuitwisseling. Dit hoofdstuk biedt algemene inzichten door in te gaan op deze overkoepelende methoden en de gevolgen van een verplichting tot E2E-versleuteling voor de aangewezen gegevensuitwisselingen die onder de Wegiz vallen.

Op basis van de uitgevoerde analyse zijn drie overkoepelende methoden van gegevensuitwisseling geïdentificeerd:

1. Gegevensuitwisseling via mail, fax, cd en dvd.
2. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert.
3. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.

Methode	1	2	3
Medicatieoverdracht	X	X	
Basisgegevensset Zorg	X	X	X
Beeldbeschikbaarheid	X	X	
Verpleegkundige overdracht	X	X	X
Acute zorg		X	

Tabel 1 - Geïdentificeerde methode per geprioriteerde gegevensuitwisseling.

In het vervolg van dit hoofdstuk is elk van deze drie methoden van gegevensuitwerking verder uitgewerkt. Dit bevat een beschrijving van de methode en de huidige toepassing, de invloed van een verplichting tot E2E-versleuteling op deze methode aan de hand van de in paragraaf 2.5.3 en 2.5.4 beschreven scenario’s, de gevolgen van een dergelijke verplichting en benodigde randvoorwaarden.

4.1. Gegevensuitwisseling via email, fax, cd en dvd

4.1.1. De huidige situatie

In de huidige situatie worden gegevens veelal ongestructureerd uitgewisseld, bijvoorbeeld aan de hand van (beveiligde) email, fax, telefonisch, cd en dvd. Zo worden in de context van beeldbeschikbaarheid beelden soms nog via koerier naar de ontvangende zorginstelling gebracht. Deze methode van gegevensuitwisseling wordt momenteel uitgefaseerd.

4.1.2. Scenario 1 (strikte interpretatie) in relatie tot de huidige situatie

Scenario 1 vereist dat de gegevensuitwisseling van verzender tot aan de ontvanger versleuteld is, wat betekent dat eventuele tussenpartijen het bericht niet in kunnen zien. Gegevensuitwisseling via fax, cd en dvd zullen niet langer geschikt zijn onder een vereiste tot E2E-versleuteling onder de

Wegiz. Hoewel het mogelijk is om additionele maatregelen te implementeren om E2E-versleuteling te waarborgen zullen deze methoden voor gegevensuitwisseling onder de Wegiz geen optie meer zijn. Op basis van de Wegiz dient de gegevensuitwisseling elektronisch plaats te vinden, waardoor fax, cd en dvd uitgefaseerd dienen te worden. In situaties waar deze methoden op dit moment nog toegepast worden moeten alternatieve methoden voor gegevensuitwisseling geïmplementeerd worden.

Daarnaast worden diverse (beveiligde) emailoplossingen gebruikt om gegevens uit te wisselen. Deze oplossingen zijn verschillend in de manier waarop versleutelingmaatregelen geïmplementeerd zijn. Een groot deel van deze (beveiligde) emailoplossingen voldoet momenteel niet aan Scenario 1, mogelijk zelfs niet wanneer deze NTA 7516 compliant zijn. Dit betekent dan ook dat er voor een groot deel van de (beveiligde) emailoplossing aanpassingen noodzakelijk zijn of dat zorginstellingen overstappen op alternatieve methoden voor gegevensuitwisseling.

4.1.3. Gevolgen van Scenario 1 (strikte interpretatie) op de huidige manier van uitwisseling

Uitgaande van Scenario 1 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolg dat gegevensuitwisseling via fax, cd en dvd niet meer mogelijk zijn. Dit vereist dan ook dat voor deze manieren van gegevensuitwisselingen alternatieven geïmplementeerd dienen te worden. Hierbij is het van belang te benoemen dat deze alternatieve methode van uitwisseling geïmplementeerd dienen te worden ongeacht de beslissing om E2E-versleuteling te verplichten onder de Wegiz. Deze manieren van uitwisseling vallen namelijk niet onder de digitale elektronische uitwisselingen die vanuit de Wegiz verplicht wordt. Daarbij is het ook van belang om mee te nemen dat mocht een vereiste tot E2E-versleuteling doorgevoerd worden, deze alternatieve methoden voor gegevensuitwisseling uiteraard aan dit vereiste moeten voldoen. Een aantal van de alternatieve methoden die op dit moment als onderdeel van bestaande initiatieven (Faexit en DVDexit) geïmplementeerd wordt, voldoet niet aan het vereiste tot E2E-versleuteling. Als gevolg kan een verplichting tot E2E-versleuteling potentieel leiden tot weerstand vanuit zorgaanbieders en leveranciers. De inspanningen die al geleverd zijn kunnen voelen als een verspilling van tijd, moeite en geld.

Uitgaande van Scenario 1 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolg dat voor veel gegevensuitwisselingen die momenteel via email verlopen op dit moment niet voldoen aan de vereisten tot E2E-versleuteling. Dit kan betekenen dat een zorgaanbieder zijn huidige infrastructuur met betrekking tot email volledig moet omgooien en versleuteling van berichten moet implementeren met S/MIME of PGP of over moet stappen op alternatieve methoden voor gegevensuitwisseling.

De technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden worden hieronder verder toegelicht.

Technische gevolgen

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- Berichtversleuteling moet geïmplementeerd worden voor gegevensuitwisseling via email, zoals S/MIME of PGP.

Organisatorische gevolgen

- Er zal relevante kennis opgedaan moeten worden bij de diverse zorgaanbieders, aangezien er in de interviews is aangegeven dat deze onvoldoende aanwezig is op vraagstukken zoals E2E-versleuteling. Hierbij is de kans groot dat de organisatorische verantwoordelijkheid veelal bij de leverancier komt te liggen en/of implementatie ondersteuning geboden moet worden. Dit zal hoogstwaarschijnlijk een langdurend proces zijn.
- Er zal rekening gehouden moeten worden met de kans op weerstand van zorgaanbieders en leveranciers. Voornamelijk in situaties waar al stappen gezet zijn om over te stappen naar alternatieve methoden voor gegevensuitwisseling die niet voldoen aan het vereiste van E2E-

versleuteling. Er moet bijvoorbeeld goed aangetoond worden dat E2E-versleuteling een toegevoegde waarde heeft.

Financiële gevolgen

- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Kosten gerelateerd aan het implementeren van additionele versleuteling maatregelen voor gegevensuitwisseling via email.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.

Randvoorwaarden

- Duidelijke sturing op landelijk niveau waarbij aangegeven wordt wat de specifieke vereisten zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

4.1.4. Scenario 2 (flexibele interpretatie) in relatie tot de huidige situatie

Scenario 2 vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er bijvoorbeeld in plaats van versleuteling van het volledige bericht (berichtversleuteling) versleuteling binnen het bericht plaatsvindt (element versleuteling). De gevoelige (medische) informatie binnen het bericht zijn dan versleuteld naast de kanaal versleuteling die toegepast wordt wanneer het bericht verstuurd wordt.

De iets flexibelere interpretatie van Scenario 2 heeft weinig invloed op deze methode van gegevensuitwisseling in relatie tot Scenario 1. Gegevensuitwisseling via email, fax, cd en dvd voldoet nog steeds niet aan de vereisten van E2E-versleuteling en de Wegiz. Voor gegevensuitwisseling middels (beveiligde) email voldoet momenteel een groot deel niet aan Scenario 2. Dit betekent dan ook dat er aanpassingen noodzakelijk zijn of dat zorginstellingen over dienen te stappen op alternatieve methoden voor gegevensuitwisseling.

4.1.5. Gevolgen van scenario 2 (flexibele interpretatie) op de huidige manier van uitwisseling

De gevolgen van een verplichting tot E2E-versleuteling onder Scenario 2 zijn identiek aan de gevolgen van Scenario 1. Uitgaande van Scenario 2 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolg dat gegevensuitwisseling via fax, cd en dvd niet meer mogelijk zijn. Dit vereist dan ook dat voor deze manieren van gegevensuitwisselingen alternatieven geïmplementeerd dienen te worden. Voor de gegevensuitwisseling via (beveiligde) email heeft versleuteling op berichtniveau de voorkeur omdat hier bestaande standaarden voor geïmplementeerd kunnen worden.

Voor de technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden refereert u naar de sectie hierboven 4.1.3.

4.1.6. Conclusie

In lijn met de Wegiz en reeds bestaande initiatieven dienen gegevensuitwisseling middels fax, cd en dvd uitgefaseerd te worden om de stap te maken naar elektronische gegevensuitwisseling. Het overstappen naar alternatieve methoden voor gegevensuitwisseling gaat tijd en geld kosten. Een verplichting tot E2E-versleuteling heeft voornamelijk tot gevolg dat de alternatieve methoden voor gegevensuitwisseling ook aan de vereisten moet voldoen. Daarnaast worden momenteel, als onderdeel van bestaande initiatieven, ook alternatieve methoden voor gegevensuitwisseling geïmplementeerd die niet aan de vereiste voldoen. Als gevolg kan een vereiste tot E2E-versleuteling potentieel weerstand vanuit zorgaanbieders en leveranciers veroorzaken. De inspanningen die al geleverd zijn kunnen voelen als een verspilling van tijd, moeite en geld.

4.2. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert

4.2.1. De huidige situatie

In de huidige situatie zijn er methoden van gegevensuitwisseling die gefaciliteerd worden door een derde partij. Dit zijn gemeenschappelijke ICT-voorzieningen die nodig zijn voor zorgverleners om onderling gegevens uit te wisselen. Enkele voorbeelden van dergelijke oplossingen zijn het LSP van VZVZ, het LSDV, de Zorgnetwerk Omgeving (ZNO) van Hinq, het Zorgplatform van Chipsoft, Care Everywhere van Epic, het Twiin Portaal van VZVZ en de EVOCS-webapplicatie.

Deze oplossingen hebben uiteenlopende doelen en functionaliteiten en wisselen in mate van integratie met de organisaties eigen systemen. Een aantal functionaliteiten die dergelijke derde partijen biedt zijn hieronder verder toegelicht.

Allereerst verbinden deze derde partijen meerdere zorgaanbieders in een infrastructuur waardoor uitwisseling direct via de oplossing kan plaatsvinden, in plaats vanuit het bronsysteem van de zorgaanbieder. Op deze manier kunnen zorgaanbieders eenvoudig gegevens uitwisselen met een andere bij de derde partij aangesloten zorgaanbieders. Zo kunnen zorgaanbieders door gebruik te maken van het Twiin Portaal van VZVZ beelden en verslagen delen met andere zorgaanbieders als onderdeel van een verwijzing en kunnen verschillende zorgaanbieders samenwerken en gegevens uitwisselen middels het Zorgplatform van Chipsoft.

Voor een aantal geprioriteerde gegevensuitwisselingen is het van belang om niet alleen gegevens te delen door middel van een verwijzing maar ook om gegevens op te vragen. Een aantal partijen zoals het LSP en het LSDV biedt een functionaliteit aan die beide varianten van gegevensuitwisseling ondersteunt. Deze oplossingen bevatten een centrale index die gebruikt kan worden om te achterhalen waar gegevens van een patiënt zich bevinden alvorens deze op te vragen.

Naast het verbinden van verschillende zorgaanbieders bevatten veel uitwisseloplossingen van derde partijen de functionaliteit om een translatie uit te voeren op de gegevens. Een translatie is een vertaalservice die uitgevoerd wordt om uitwisselingen tussen uitwisselstandaarden die verschillen van structuur (bijvoorbeeld XDS/XCA, FHIR) mogelijk te maken. Op deze manier wordt uitwisseling tussen zorgaanbieders die verschillende uitwisselstandaarden hanteren mogelijk.

4.2.2. Scenario 1 (strikte interpretatie) in relatie tot de huidige situatie

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een derde partij die deze uitwisseling faciliteert en een eventuele translatie uitvoert. Binnen Scenario 1 is het delen van gegevens via een dergelijke derde partij veelal geen optie meer, omdat berichtversleuteling betekent dat er geen tussentijdse translatie plaats kan vinden. Een verplichting tot E2E-versleuteling betekent in een dergelijke situatie dan ook dat deze manier van uitwisselen niet langer geschikt zal zijn en er alternatieve methoden geïmplementeerd dienen te worden.

Daarnaast komen er ook situaties voor waar wel berichtversleuteling wordt toegepast, echter gebeurt dit in die gevallen vaak door de derde partij zelf, dus geen E2E-berichtversleuteling. Deze manier van gegevensuitwisseling is niet mogelijk in Scenario 1 wat betekent dat aanpassingen noodzakelijk zijn om aan de vereisten van E2E-versleuteling te voldoen.

Ten slotte bestaan er ook use cases die op basis van een vereiste tot E2E-versleuteling niet meer kunnen plaatsvinden. Een voorbeeld hiervan is het uitwisselen van beelden met zorgverleners die zelf geen ontvangend bronsysteem hebben. In de huidige situatie kunnen deze zorginstellingen de beelden via het portaal van een derde partij inzien. Echter is dit portaal formeel gezien geen “end”. Dit betekent dat onder de definitie van E2E-versleuteling zorgaanbieders zonder een ontvangend systeem de beelden niet meer in kunnen zien.

4.2.3. Gevolgen van scenario 1 (strikte interpretatie) op de huidige manier van uitwisseling

Uitgaande van scenario 1 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolgen dat een aantal methoden die momenteel toegepast worden om gegevens uit te wisselen niet langer mogelijk zijn. Zo kunnen gegevens veelal niet meer uitgewisseld worden via een derde partij zoals het LSP, Zorgplatform of het Twiin Portaal, gezien deze systemen geen (E2E-) berichtversleuteling toepassen.

Zoals reeds benoemd is een belangrijk kenmerk van een aantal van deze gegevensuitwisselingsystemen zoals het LSP en het LSDV dat deze methode vaak niet alleen gebruikt wordt voor verwijzingen maar ook om gegevens op te vragen. Alternatieve gegevensuitwisseling zoals via een gedistribueerd netwerk of via de email lenen zich niet voor deze functionaliteit. Dit betekent dan ook dat, wanneer deze methode van uitwisseling niet meer mogelijk is, er alleen nog maar verwijzingen kunnen plaatsvinden. Het opvragen van gegevens wordt dan complex in verband met problemen voor routering en indexen omdat er geen centraal register is waar een zorgaanbieder kan achterhalen bij welke zorginstelling gegevens opgevraagd kunnen worden. Een gebrek aan zo'n register zal leiden tot overbevragen. In theorie zou E2E-berichtversleuteling geïmplementeerd kunnen worden. Echter heeft dit wel tot gevolgen dat een eventuele translatieslag niet meer mogelijk is.

Een tweede kenmerk van de huidige methode van gegevensuitwisseling is dat deze zorginstellingen in staat stelt gegevens te delen met zorginstellingen die een ander type gegevens gebruiken door een translatie uit te voeren. Wanneer de translatie niet meer uitgevoerd kan worden door een derde partij betekent dit dat ofwel translatie plaats moet vinden bij de bron, wat aanpassingen aan de bronsystemen vereist, ofwel dat er een uniforme standaard voor gegevens geïmplementeerd dient te worden.

Zoals reeds toegelicht bestaan er ook use cases die niet meer uitgevoerd kunnen worden onder een vereiste tot E2E-versleuteling. Bijvoorbeeld in gevallen dat de ontvanger zelf geen ontvangend systeem (een "end") heeft waardoor deze zorginstelling afhankelijk is van het platform van de derde partij om de gegevens in te zien.

De bestaande manieren van gegevensuitwisseling die voldoen aan het vereiste van E2E-versleuteling kunnen niet al deze problemen oplossen, wat betekent dat in situaties waar deze methoden toegepast worden alternatieve methoden voor gegevensuitwisseling dienen te worden gedefinieerd.

De technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden worden hieronder verder toegelicht.

Technische gevolgen

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- Alternatieve oplossingen dienen ontwikkeld te worden voor het lokaliseren, routeren en indexeren van gegevens om overbevraging te voorkomen. Deze oplossingen dienen in lijn te zijn met de principes van E2E-beveiliging.
- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste tot E2E-versleuteling te voldoen. Namelijk het encrypteren van berichten.
- Aanpassingen aan bronsystemen om translatie bij de bron te bewerkstelligen of het implementeren van een uniforme standaard voor gegevens.

Organisatorische gevolgen

- Er moet aangetoond worden dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft zodat weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders opgevangen kan worden.
- Er zal relevante kennis opgedaan moeten worden bij de diverse zorgaanbieders, aangezien er in de interviews is aangegeven dat er onvoldoende kennis aanwezig is op vraagstukken zoals E2E-versleuteling. Hierbij is de kans groot dat de organisatorische verantwoordelijkheid

veelal bij de leverancier komt te liggen en/of implementatie ondersteuning geboden moet worden. De implementatie van E2E-versleuteling zal hoogstwaarschijnlijk een langdurend proces zijn.
- Kans op overbevraging van zorgaanbieders doordat het onduidelijk is waar gegevens zich bevinden (lokalisatie probleem).
- Nieuwe methode voor gegevensuitwisseling dienen ontwikkeld te worden waardoor het een lange tijd kan duren voordat de zorgaanbieders overgestapt zijn op een methode voor gegevensuitwisseling die voldoet aan de eisen van E2E-versleuteling.

Financiële gevolgen

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.

Randvoorwaarden

- Duidelijke sturing op landelijk niveau waarbij aangegeven wordt wat de specifieke vereisten zijn.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

4.2.4. Scenario 2 (flexibele interpretatie) in relatie tot de huidige situatie

Scenario 2 vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er bijvoorbeeld in plaats van versleuteling van het volledige bericht (berichtversleuteling) versleuteling binnen het bericht plaatsvindt (element versleuteling). De gevoelige (medische) informatie binnen het bericht zijn dan versleuteld naast de kanaal versleuteling die toegepast wordt wanneer het bericht verstuurd wordt.

In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een derde partij die deze uitwisseling faciliteert en een translatieslag uitvoert. Om aan de vereisten van E2E-beveiliging te voldoen betekent dit dat deze partij de inhoud van dit bericht niet mag zien. Echter is het voor de translatie noodzakelijk om het bericht te kunnen inzien, waardoor berichtversleuteling geen oplossing is (scenario 1).

De enige werkbare oplossing waarbij de huidige manier van uitwisselen kan blijven bestaan is door versleuteling toe te passen binnen het bericht zelf. Op deze manier is de derde partij nog wel in staat het format te identificeren, echter zijn de daadwerkelijke (medische) gegevens niet meer zichtbaar. Om aan de vereiste tot E2E-versleuteling te voldoen zijn aanpassingen noodzakelijk. Zo dienen er berichtdefinities geformaliseerd te worden zodat de translatie nog steeds uitgevoerd kan worden. Daarnaast moet E2E-versleuteling op elementniveau ingericht worden, wat betekent dat de zorgverlener zelf deze elementen dient te versleutelen alvorens deze beschikbaar worden gesteld aan de derde partij voor uitwisseling.

4.2.5. Gevolgen van Scenario 2 (flexibele interpretatie) op de huidige manier van uitwisseling

Uitgaande van scenario 2 heeft een vereiste tot E2E-beveiliging van gegevensuitwisseling tot gevolg dat een aantal grote aanpassingen gedaan moet worden. Zo kunnen gegevens alleen uitgewisseld worden via een derde partij zoals het LSP, Zorgplatform of Care Everywhere, wanneer er verdere standaardisatie van berichtdefinities plaatsvindt en additionele maatregelen worden geïmplementeerd.

Daarnaast is het goed om te benadrukken dat zulke aanpassingen niet van de een op de andere dag doorgevoerd kunnen worden. Het proces van het verder standaardiseren van berichtdefinities is ingewikkeld en gaat tijd en afstemming tussen verscheidene partijen vereisen. Daarnaast moet het onderzocht worden of er use cases zijn waarbij versleuteling op elementniveau niet werkbaar

is voor de translatie, zoals bijvoorbeeld het geval is bij het delen van beelden. Een ander voorbeeld het gegevenselement “naam”. Als deze opgeknipt moet worden naar “voornaam” en “achternaam” kan dat niet op de versleutelde vorm. Ook kunnen er beperkingen zijn in het ontvangende of verzendende systeem met betrekking tot het verwerken van het versleutelde bericht. Hierover moeten dus afspraken gemaakt worden en moet de technische uitwerking geïmplementeerd worden. Daarnaast valt ook te beargumenteren dat het hebben van een centrale index voor het lokaliseren van medische gegevens ook aan de principes van E2E-beveiliging zou moeten voldoen.

De technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden worden hieronder verder toegelicht.

Technische gevolgen

- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste tot E2E-versleuteling te voldoen.
- Berichtdefinities dienen geformaliseerd te worden.
- Versleuteling binnen de berichten aan de hand van de berichtdefinities dienen geïmplementeerd te worden.
- Alternatieve oplossingen dienen ontwikkeld te worden voor het lokaliseren, routeren en indexeren van gegevens in lijn met de principes van E2E-beveiliging.

Organisatorische gevolgen

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde heeft met betrekking tot informatiebeveiliging.
- Er zal relevante kennis opgedaan moeten worden bij de diverse zorgaanbieders, aangezien er in de interviews is aangegeven dat er onvoldoende kennis aanwezig is op vraagstukken zoals E2E-versleuteling. Hierbij is de kans groot dat de organisatorische verantwoordelijkheid veelal bij de leverancier komt te liggen en/of implementatie ondersteuning geboden moet worden. De implementatie van E2E-versleuteling zal hoogstwaarschijnlijk een langdurend proces zijn.
- Er dient afstemming plaats te vinden tussen verscheidene partijen met betrekking tot de berichtdefinities.
- Alle partijen dienen de geformaliseerde berichtdefinities over te nemen voor gegevensuitwisseling die via een derde partij loopt, waardoor het een lange tijd kan duren voordat de zorgaanbieders overgestapt zijn op een methode voor gegevensuitwisseling die voldoet aan de eisen van E2E-versleuteling.

Financiële gevolgen

- Kosten gerelateerd aan het implementeren van additionele maatregelen.
- Kosten gerelateerd aan het ontwikkelen van berichtdefinities.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.

Randvoorwaarden

- Duidelijke sturing op landelijk niveau waarbij aangegeven wordt wat de specifieke vereisten zijn.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

4.2.6. Conclusie

Een groot deel van de huidige gegevensuitwisselingen vindt plaats aan de hand van een derde partij die de uitwisseling faciliteert. Een verplichting tot E2E-versleuteling heeft tot gevolg dat een groot deel van deze gegevensuitwisselingen niet meer (in de bestaande vorm) uitgevoerd kunnen worden. De grootste knelpunten zitten hierbij in drie hoofdzakelijke punten; 1) gegevensuitwisseling over verschillende standaarden, 2) lokalisatie (lokaliseren van gegevens) voor het opvragen van gegevens en 3) use cases die zich niet lenen voor E2E-versleuteling.

Een verplichting tot E2E-versleuteling betekent dus fundamentele aanpassingen aan de huidige manier van gegevensuitwisseling. Daarnaast introduceert deze verplichting een aantal complexiteiten waar op dit moment nog geen passende oplossingen voor zijn. Om die reden moet een afweging gemaakt worden of de additionele mate van beveiliging opweegt tegen de gevolgen en of het de interoperabiliteit bevordert.

4.3. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen

4.3.1. De huidige situatie

Een derde vorm van gegevensuitwisseling is gegevensuitwisseling die uitgevoerd wordt door gebruik te maken van directe uitwisseling tussen de zorgsystemen. Zorgaanbieders wisselen vanuit hun eigen bronsysteem rechtstreeks gegevens uit zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Deze methode leent zich voornamelijk voor gegevensuitwisseling met betrekking tot verwijzingen waarbij eenzelfde standaard gebruikt wordt. Over de verschillende gegevensuitwisselingen heen zijn twee varianten geïdentificeerd: 1) gegevensuitwisseling op basis van de Nuts Standaarden en 2) point-to-point oplossingen.

Een deel van de gegevensuitwisselingen vindt plaats op basis van de Nuts Standaarden. Zorgaanbieders kunnen aansluiten op het Nuts-netwerk om zo onderling gegevens uit te wisselen. Het Nuts-netwerk creëert een vertrouwenslaag waarbij geen centrale Nuts-server gebruikt wordt. Bij Nuts vormen de deelnemers samen een gedistribueerd netwerk, waarbij verantwoordelijkheid voor het netwerk bij de deelnemers ligt. Gegevens blijven zo alleen bij de uitwisselende partijen. Aan deze methode voor gegevensuitwisseling zijn verschillende leveranciers aangesloten. Zo kunnen er bijvoorbeeld in relatie tot de BgZ vanuit het Nexus EPD van Nexus-Nederland en het Medicore ECD van Tenzinger gegevens uitgewisseld worden met andere partijen uit het Nuts-netwerk. Het gaat hierbij om verwijzingen op basis van eenzelfde gegevensstandaard.

Een tweede variant van gegevensuitwisseling die wordt toegepast zijn zogenaamde point-to-point oplossingen. In deze variant vindt gegevensuitwisseling plaats tussen de zorginstellingen die eenzelfde leverancier gebruiken. In dit geval kunnen gegevens direct uitgewisseld worden.

4.3.2. Scenario 1 (strikte interpretatie) in relatie tot de huidige situatie

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals bijvoorbeeld kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. Voor gegevensuitwisseling via een gedistribueerd netwerk worden de gegevens rechtstreeks vanuit het bronsysteem van de zorgaanbieder gecommuniceerd naar het bronsysteem van de ontvangende zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Daarnaast worden er versleutelingmaatregelen genomen om te bewerkstelligen dat alleen de versturende en de ontvangende partij de gegevens in kunnen zien. In de meeste gevallen bevat dit zowel bericht- als kanaal-versleuteling waardoor deze manier van uitwisseling voldoet aan de vereisten van E2E-versleuteling. In sommige point-to-point oplossingen wordt geen berichtversleuteling toegepast. In een dergelijke situatie zijn aanpassingen noodzakelijk.

4.3.3. Gevolgen van Scenario 1 (strikte interpretatie) op de huidige manier van uitwisseling

Een groot deel van de uitwisselingen die direct van zorgsysteem tot zorgsysteem verlopen voldoet al aan de vereisten van E2E-versleuteling. In de situaties waar op dit moment nog geen berichtversleuteling ingericht is, dient deze te worden geïmplementeerd. Dit betekent dan ook dat de gevolgen van een dergelijke versleuteling beperkt zijn.

De technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden worden hieronder verder toegelicht.

Technische gevolgen

- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste E2E-versleuteling te voldoen. Namelijk het encrypten van berichten.

Organisatorische gevolgen

- Er zal rekening gehouden moeten worden met de kans op weerstand van zorgaanbieders en leveranciers. Voornamelijk in situaties waar al stappen gezet zijn om over te stappen naar een alternatieve methode voor gegevensuitwisseling die niet voldoen aan het vereiste van E2E-versleuteling. Er moet bijvoorbeeld goed aangetoond worden dat E2E-versleuteling een toegevoegde waarde heeft.
- Er zal relevante kennis opgedaan moeten worden bij de diverse zorgaanbieders, aangezien er in de interviews is aangegeven dat er onvoldoende kennis aanwezig is op vraagstukken zoals E2E-versleuteling. Hierbij is de kans groot dat de organisatorische verantwoordelijkheid veelal bij de leverancier komt te liggen en/of implementatie ondersteuning geboden moet worden. De implementatie van E2E-versleuteling zal hoogstwaarschijnlijk een langdurend proces zijn.

Financiële gevolgen

- Kosten gerelateerd aan het implementeren, beheren en in stand houden van de additionele maatregelen.

Randvoorwaarden

- Duidelijke sturing op landelijk niveau. Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

4.3.4. Scenario 2 (flexibele interpretatie) in relatie tot de huidige situatie

Scenario 2 vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er bijvoorbeeld in plaats van versleuteling van het volledige bericht (berichtversleuteling) versleuteling binnen het bericht plaatsvindt (element versleuteling). De gevoelige (medische) informatie binnen het bericht zijn dan versleuteld naast de kanaal versleuteling die toegepast wordt wanneer het bericht verstuurd wordt.

De iets flexibelere interpretatie van Scenario 2 heeft weinig invloed op deze methode van gegevensuitwisseling in relatie tot Scenario 1. Een groot deel van de uitwisselingen die via een gedistribueerd netwerk verloopt voldoet al aan de vereisten van E2E-versleuteling. Dit betekent dan ook dat de gevolgen van een dergelijke versleuteling beperkt zijn. In de situaties waar op dit moment nog geen berichtversleuteling ingericht is, dient deze te worden geïmplementeerd.

4.3.5. Gevolgen van Scenario 2 (flexibele interpretatie) op de huidige manier van uitwisseling

De gevolgen van een verplichting tot E2E-versleuteling onder Scenario 2 zijn identiek aan de gevolgen van Scenario 1. Een groot deel van de uitwisselingen die via een gedistribueerd netwerk verloopt voldoet al aan de vereisten van E2E-versleuteling. In de situaties waar op dit moment nog geen berichtversleuteling ingericht is, dient deze te worden geïmplementeerd. Dit betekent dan ook dat de gevolgen van een dergelijke versleuteling beperkt zijn.

Voor de technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden refereert u naar sectie 4.3.3.

4.3.6. Conclusie

Een verplichting tot E2E-versleuteling zal geen grote gevolgen hebben voor een groot deel van de bestaande gegevensuitwisselingen die ingericht zijn volgens de Nuts Standaarden of een point-to-point oplossing gebruiken. Wel moet er vastgesteld worden of er voor alle point-to-point oplossingen berichtversleuteling plaatsvindt. Voor de gevallen waar dit niet zo is moeten aanpassingen gemaakt worden.

4.4. Conclusie algemene inzichten verplichting E2E-Versleuteling

Op basis van de uitgevoerde analyse zijn drie overkoepelende methoden van gegevensuitwisseling geïdentificeerd die over de verschillende geprioriteerde gegevensuitwisselingen toegepast worden:

1. Gegevensuitwisseling via email, fax cd en dvd.
2. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert.

3. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.

Een verplichting tot E2E-versleuteling is in een zekere mate van invloed op elk van deze methoden. Methode 1 moet de komende jaren volledig uitgefaseerd worden als onderdeel van de Wegiz. Een verplichting tot E2E-versleuteling is alleen van invloed op de alternatieve methoden die als gevolg van de uitfasering geïmplementeerd worden. Gezien de grote afhankelijkheid van methode 2 is het niet realistisch om voor deze gegevensuitwisseling op de korte termijn over te gaan naar een manier van gegevensuitwisseling die voldoet aan de vereisten zonder een aantal cruciale functionaliteiten te verliezen zoals translatie en lokalisatie. Eventueel kan met een langere termijn visie, voldoende sturing en technologische ontwikkeling een doelsituatie van E2E-versleuteling wel bereikt worden. De gevolgen van een verplichting tot E2E-beveiliging op methode 3 zijn te overzien. De voornaamste reden hiervoor is dat een groot deel van de gegevensuitwisselingen momenteel al voldoen het vereiste van E2E-versleuteling.

5. Algemene inzichten verplichting E2E-authenticatie

5.1.1.1. E2E-authenticatie in relatie tot de huidige situaties

De vele vormen van authenticatie en de mogelijke combinaties van zowel systeem als eindgebruiker authenticatie maken het E2E-authenticatie vraagstuk complexer. Authenticatie moet als een verhaal naast E2E-versleuteling gezien worden. Waar E2E-authenticatie voor beide eindes belangrijk is, kan het niet op een verzendende of ontvangende partij afgezet worden als de verantwoordelijke om dit te voorzien. Zowel de zender als ontvanger moet een hoge mate van zekerheid hebben dat de verzender en de ontvanger de correcte personen zijn die de gegevens mogen versturen en inzien. De manieren waarop dat bewerkstelligd kan worden zijn uitgewerkt in paragraaf 2.5.5.

In de huidige situatie vindt een deel van de gegevensuitwisselingen plaats conform betrouwbaarheidsniveau eIDAS hoog, namelijk door middel van de UZI-pas, zo is deze bijvoorbeeld verplicht binnen de LSP. In andere gevallen vindt er geen gegevensuitwisselingen plaats conform betrouwbaarheidsniveau eIDAS hoog. Voor bijvoorbeeld verpleegkundige overdracht wordt gebruikgemaakt van Single-Sign-On (SSO), 2-factor authenticatie en Yivi (self-sovereign identity). Daarnaast wordt er bij andere gegevensuitwisselingen ook gekeken om DigiD te implementeren als authenticatiemiddel.

5.1.1.2. Gevolgen van E2E-authenticatie op de huidige manier van uitwisseling

Indien de vereiste van E2E-authenticatie er komt heeft dat tot gevolg voor de situaties wanneer er bijvoorbeeld enkel SSO, 2-factor authenticatie of Yivi toegepast wordt. Deze manieren van authenticatie zijn niet langer mogelijk of schieten tekort in het leveren van het correct en met zekerheid identificeren van de gebruiker. Bijvoorbeeld dat er geen fysieke controle van de identificatie plaatsvindt. Dit vereist dat alternatieve methoden voor authenticatie dienen te worden gedefinieerd en geïmplementeerd. Belangrijk is hier om steeds een onderscheid te maken tussen systemen die informatie uitwisselen en eindgebruikers die zich authenticeren om ofwel de gegevens te versturen ofwel deze op te vragen.

Een alternatieve methode om E2E-authenticatie te bereiken is de implementatie van de UZI-pas. Echter is tijdens de gesprekken vastgesteld dat deze methode niet altijd leidt tot de juiste toepassing in de praktijk. Zo is het niet voor alle zorgverleners mogelijk een UZI-pas te verkrijgen en is dit authenticatiemiddel erg kostbaar, en ontbreekt het aan een landelijk dekkend netwerk om authenticatie op te vangen voor een brede groep zorgverleners, professionals en patiënten. Daarnaast wordt de huidige toepasbaarheid van de UZI-pas niet als gebruiksvriendelijk ervaren waardoor er soms naar workarounds binnen het authenticatie proces gezocht wordt. Ook zou de toepassing van DigiD Hoog een mogelijke methode zijn, echter zal hier verder onderzoek naar gedaan moeten worden.

Een zwaarwegend gevolg van een nieuwe methode is de gebruikersimpact. In tegenstelling tot E2E-versleuteling, heeft een nieuwe vorm van authenticeren direct impact op zorgverleners. Uit de interviews kwam naar voren dat het authenticeren op het niveau van de gebruiker op voorhand al als ongewenst gezien wordt omdat dit niet bruikbaar is in de praktijk. Dit kan, volgens de geïnterviewden, namelijk resulteren in de belemmering voor het leveren van bijvoorbeeld acute zorg.

Technische gevolgen:

- Alternatieve methoden voor authenticatie dienen gedefinieerd en geïmplementeerd te worden conform betrouwbaarheidsniveau eIDAS Hoog.

- (Landelijke) betrouwbare voorziening in een bron voor authenticatie & autorisatie van gebruikers.
- Het beheer van middelen, zoals telefoons of passen, zal in complexiteit en aantallen toenemen.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Naast algemene kennis op informatiebeveiliging betekent dit dat er meer gespecialiseerde kennis nodig is op de concepten van sleutel- en certificaatbeheer. In de huidige situatie is dit al gesignaleerd als een beheer probleem.
- Het definiëren van en overstappen naar andere methoden voor authenticatie is een langdurend proces wat aanzienlijk verandermanagement capaciteiten vereisen.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor authenticatie.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van authenticatie die wel voldoet aan het vereiste van betrouwbaarheidsniveau eIDAS Hoog.
- Kosten gerelateerd aan het (middelen)beheer die benodigd zijn voor eIDAS Hoog.

Randvoorwaarden:

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals, zoals niet steeds opnieuw in moeten loggen.
- Oplossingen dienen gebruiksvriendelijk te zijn. Zo weinig mogelijk belemmeringen.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

Naast deze gevolgen zijn er een aantal landelijke initiatieven en ontwikkelingen, zoals het “Toekomst bestendig maken UZI-middelen”, eIDAS 2.0 en Wet digitale overheid, die niet meegenomen zijn in dit onderzoek. Mocht er een E2E-authenticatie verplichting komen dan zullen deze vereisten ook meegenomen moeten worden in deze initiatieven.

6. Analyse op relevante normen en afsprakenstelsels

Het is geen doelstelling van dit onderzoek om een uitvoerige analyse uit te voeren op de NEN-normen of het MedMij-afsprakenstelsel. Desondanks is het wel van belang om het mee te nemen, omdat veel van de geïnterviewde deelnemers leunen op deze normen om aan te tonen dat ze E2E-beveiliging hebben geïmplementeerd. Deze normen geven de basis-ingrediënten aan om E2E-beveiliging toe te passen. Het beschrijft bijvoorbeeld dat er versleuteling van het bericht en kanaal moet plaatsvinden, alsmede dat logging ingeregeld moet worden, en hoe er geauthenticeerd moet worden, maar het schrijft niet voort dat tussenliggende verwerkers of endpoints geen inzage in de gegevens mogen hebben. Daarnaast is het MedMij afsprakenstelsel van belang voor gegevensuitwisselingen waarbij een Persoonlijke Gezondheidsomgeving (PGO) betrokken is. In principe is de PGO bij alle aangewezen gegevensuitwisselingen in beeld. Voor dit onderzoek heeft het extra relevantie, omdat bij het uitwisselen van bijvoorbeeld beeldmateriaal en verslagen tussen MSZ-instellingen, evenals bij VRHT Medicatieoverdracht de PGO in beeld is.

6.1. De normen NEN7510, NEN7512 en NEN7513

De NEN 7510-normen zijn specifiek ontwikkeld voor de sector gezondheidszorg in Nederland. Deze normen hebben betrekking op de informatiebeveiliging binnen de gezondheidszorg en zijn bedoeld om de vertrouwelijkheid, integriteit en beschikbaarheid van gezondheidsinformatie te waarborgen. Een certificering op de NEN7510 normen geeft in zekere mate aan dat de betreffende partij betrokken bij een gegevensuitwisseling een effectief management systeem voor informatiebeveiliging heeft, maar geeft geen inzicht in de mate en kwaliteit van E2E-beveiliging. De verdiepende normen op veilige gegevensuitwisseling NEN 7512 en op logging NEN7513 geven dit inzicht evenmin.

De NEN 7512 norm, ontwikkeld voor elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, onderschrijft het belang van versleuteling in-transit. In het onderdeel “6.2.5 Versleuteling” wordt gesproken over diverse beheersmaatregelen die genomen kunnen worden. Hierbij wordt ook het algemeen gedragen “defence in depth” model gebruikt, waarbij wordt aangegeven dat er in principe vertrouwd moet worden op een gelaagde verdediging. Dat betekent in het geval van hoge risicoklassen, wat van toepassing is op de vijf onderzochte gegevensuitwisselingen, er altijd meerdere lagen van versleuteling toegepast moet worden. Hierbij heeft men de keuze uit berichtversleuteling, kanaalversleuteling of het gebruik van een beveiligd netwerk. Ook beschrijft het maatregelen op het ondertekenen van berichten en met welk eIDAS betrouwbaarheidsniveau er authenticatie moet plaatsvinden. Daarentegen, schrijft het niet voor dat tussenliggende verwerkers of endpoints geen inzage in de gegevens mogen hebben en voorziet deze norm dus niet in E2E-versleuteling.

Hetzelfde principe geldt voor de NEN 7513 norm. Deze norm biedt zorgaanbieders aanwijzingen voor het loggen en gebruik van de logging om te voldoen aan wettelijke verplichtingen en levert ontwikkelaars van informatiesystemen een aantal eisen waaraan hun systemen moeten voldoen. Deze beschrijft op hoofdlijnen hoe de logbestanden opgeslagen moet worden, maar niet voldoende om interoperabiliteit op logging vast te stellen wat benodigd is voor E2E-beveiliging.

Aangegeven kan worden dat met het voldoen aan de NEN-normen, er niet per definitie voldaan wordt aan de strikte of flexibele definitie van E2E-versleuteling. Als een E2E-beveiliging, met de huidige definities van E2E-authenticatie en E2E-versleuteling, verplichting bewerkstelligd wil worden via de NEN-normen dan vereist dat aanpassingen aan de normen zelf. Deze moeten uitgebreid worden met specifieke maatregelen en de bestaande maatregelen moeten explicieter uitgeschreven worden.

6.2. MedMij-afsprakenstelsel

Het MedMij-afsprakenstelsel draagt eraan bij dat persoonsgebonden, gevoelige en vertrouwelijke gezondheidsgegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen persoonlijke gezondheidsomgevingen en aanbieders. Het MedMij-afsprakenstelsel bestaat uit een samenhangende set afspraken, voorzieningen en ingerichte ontwikkel- en beheerprocessen. Partijen die diensten willen bieden aan personen of aanbieders kunnen als deelnemer toetreden tot het afsprakenstelsel in de rol van dienstverlener aanbieder (DVA's) en dienstverleners persoonsdomein (DVP's). DVA's kunnen bijvoorbeeld ICT-leveranciers van zorgverleners zijn, terwijl DVP's ICT-leveranciers van Persoonlijke Gezondheidsomgevingen (PGO's) vertegenwoordigen. Via dit afsprakenstelsel kunnen ze informatie uitwisselen, waardoor DVP's verbinding kunnen maken met DVA's en vice versa. De uitwisseling vindt plaats in beide richtingen, waardoor mensen gegevens kunnen verzamelen en delen.

MedMij legt geen specifieke technische implementatiedetails op aan de deelnemers. In plaats daarvan stelt het eisen waaraan zij moeten voldoen. Alle deelnemers dienen in het bezit te zijn van een geldige NEN 7510-certificering, ongeacht hun grootte en of ze dienstverlener in het persoonsdomein of aanbiedersdomein zijn. Deelnemers dienen jaarlijks met een aanvullende auditverklaring aan te tonen dat ze daarnaast voldoen aan het normenkader MedMij. Echter, deze normen bieden onvoldoende garanties voor E2E-beveiliging, zoals aangegeven in het hoofdstuk over NEN-normen. Het verplicht stellen van E2E-beveiliging kan echter ook impact hebben op verschillende punten.

Allereerst fungeert het MedMij-afsprakenstelsel als een netwerk van verbindingen tussen MedMij-deelnemers, de DVA’s en DVP's. Momenteel worden zorgaanbieders en DVA's gezien als dezelfde eindpunten binnen het MedMij-netwerk. Als strikte E2E-beveiliging wordt geïmplementeerd, zouden technische beperkingen moeten worden opgelegd aan de DVA's, waardoor ze de berichten niet kunnen lezen of bepaalde bewerkingen kunnen uitvoeren, zoals translaties.

Ten tweede wordt op dit moment alleen kanaalversleuteling toegepast bij het uitwisselen van berichten tussen de deelnemers. Op dit moment worden de berichten zelf nog niet versleuteld en is het onduidelijk wat de impact zou zijn als deze ook versleuteld zouden worden. Er wordt hier momenteel onderzoek naar gedaan.

Bovendien kan strikte E2E-beveiliging ook gevolgen hebben voor de manier van authenticatie en certificaatbeheer. Het huidige authenticatiesysteem, afhankelijk van DigiD, zou moeten worden aangepast van groepsaansluiting naar clusteraansluiting. Het is echter onduidelijk of dit voldoende is voor E2E-authenticatie, aangezien clusteraansluitingen geen individuele aansluitingen voor zorgaanbieders hebben.

Daarnaast vereist MedMij het gebruik van het certificaat van de DVA in plaats van het certificaat van de zorgaanbieder zelf. Voor E2E-authenticatie zou echter overgegaan moeten worden naar certificaten per zorgaanbieder, wat aanzienlijke organisatorische en financiële gevolgen zal hebben. Het aantal certificaten en de bijbehorende beheerlast zal toenemen.

De E2E-beveiliging verplichting zal dus ook aanzienlijke impact hebben op het MedMij-afsprakenstelsel. Het afsprakenstelsel zelf zou aangepast moeten worden wat zijn doorwerking zal hebben bij de organisaties die betrokken zijn bij het uitwisselen van beeldmateriaal en verslagen tussen MSZ-instellingen, evenals bij VRHT Medicatieoverdracht. Het is daarbij van belang om de afweging te maken of de toegenomen mate aan informatiebeveiliging van de gedeelde gegevens met de vereisten tot E2E-beveiliging in deze context opwegen tegen de gevolgen.

7. Conclusie en advies

7.1. Conclusie

Een verplichting tot E2E-beveiliging kan resulteren in een hogere mate van informatiebeveiliging. Hierbij moet wel duidelijk gemaakt worden dat er een verschil is tussen E2E-versleuteling en E2E-authenticatie. Beide concepten dienen andere doelen en hebben andere kansen en beperkingen. Door E2E-versleuteling worden gegevens versleuteld op meerdere manieren waardoor ze minder inzichtelijk worden voor diverse partijen. Hoe minder partijen de gegevens in kunnen zien, hoe minder groot de kans is dat ze gelekt worden. Door E2E-authenticatie is er meer vertrouwen in de identiteit van de opvragende partij over de gehele keten. In het verlengde daarvan zou ongeautoriseerde toegang tot gegevens minder vaak kunnen voorkomen.

Echter, vereist een dergelijke verplichting grote aanpassingen aan de methode waarop zorgverleners zich kunnen authenticeren en de manier waarop gegevens op dit moment gedeeld worden. Dit is met name het geval voor de verplichting van E2E-versleuteling. Afhankelijk van het type gegevensuitwisseling, zal er een grote technische impact zijn en zijn grote infrastructurele veranderingen nodig om het mogelijk te maken. In enkele gevallen is zelfs complete vernieuwing van de infrastructuur benodigd. Dit zal niet alleen uitdagingen meebrengen voor de technologie, maar dit moet ook georganiseerd worden. Daarnaast zal deze verandering ook een financiële impact hebben door het change proces, maar ook in het beheer van de nieuwe maatregelen.

Voor E2E-authenticatie gelden min of meer dezelfde uitdagingen als hiervoor beschreven. Alhoewel het technologisch iets haalbaarder lijkt in de huidige situaties zal hier de praktische uitvoerbaarheid wel een groter knelpunt zijn, omdat hier een veel grotere gebruikersimpact verwacht wordt. Gebruikers moeten zichzelf in sommige situaties op een andere manier, wellicht complexere, manier authenticeren. Er moet voor gezorgd worden dat dit het slagvaardig handelen van zorgverleners niet in de weg staat en minimale impact moet hebben op (ervaren) administratieve lasten.

Een additionele factor die E2E-beveiliging kan bemoeilijken is de gefragmenteerde kennis op het gebied van informatiebeveiliging, zowel van de zorgaanbieders zelf als van de zorgprofessionals. Binnen sommige zorgaanbieders is er voldoende kennis en kunde om complexe vraagstukken zoals E2E-beveiliging op te kunnen pakken. In andere zorginstelling is dit in mindere mate het geval. Dit is ook van invloed op de huidige volwassenheid op het gebied van informatiebeveiliging in het zorgveld. Basishygiëne op het gebied van informatiebeveiliging is randvoorwaardelijk voor E2E-beveiliging. Daarnaast zal er voor de implementatie van E2E-beveiliging een grote mate van afhankelijkheid zijn van de leverancier omdat niet alle zorgaanbieders instaat zijn dit vraagstuk zelf op te pakken. Daarnaast komt er uit de analyse dat de huidige NEN-normenkaders onvoldoende invulling geven aan E2E-versleuteling en E2E-authenticatie. Eveneens zal het afsprakenstelsel MedMij aangepast moeten worden aan deze verplichting.

Als laatst is het belangrijk om mee te nemen dat er in de huidige wet niet E2E-versleuteling of E2E-authenticatie staat omschreven. Hierin staat: “*op het volledige traject tussen zender en ontvanger zijn beveiligd*” waarin E2E-versleuteling en E2E-authenticatie niet gespecificeerd worden.

7.2. Kansen voor verder onderzoek

In dit onderzoek is er ook een aantal keuzes gemaakt over wat E2E-versleuteling en E2E-authenticatie is. Door bijvoorbeeld de optie open te laten tot element versleuteling en door te kiezen voor een systeem als “end” en niet een gebruiker als “end”. Hiermee hebben wij het onderzoek kunnen kaderen, maar er zijn vele interpretaties mogelijk. Mocht een verplichting van E2E-versleuteling of authenticatie er komen dan zal er duidelijkheid geschept moeten worden en keuzes gemaakt moeten worden over de definities en implementaties.

Daarnaast is een handreiking gedaan voor een flexibele interpretatie van E2E-versleuteling. Hierbij is alleen nog onvoldoende bekend wat de praktische uitvoerbaarheid van dit scenario is, omdat er

verder onderzoek gedaan moet worden naar de berichtdefinities en of het juridisch wel opgaat of de metadata wel onversleuteld verstuurd mag worden en niet als persoonsgegevens gezien worden.

Als laatst is er bij meerdere interviews aangegeven dat door deze verplichtingen het gebruik van data voor secundaire doeleinden lastiger tot onmogelijk gemaakt kan worden. Dit behoeft verder onderzoek, maar is wel van invloed op de bepaling van de verplichting van E2E-beveiliging.

7.3. Advies

Een regelrechte verplichting om E2E-beveiliging te implementeren lijkt een te grote stap voor veel gegevensuitwisselingen. Het is daarbij van belang om de afweging te maken of de toegenomen mate aan informatiebeveiliging van de gedeelde gegevens met een vereiste tot E2E-beveiliging in deze context opwegen tegen de gevolgen. Deze gevolgen zijn niet uniform over de gegevensuitwisselingen heen, maar zijn in het geval van uitwisseling via een derde partij significant.

Ook voor gegevensuitwisselingen die vergevorderd zijn in het elektronisch uitwisselen van gegevens kan deze verplichting veel impact hebben. Daarentegen kan het voor gegevensuitwisselingen die vroeger in het proces zitten wel van toegevoegde waarde zijn. Hierbij zal de impact minder zijn, zoals bij het geval van gegevensuitwisseling tussen directe zorgsystemen.

Ondanks de complexiteit van E2E-versleuteling en E2E-authenticatie zitten er wel degelijk voordelen aan. Zo kan een verplichting tot E2E-beveiliging resulteren in een hogere mate van informatiebeveiliging doordat er een additionele laag aan beveiligingsmaatregelen geïmplementeerd wordt. Een minder stringent “pas-toe-of-leg-uit” beleid, dat van toepassing is op nieuw te ontwikkelen methodes om gegevens uit te wisselen kan wellicht een optimalere insteek zijn. Een risicobepaling vooraf, om te bepalen of E2E-versleuteling of E2E-authenticatie van toegevoegde waarde is, kan een adequate toevoeging zijn.

8. Bijlagen

A. Analyse “Medicatieoverdracht”

A.1. Huidige status

In de context van elektronische gegevensuitwisseling draait het programma Medicatieoverdracht dat zich richt op een goede, complete elektronische overdracht van medicatiegegevens. In de Richtlijn Overdracht van medicatiegegevens in de keten is een basisset medicatiegegevens afgesproken. Deze basisgegevens moeten beschikbaar zijn voor iedere zorgverlener die voorschrijft, ter hand stelt of toedient. Onder het programma Medicatieoverdracht vallen de volgende typen medicatieoverdracht:

- Medicatieoverdracht | Digitaal voorschrijven en ter hand stellen
- Medicatieoverdracht | Medicatie- en toediengegevens
- Medicatieoverdracht | Laboratoriumgegevens voor medicatie
- Medicatieoverdracht | Contra-indicatie en overgevoeligheden

Op dit moment vindt gegevensuitwisseling plaats langs 2 stromen:

I. Ongestructureerde gegevensuitwisseling
II. Gegevensuitwisseling via een centrale voorziening

Deze twee stromen worden hieronder kort toegelicht aan de hand van enkele voorbeelden.

I. Ongestructureerde gegevensuitwisseling

In de huidige situatie worden gegevens veelal ongestructureerd uitgewisseld, bijvoorbeeld aan de hand van (beveiligde) email, fax en telefonisch. Ongestructureerde gegevens worden bijvoorbeeld uitgewisseld aan de hand van ZorgMail, beveiligde email waarbij gegevens worden beveiligd met kanaalversleuteling en in enkele gevallen ook met berichtversleuteling, wanneer systemen dat ondersteunen (S/MIME, PGP). Voor beveiligde email is de NTA 7516 norm ontwikkeld. Deze beschrijft de eisen waaraan email, met daarin patiëntgegevens, zou moeten voldoen om veilig te zijn.

II. Gegevensuitwisseling via een centrale voorziening

Gegevensuitwisseling vindt plaats door gebruik te maken van een centrale voorziening zoals een platform of schakelpunt dat gegevensuitwisseling rondom medicatieoverdracht regelt.

Zo wordt er grootschalig gebruikgemaakt van het Landelijk Schakelpunt (LSP), een zorginfrastructuur waar zorgaanbieders op kunnen aansluiten. Het LSP bevat enerzijds een verwijsindex die wordt gebruikt om te achterhalen waar de medicatiegegevens van een patiënt zich bevinden alvorens deze op te vragen. Anderzijds wordt het LSP ook gebruikt voor verwijzingen. Apothekers vragen bijvoorbeeld via het LSP actuele medische gegevens op of stellen deze beschikbaar als dit noodzakelijk is voor de behandeling van een patiënt. Daarnaast biedt het LSP ICA de mogelijkheid om de meeste actuele intoleranties, contra-indicaties en allergiegegevens op te vragen bij de huisarts of apotheker met wie de patiënt een behandelrelatie heeft. Wanneer gegevensuitwisseling via het LSP plaatsvindt dan wordt er van de zorgaanbieder tot het LSP en van het LSP tot de ontvangende zorgaanbieder kanaalversleuteling toegepast. Daarnaast verloopt de gegevensuitwisseling over een eigen netwerk, waar alleen partijen die voldoen aan de gestelde beveiligingseisen op mogen aansluiten. Dit is onder andere NEN7510 certificering en additionele AORTA eisen op bijvoorbeeld authenticatie. Deze manier van gegevensuitwisseling maakt onder andere gebruik van HL7 FHIR.

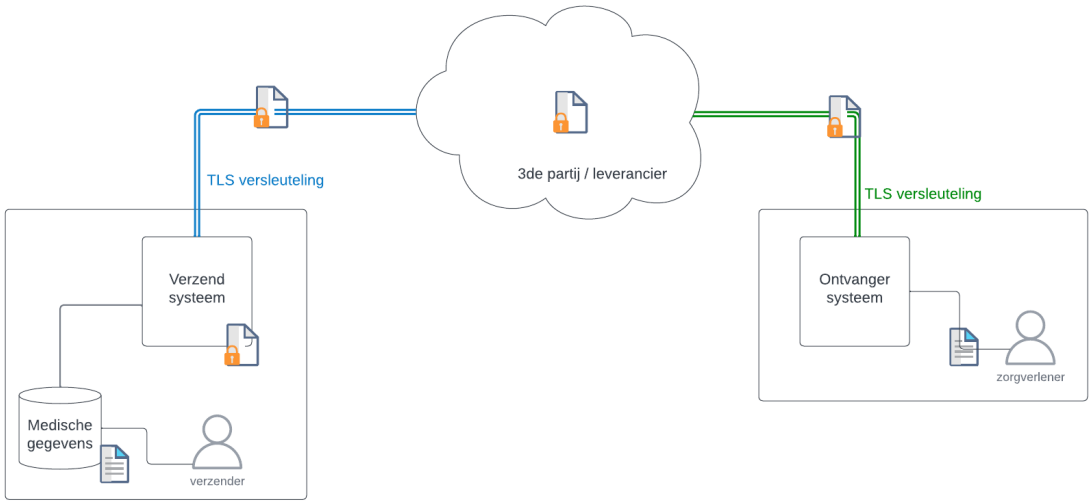
Gegevensuitwisseling vindt ook plaats door gebruik te maken van een centrale voorziening zoals een platform dat gegevensuitwisseling rondom medicatieoverdracht regelt. Een zogenoemde makelaars-applicatie. Zo wordt bijvoorbeeld het ZorgDomein gebruikt voor de medicatie-overdracht als onderdeel van een verwijzing van een patiënt door de huisarts naar een ziekenhuis. De gegevens worden vanuit het bronsysteem verstuurd naar het ZorgDomein waar deze worden gebundeld in een FHIR-document en vervolgens aangeboden worden bij het ontvangende systeem.

A.2. E2E-versleuteling voor medicatieoverdracht

E2E-versleuteling voor medicatieoverdracht wordt uitgewerkt aan de hand van twee scenario's. Binnen deze scenario's wordt een striktere (sectie 2.1: Scenario 1) en een iets flexibelere interpretatie (sectie 2.2: Scenario 2) van E2E-versleuteling gehanteerd. Elk van deze scenario's wordt uitgezet tegen de huidige manier van gegevensuitwisseling en vervolgens worden de technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden voor het scenario uitgewerkt.

A.2.1. Scenario 1: Een strikte interpretatie van E2E-versleuteling

De strikte interpretatie van E2E-versleuteling vereist dat de gegevensuitwisseling van verzendende systeem tot aan het ontvangende systeem versleuteld is, wat betekend dat eventuele tussenpartijen het bericht niet in kunnen zien. Binnen dit scenario zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen het versturende en ontvangende systeem inzicht hebben in de informatie die wordt uitgewisseld.



Figuur 8: Schematische weergave van strikte interpretatie van E2E-versleuteling

A.2.1.1. Scenario 1 in relatie tot de huidige situatie

I. Ongestructureerde gegevensuitwisseling

In de huidige situatie worden gegevens veelal uitgewisseld via onbeveiligde email en fax. Deze manier van gegevensuitwisseling voldoet niet standaard aan de vereisten van E2E-versleuteling en de Wegiz. Onder de Wegiz is de huidige manier van uitwisselen via fax niet langer geschikt wat vereist dat er alternatieve methoden geïmplementeerd dienen te worden. Om aan een vereiste tot E2E-versleuteling te voldoen voor email zijn aanpassingen noodzakelijk, zoals het versleutelen van het bericht met S/MIME of PGP. Er moet zorggedragen worden dat E2E-versleuteling plaatsvindt. Dit kan betekenen dat een zorginstelling zijn huidige infrastructuur met betrekking tot email volledig moet omgooien of over moet stappen op alternatieve methoden voor gegevensuitwisseling. Of voldoen aan de norm NTA 7516 ook betekent dat er voldaan wordt aan E2E-versleuteling is niet meegenomen in dit onderzoek.

II. Gecentraliseerde gegevensuitwisseling via een derde partij

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een derde partij die deze uitwisseling faciliteert door een translatieslag uit te voeren. Binnen Scenario 1 is het delen van gegevens via een dergelijke derde partij geen optie meer, omdat berichtversleuteling betekend dat er geen tussentijdse translatie plaats kan vinden. Dit betekent dan ook dat de huidige manier van uitwisselen niet langer geschikt zal zijn en er alternatieve methoden geïmplementeerd dienen te worden.

A.2.1.2. Gevolgen van Scenario 1 op de huidige manier van uitwisseling

Uitgaande van Scenario 1 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolg dat de huidige methoden voor gegevensuitwisseling niet langer mogelijk zijn. Zo kunnen gegevens niet meer uitgewisseld worden wanneer deze over een centrale voorziening lopen zoals het LSP of ZorgDomein, omdat hier geen berichtversleuteling op toegepast kan worden. Dit vereist dat alternatieve methoden voor gegevensuitwisseling dienen te worden gedefinieerd en geïmplementeerd.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste tot E2E-versleuteling te voldoen. Namelijk het encrypteren van berichten.
- De bestaande infrastructuur moet opnieuw ingericht worden.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning geboden moet worden.
- Kans op overbevraging van zorgaanbieders doordat het onduidelijk is waar gegevens zich bevinden (lokalisatie probleem).
- Overstappen op andere methoden van gegevensuitwisseling is een langdurend proces.
- Kleinere zorgaanbieders kunnen mogelijk niet mee met de verandering.

Financiële gevolgen:

- Kosten gerelateerd aan het implementeren van additionele maatregelen.
- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.

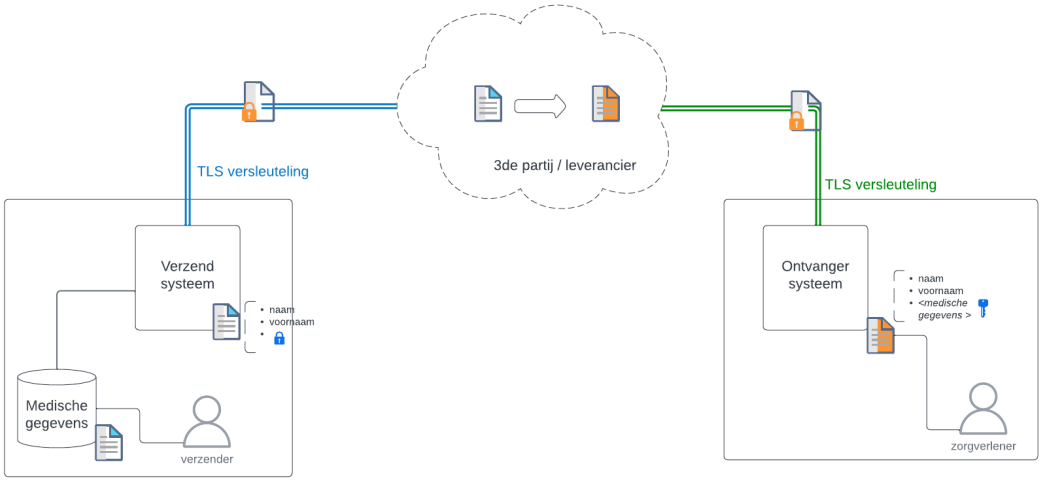
***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau waarbij de voordelen van E2E-beveiliging duidelijk moeten zijn én er uniformiteit over de verschillende gegevensuitwisselingen moet plaatsvinden.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Veranderingen moeten werkbaar en behapbaar blijven voor de verschillende partijen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

A.2.2. Scenario 2: Een flexibelere interpretatie van E2E-beveiliging

De flexibelere interpretatie van E2E-versleuteling vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er in plaats van versleuteling van het volledige bericht (berichtversleuteling) zoals bij Scenario 1, versleuteling binnen het bericht plaatsvindt (element versleuteling) waardoor de gevoelige (medische) informatie binnen het bericht versleuteld zijn. Daarnaast wordt kanaalversleuteling toegepast. Op de gegevenselementen kunnen dus ook nog bepaalde bewerkingen of mappings uitgevoerd worden, gezien de derde partij de metadata kan uitlezen. Hierdoor kan de derde partij het bericht eventueel in het juiste formaat en vorm zetten om vervolgens door te zenden naar de

ontvanger.



Figuur 9: Schematische weergave van de flexibele interpretatie van E2E-versleuteling

A.2.2.1. Scenario 2 in relatie tot de huidige situatie

I. Ongestructureerde gegevensuitwisseling

In de huidige situatie worden gegevens veelal uitgewisseld via (beveiligde) email en fax. Deze manier van gegevensuitwisseling voldoet niet standaard aan de vereisten van E2E-versleuteling en de Wegiz. Onder de Wegiz is de huidige manier van uitwisselen via fax niet langer geschikt wat vereist dat er alternatieve methoden geïmplementeerd dienen te worden. Om aan een vereiste tot E2E-versleuteling te voldoen voor email zijn aanpassingen noodzakelijk, zoals het versleutelen van het bericht met S/MIME of PGP. Er moet zorggedragen worden dat E2E-versleuteling plaatsvindt. Dit kan betekenen dat een zorginstelling zijn huidige infrastructuur met betrekking tot email volledig moet omgooien of over moet stappen op alternatieve methoden voor gegevensuitwisseling. Of voldoen aan de norm NTA 7516 ook betekent dat er voldaan wordt aan E2E-versleuteling is niet meegenomen in dit onderzoek.

II. Gecentraliseerde gegevensuitwisseling via een derde partij

Binnen Scenario 2 kunnen alleen de versturende en de ontvangen partij de (medische) gegevens zien die gedeeld worden. In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een derde partij die deze uitwisseling faciliteert door een translatieslag uit te voeren. Om aan de vereisten van E2E-beveiliging te voldoen betekent dit dat deze partij de inhoud van dit bericht niet mag zien. Echter is het voor de translatie noodzakelijk om het bericht te kunnen inzien, waardoor berichtversleuteling geen oplossing is (Scenario 1). De enige werkbare oplossing waarbij de huidige manier van uitwisselen kan blijven bestaan is door versleuteling toe te passen binnen het bericht zelf. Op deze manier is de derde partij nog wel in staat het format te identificeren, echter zijn de daadwerkelijke (medische) gegevens niet meer zichtbaar. Om aan een vereiste tot E2E-versleuteling te voldoen zijn aanpassingen noodzakelijk.

A.2.2.2. Gevolgen van Scenario 2 op de huidige manier van uitwisseling

Uitgaande van Scenario 2 heeft een vereiste tot E2E-beveiliging van gegevensuitwisseling tot gevolg dat een aantal grote aanpassingen gedaan moeten worden. Zo is de fax niet langer een optie en kunnen gegevens alleen uitgewisseld worden via een centrale voorziening zoals het LSP en het ZorgDomein wanneer er verdere standaardisatie van berichtdefinities plaatsvindt en additionele maatregelen worden geïmplementeerd. Daarnaast is het goed om te benadrukken dat zulke aanpassingen niet van de een op de andere dag doorgevoerd kunnen worden. Het proces van het verder standaardiseren van berichtdefinities gaat tijd en afstemming tussen verscheidene partijen vereisen. Hierbij is alleen nog onvoldoende bekend wat de praktische uitvoerbaarheid van dit scenario is, omdat er verder onderzoek gedaan moet worden naar de berichtdefinities en of die in voldoende mate te mappen zijn. Een complicerende factor is bijvoorbeeld het gegevenselement “naam”. Als deze opgeknipt moet worden naar “voornaam” en “achternaam” dan kan dat niet op de

versleutelde vorm. Hierover moeten dus afspraken gemaakt worden en de technische uitwerking geïmplementeerd worden.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- De bestaande infrastructuur moet opnieuw ingericht worden.
- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste tot E2E-versleuteling te voldoen.
- Berichtdefinities dienen geformaliseerd te worden.
- Versleuteling binnen de berichten aan de hand van de berichtdefinities dienen geïmplementeerd te worden.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Er dient afstemming plaats te vinden tussen verscheidene partijen met betrekking tot de berichtdefinities.
- Alle partijen dienen de geformaliseerde berichtdefinities over te nemen voor gegevensuitwisseling die via een derde partij loopt.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Overstappen op andere methoden van gegevensuitwisseling is een langdurend proces.
- Kleinere zorgaanbieders kunnen mogelijk niet mee met de verandering.

Financiële gevolgen:

- Kosten gerelateerd aan het implementeren van additionele maatregelen.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.
- Kosten gerelateerd aan het ontwikkelen van berichtdefinities.
- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau waarbij de voordelen van E2E-beveiliging duidelijk moeten zijn én er uniformiteit over de verschillende gegevensuitwisselingen moet plaatsvinden.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Veranderingen moeten werkbaar en behapbaar blijven voor de verschillende partijen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.
- Uniformiteit in zorgdossiers en terminologie.
- De methoden voor gegevensuitwisseling moeten in lijn blijven met internationale standaarden.

A.3. E2E-authenticatie

E2E-authenticatie kan op verscheidene manieren bewerkstelligd worden. De belangrijkste uitgangspunten daarbij zijn dat er onderling vertrouwen tussen IAM-oplossingen dient te zijn en dat de methode voor authenticatie eIDAS Hoog moeten classificeren, in verband met de gevoeligheid van de gegevens die uitgewisseld worden. Een voorbeeld van een inlogmiddel met een hoog betrouwbaarheidsniveau is de UZI-pas.

A.3.1.1. E2E-authenticatie in relatie tot de huidige situatie

In de huidige situatie vinden er verschillende manieren van authenticatie plaats. Echter, voldoen niet alle methoden van authenticatie op dit moment aan de eIDAS Hoog vereiste die vanuit het principe van E2E-authenticatie verwacht zou worden. De enige methode die op dit moment toegepast wordt en die conform betrouwbaarheidsniveau eIDAS Hoog classificeert is de UZI-pas. Deze methode van authenticatie wordt momenteel alleen toegepast voor gegevensuitwisseling via het LSP. Echter is tijdens de gesprekken vastgesteld dat deze methode niet altijd leidt tot de juiste toepassing in de praktijk. Zo is het niet voor alle zorgverleners mogelijk een UZI-pas te verkrijgen en is dit authenticatiemiddel erg kostbaar. Daarnaast wordt de huidige toepasbaarheid van de UZI-pas niet als gebruiksvriendelijk ervaren waardoor er soms naar workarounds binnen het authenticatie proces gezocht wordt.

A.3.1.2. Gevolgen van E2E-authenticatie op de huidige manier van uitwisseling

Een vereiste van E2E-authenticatie heeft tot gevolg dat een aantal methoden die momenteel toegepast worden ter authenticatie niet langer mogelijk zijn. Dit vereist dat in situaties waar deze methoden toegepast worden alternatieve methoden voor authenticatie dienen te worden gedefinieerd. Daarnaast zal het ook betekenen dat het aantal certificaten in aantallen zal toenemen.

Technische gevolgen:

- Alternatieve methoden voor authenticatie dienen gedefinieerd en geïmplementeerd te worden conform betrouwbaarheidsniveau eIDAS Hoog.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning geboden moet worden.
- Naast algemene kennis op informatiebeveiliging betekent dit dat er meer gespecialiseerde kennis nodig is op de concepten van sleutel- en certificaatbeheer. In de huidige situatie is deze al gesignaleerd als een beheer probleem.
- Definiëren van andere methoden voor authenticatie is een langdurend proces.
- Overstappen op andere methoden voor authenticatie is een langdurend proces.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor authenticatie.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van authenticatie die wel voldoet aan het vereiste van betrouwbaarheidsniveau eIDAS Hoog.
- Kosten gerelateerd aan het gebruik van systemen zoals de UZI-pas.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals, zoals niet steeds opnieuw in moeten loggen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

B. Analyse “Basisgegevensset Zorg (BgZ)”

B.1. Huidige status

De Basisgegevensset Zorg (hierna: BgZ) bevat een minimale set van patiëntgegevens die specialisme-, ziektebeeld- en beroepsgroep overstijgend relevant is en van belang is voor de continuïteit van de zorg. Het bevat onder andere administratieve gegevens (naam, adres, woonplaats), diagnose, medicatie en allergieën. De BgZ zorgt ervoor dat zorgverleners beschikken over adequate, actuele en uniforme gegevens over de patiënt op de juiste plek op het juiste moment en is afgeleid van en gebaseerd op de International Patient Summary (IPS) zoals die binnen de Europese Unie is vastgesteld. MSZ-instellingen zijn verplicht om hiervoor gebruik te maken van gecertificeerde ICT-producten en diensten, conform de Nen-norm 7540.

Momenteel vinden er twee typen gegevensuitwisseling plaats. Enerzijds worden gegevens verzonden aan de hand van een doorverwijzing. Daarnaast worden gegevens opgevraagd na toestemming van de patiënt. In de huidige situatie vinden er vier manieren van gegevenstuitwisseling plaats:

I. Gegevensuitwisseling via de email en fax:
In de huidige situatie worden gegevens veelal ongestructureerd uitgewisseld, bijvoorbeeld aan de hand van (beveiligde) email, fax en telefonisch.

II. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert:
In de huidige situatie zijn er ook methoden van uitwisseling die gefaciliteerd worden door een derde partij. Dit is een gemeenschappelijke ICT-voorziening die nodig is voor zorginstellingen om onderling gegevens uit te wisselen. Deze methode leent zich zowel voor gegevensuitwisseling met betrekking tot verwijzingen als voor het opvragen van gegevens en kan ook gegevens van verschillende standaarden uitwisselen door een translatie toe te passen. In de huidige situatie worden twee varianten gebruikt:

1. Gegevensuitwisseling via een centrale voorziening. Een centrale voorziening is een centraal schakelpunt waar uit te wisselen gegevens langs gaan. Zo wordt er voor uitwisseling met betrekking tot de BgZ gebruikgemaakt van het Landelijk Schakelpunt (LSP), een zorginfrastructuur waar zorgaanbieders op kunnen aansluiten. Het LSP bevat enerzijds een verwijsindex die wordt gebruikt om te achterhalen waar BgZ-gegevens van een patiënt zich bevinden alvorens deze op te vragen. Anderzijds wordt het LSP ook gebruikt voor verwijzing. Wanneer gegevensuitwisseling via het LSP plaatsvindt, dan wordt er van de zorgaanbieder tot het LSP en van het LSP tot de ontvangende zorgaanbieder kanaalversleuteling toegepast. Daarnaast verloopt de gegevensuitwisseling over een eigen netwerk, waar alleen partijen die voldoen aan de gestelde beveiligingseisen op mogen aansluiten. Dit is onder andere NEN7510 certificering en additionele AORTA-eisen op bijvoorbeeld authenticatie. Deze manier van gegevensuitwisseling maakt onder andere gebruik van HL7 FHIR.
2. Gegevensuitwisseling via een netwerk/platform-oplossing. Naast gegevensuitwisseling via een centrale voorziening kunnen gegevens ook uitgewisseld worden door aan te sluiten op een netwerk of platform-oplossing. Deze oplossingen worden veelal geïntegreerd in het EPD/ECD en maken het mogelijk om gegevens uit te wisselen met andere partijen die aangesloten zijn op dit platform. De uitwisselingen vanuit zo’n platform kunnen vervolgens zowel centraal als decentraal plaatsvinden. Een aantal voorbeelden van een dergelijke oplossing zijn de Zorgnetwerk Omgeving (ZNO) van Hinq, het Zorgplatform van Chipsoft en Care Everywhere van Epic.

III. Gegevensuitwisseling door middel van een gedistribueerd netwerkdirecte uitwisseling tussen zorgsystemen:
Gegevensuitwisseling die uitgevoerd wordt door directe uitwisseling tussen de zorgsystemen. Zorgaanbieders wisselen vanuit hun eigen bronsysteem rechtstreeks gegevens uit zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Deze methode leent zich voornamelijk voor gegevensuitwisseling met betrekking tot verwijzingen waarbij

eenzelfde standaard gebruikt wordt. Voor gegevensuitwisseling van de BgZ worden twee varianten gebruikt:

1. Gegevensuitwisseling op basis van de Nuts Standaarden. Zorgaanbieders kunnen aansluiten op het netwerk om zo onderling gegevens uit te wisselen. Deze methode voor gegevensuitwisseling is gebaseerd op de Nuts Standaarden, waar verschillende leveranciers voor de BgZ bij aangesloten zijn. Zo kunnen er bijvoorbeeld vanuit het Nexus EPD van Nexus-Nederland en het Medicore ECD van Tenzinger gegevens uitgewisseld worden met andere partijen uit het Nuts-netwerk.
2. Point-to-point oplossingen. Daarnaast vindt er ook gegevensuitwisseling plaats tussen de zorginstellingen die eenzelfde leverancier gebruiken. In dit geval kunnen gegevens direct uitgewisseld worden.

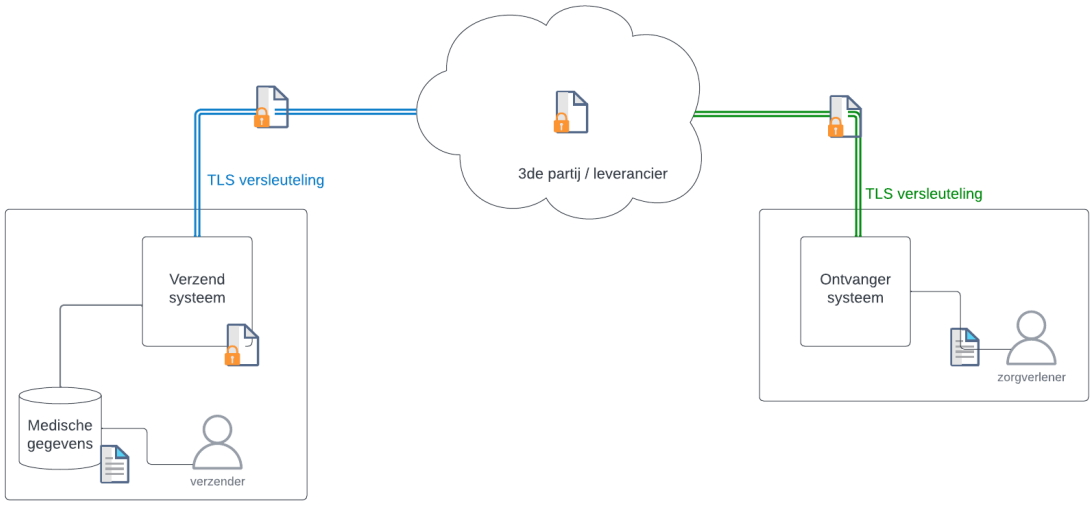
III. Gegevensuitwisseling door zorg professionals zelf:
Artsen die nul-urencontracten hebben bij meerdere instellingen kijken via een VPN in elkaars systemen om relevante informatie te bekijken. Omdat deze manier geen additionele methode van gegevensuitwisseling biedt wordt deze optie voor het vervolg van de analyse buiten beschouwing gelaten.

B.2. E2E-versleuteling voor de BgZ

E2E-versleuteling voor BgZ wordt uitgewerkt aan de hand van twee scenario's. Binnen deze scenario's wordt een striktere (sectie 2.1: Scenario 1) en een iets flexibelere interpretatie (sectie 2.2: Scenario 2) van E2E-versleuteling gehanteerd. Elk van deze scenario's wordt uitgezet tegen de huidige manier van gegevensuitwisseling en vervolgens worden de technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden voor het scenario uitgewerkt.

B.2.1. Scenario 1: Een strikte interpretatie van E2E-versleuteling

De strikte interpretatie van E2E-versleuteling vereist dat de gegevensuitwisseling van het verzendende systeem tot aan het ontvangende systeem versleuteld is, wat betekend dat eventuele tussenpartijen het bericht niet in kunnen zien. Binnen dit scenario zijn versleutelingsmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen het versturende en ontvangende systeem inzicht hebben in de informatie die wordt uitgewisseld.



Figuur 10: Schematische weergave van strikte interpretatie van E2E-versleuteling

B.2.1.1. Scenario 1 in relatie tot de huidige situatie

I. Gegevensuitwisseling via de email en fax
In de huidige situatie worden gegevens veelal uitgewisseld via onbeveiligde email en fax. Deze manier van gegevensuitwisseling voldoet niet standaard aan de vereisten van E2E-versleuteling

en de Wegiz. Onder de Wegiz is de huidige manier van uitwisselen via de fax niet langer geschikt wat vereist dat er alternatieve methoden geïmplementeerd dienen te worden. Om aan een vereiste tot E2E-versleuteling te voldoen voor email zijn aanpassingen noodzakelijk, zoals het versleutelen van het bericht met S/MIME of PGP. Er moet zorggedragen worden dat E2E-versleuteling plaatsvindt. Dit kan betekenen dat een zorginstelling zijn huidige infrastructuur met betrekking tot email volledig moet omgooien of over moet stappen op alternatieve methoden voor gegevensuitwisseling.

II. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert

Binnen Scenario 1 zijn versleutelingsmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een derde partij die deze uitwisseling faciliteert en een translatieslag uit voert. Binnen Scenario 1 is het delen van gegevens via een dergelijke derde partij geen optie meer, omdat berichtversleuteling betekent dat er geen tussentijdse translatie plaats kan vinden. Dit betekent dan ook dat in situaties waar een translatieslag uitgevoerd dient te worden, deze manier van uitwisselen niet langer geschikt zal zijn en er alternatieve methoden geïmplementeerd dienen te worden. Daarnaast komen er ook situaties voor waar wel berichtversleuteling wordt toegepast, echter gebeurt dit in die gevallen vaak door de derde partij zelf, dus geen E2E-berichtversleuteling. Deze manier van gegevensuitwisseling is niet mogelijk in Scenario 1 wat betekent dat aanpassingen noodzakelijk zijn om aan de vereisten van E2E-versleuteling te voldoen.

III. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.

Binnen Scenario 1 zijn versleutelingsmaatregelen verplicht, zoals bijvoorbeeld kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. Voor gegevensuitwisseling via een gedistribueerd netwerk worden de gegevens rechtstreeks vanuit het bronsysteem van de zorgaanbieder gecommuniceerd naar het bronsysteem van de ontvangende partij zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Daarnaast worden er versleutelingsmaatregelen genomen om te bewerkstelligen dat alleen de versturende en de ontvangende partij de gegevens in kunnen zien. Deze manier van uitwisseling voldoet aan de vereisten van E2E-versleuteling.

B.2.1.2. Gevolgen van Scenario 1 op de huidige manier van uitwisseling

Uitgaande van scenario 1 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolg dat een aantal methoden die momenteel toegepast worden om gegevens uit te wisselen niet langer mogelijk zijn. Zo is de fax niet langer een optie en kunnen gegevens ook niet meer uitgewisseld worden via een derde partij zoals het LSP, Zorgplatform of Care Everywhere, gezien deze systemen geen berichtversleuteling toepassen.

Dit betekent dan ook dat in de huidige situatie alleen verwijzingen kunnen plaatsvinden en dat de huidige manier voor het opvragen van BgZ-gegevens geen optie meer is. Dit resulteert in problemen voor routering en indexen omdat er geen centraal register is waar een zorgaanbieder kan achterhalen bij welke zorginstelling gegevens opgevraagd kunnen worden. Een gebrek aan zo'n register zal leiden tot overbevragen. Een ander gevolg is dat er geen translaties meer uitgevoerd kunnen worden door een derde partij. Wanneer de translatie niet meer uitgevoerd kan worden door een derde partij betekent dit dat ofwel translatie plaats moet vinden bij de bron, wat aanpassingen aan de bronsystemen vereist, ofwel dat er een uniforme standaard voor gegevens geïmplementeerd dient te worden.

De bestaande manieren van gegevensuitwisseling die voldoen aan het vereiste van E2E-versleuteling kunnen deze problemen niet oplossen, wat betekent dat in situaties waar deze methoden toegepast worden alternatieve methoden voor gegevensuitwisseling dienen te worden gedefinieerd. Daarnaast betekent Scenario 1 dat additionele beheersmaatregelen genomen moeten worden om de huidige manier van gegevensuitwisseling conform de vereiste van E2E-versleuteling te laten verlopen.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- Alternatieve oplossingen dienen ontwikkeld te worden voor het lokaliseren, routeren en indexeren van gegevens om overbevraging te voorkomen. Deze oplossingen dienen in lijn te zijn met de principes van E2E-beveiliging.
- Technische maatregelen dienen geïmplementeerd te worden om aan de vereisten tot E2E-versleuteling te voldoen. Namelijk het encrypteren van berichten.
- Aanpassingen aan bronsystemen om translatie bij de bron te bewerkstelligen of het implementeren van een uniforme standaard voor gegevens.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Kans op overbevraging van zorgaanbieders doordat het onduidelijk is waar gegevens zich bevinden (lokalisatie probleem).
- Overstappen op andere methode van gegevensuitwisseling is een langdurend proces.

Financiële gevolgen:

- Kosten gerelateerd aan het implementeren van additionele maatregelen.
- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.

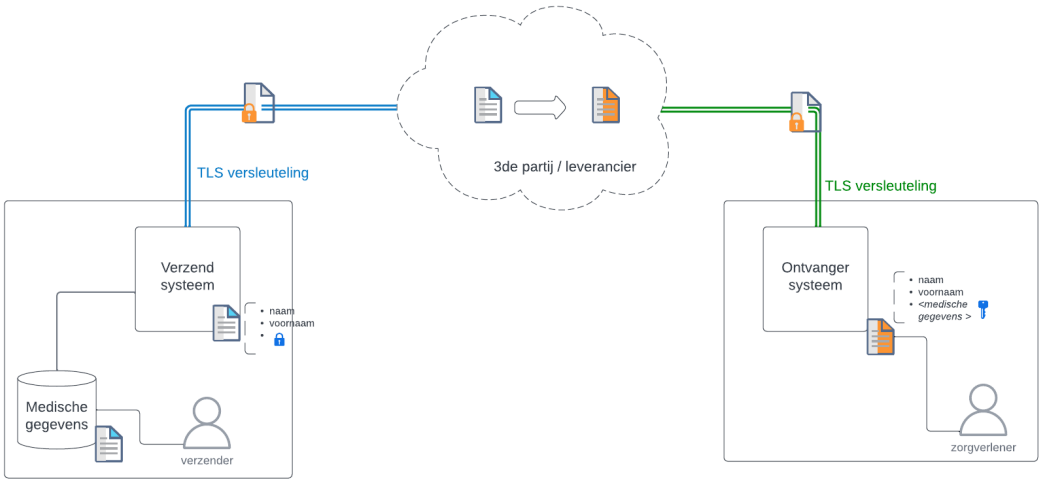
***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

B.2.2. Scenario 2: Een flexibelere interpretatie van E2E-beveiliging

De flexibelere interpretatie van E2E-versleuteling vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er in plaats van versleuteling van het volledige bericht (berichtversleuteling) zoals bij Scenario 1, versleuteling binnen het bericht plaatsvindt (element versleuteling) waardoor de gevoelige (medische) informatie binnen het bericht versleuteld zijn. Daarnaast wordt kanaalversleuteling toegepast. Op de gegevenselementen kunnen dus ook nog bepaalde bewerkingen of mappings op uitgevoerd worden, gezien de derde partij de metadata kan uitlezen. Hierdoor kan de derde partij het bericht eventueel in het juiste formaat en vorm zetten om vervolgens door te zenden naar de

ontvanger.



Figuur 11: Schematische weergave van de flexibele interpretatie van E2E-versleuteling

B.2.2.1. Scenario 2 in relatie tot de huidige situatie

I. Gegevensuitwisseling via de email en fax

In de huidige situatie worden gegevens veelal uitgewisseld via onbeveiligde email en fax. Deze manier van gegevensuitwisseling voldoet niet standaard aan de vereisten van E2E-versleuteling en de Wegiz. Onder de Wegiz is de huidige manier van uitwisselen via de fax niet langer geschikt wat vereist dat er alternatieve methoden geïmplementeerd dienen te worden. Om aan een vereiste tot E2E-versleuteling te voldoen voor email zijn aanpassingen noodzakelijk. Er moet zorggedragen worden dat E2E-versleuteling plaatsvindt. Dit kan betekenen dat een zorginstelling zijn huidige infrastructuur met betrekking tot email volledig moet omgooien of over moet stappen op een alternatieve methode voor gegevensuitwisseling.

II. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert

Binnen Scenario 2 kunnen alleen de versturende en de ontvangen partij de (medische) gegevens zien die gedeeld worden. In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een derde partij die deze uitwisseling faciliteert en een translatieslag uitvoert. Om aan de vereisten van E2E-beveiliging te voldoen betekent dit dat deze partij de inhoud van dit bericht niet mag zien. Echter is het voor de translatie noodzakelijk om het bericht te kunnen inzien, waardoor berichtversleuteling geen oplossing is (Scenario 1). De enige werkbare oplossing waarbij de huidige manier van uitwisselen kan blijven bestaan is door versleuteling toe te passen binnen het bericht zelf. Op deze manier is de derde partij nog wel in staat het format te identificeren, echter zijn de daadwerkelijke (medische) gegevens niet meer zichtbaar. Om aan een vereiste tot E2E-versleuteling te voldoen zijn aanpassingen noodzakelijk. Zo dienen er berichtdefinities geformaliseerd te worden zodat de translatie nog steeds uitgevoerd kan worden. Daarnaast moet E2E-versleuteling op elementniveau ingericht worden, wat betekent dat de zorgverlener zelf deze elementen dient te versleutelen alvorens deze beschikbaar worden gesteld aan de derde partij voor uitwisseling.

III. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.

Binnen Scenario 2 zijn versleutelingsmaatregelen verplicht, zoals bijvoorbeeld kanaal- en bericht of elementversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de medische gegevens die worden uitgewisseld. Voor gegevensuitwisseling via een gedistribueerd netwerk worden de gegevens rechtstreeks vanuit het bronsysteem van de zorgaanbieder gecommuniceerd naar het bronsysteem van de ontvangende zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Daarnaast worden er versleutelingsmaatregelen genomen om te bewerkstelligen dat alleen de versturende en de

ontvangende partij de gegevens in kunnen zien. Deze manier van uitwisseling voldoet aan de vereisten van E2E-versleuteling.

B.2.2.2. Gevolgen van Scenario 2 op de huidige manier van uitwisseling

Uitgaande van Scenario 2 heeft een vereiste tot E2E-beveiliging van gegevensuitwisseling tot gevolg dat een aantal grote aanpassingen gedaan moeten worden. Zo is de fax niet langer een optie en kunnen gegevens alleen uitgewisseld worden via een derde partij zoals het LSP, Zorgplatform of Care Everywhere, wanneer er verdere standaardisatie van berichtdefinities plaatsvindt en additionele maatregelen worden geïmplementeerd. Daarnaast is het goed om te benadrukken dat zulke aanpassingen niet van de een op de andere dag doorgevoerd kunnen worden. Het proces van het verder standaardiseren van berichtdefinities is ingewikkeld gaat tijd en afstemming tussen verscheidene partijen vereisen. Een belangrijke kanttekening daarbij is ook dat versleuteling op elementniveau tot gevolg heeft dat een translatie uitgevoerd kan worden. Echter valt ook te beargumenteren dat het hebben van een centrale index voor het lokaliseren van medische gegevens ook aan de principes van E2E-beveiliging zou moeten voldoen. Daarnaast betekent Scenario 2 dat additionele beheersmaatregelen genomen moeten worden om de huidige manier van gegevensuitwisseling conform de vereiste van E2E-versleuteling te laten verlopen.

Versleuteling op elementniveau is heel ingewikkeld. Het gaat jaren duren voordat je dat voor elkaar hebt. Dit is ook moeilijk voor bestaande systemen om te ondersteunen.

Technische gevolgen:

- Technische maatregelen dienen geïmplementeerd te worden om aan de vereisten tot E2E-versleuteling te voldoen.
- Berichtdefinities dienen geformaliseerd te worden.
- Versleuteling binnen de berichten aan de hand van de berichtdefinities dienen geïmplementeerd te worden.
- Alternatieve oplossingen dienen ontwikkeld te worden voor het lokaliseren, routeren en indexeren van gegevens in lijn met de principes van E2E-beveiliging.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Er dient afstemming plaats te vinden tussen verscheidene partijen met betrekking tot de berichtdefinities.
- Alle partijen dienen de geformaliseerde berichtdefinities over te nemen voor gegevensuitwisseling die via een derde partij loopt.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.

Financiële gevolgen:

- Kosten gerelateerd aan het implementeren van additionele maatregelen
- Kosten gerelateerd aan het ontwikkelen van berichtdefinities.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

B.3. Authenticatie

E2E-authenticatie kan op verscheidene manieren bewerkstelligd worden. De belangrijkste uitgangspunten daarbij zijn dat er onderling vertrouwen tussen IAM-oplossingen dient te zijn en dat de methode voor authenticatie eIDAS Hoog moeten classificeren, in verband met de gevoeligheid van de gegevens die uitgewisseld worden. Een voorbeeld van een inlogmiddel met een hoog betrouwbaarheidsniveau is de UZI-pas.

B.3.1. E2E-authenticatie in relatie tot de huidige situatie

In de huidige situatie vinden er verschillende manieren van authenticatie plaats. Echter, voldoen het merendeel van deze methoden van authenticatie op dit moment niet aan de eIDAS Hoog vereisten die vanuit het principe van E2E-authenticatie verwacht zou worden. De enige methode die op dit moment toegepast wordt en die conform betrouwbaarheidsniveau eIDAS Hoog classificeert is de UZI-pas. Echter is tijdens de gesprekken vastgesteld dat deze methode niet altijd leidt tot de juiste toepassing in de praktijk. Zo is het niet voor alle zorgverleners mogelijk een UZI-pas te verkrijgen en is dit authenticatiemiddel erg kostbaar. Daarnaast wordt de huidige toepasbaarheid van de UZI-pas niet als gebruiksvriendelijk ervaren waardoor er soms naar workarounds binnen het authenticatie proces gezocht wordt.

B.3.2. Gevolgen van E2E-authenticatie op de huidige manier van uitwisseling

Een vereiste van E2E-authenticatie heeft tot gevolg dat een aantal methoden die momenteel toegepast worden ter authenticatie niet langer mogelijk zijn. Dit vereist dat in situaties waar deze methoden toegepast worden alternatieve methoden voor authenticatie dienen te worden gedefinieerd.

Technische gevolgen:

- Alternatieve methoden voor authenticatie dienen gedefinieerd en geïmplementeerd te worden conform betrouwbaarheidsniveau eIDAS Hoog.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Definiëren van andere methode voor authenticatie is een langdurend proces.
- Overstappen op andere methode voor authenticatie is een langdurend proces.
- Mogelijke hinder voor gegevensuitwisselingen die momenteel geautomatiseerd verlopen.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor authenticatie.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van authenticatie die wel voldoet aan het vereiste van betrouwbaarheidsniveau eIDAS Hoog.
- Kosten gerelateerd aan het gebruik van systemen zoals de UZI-pas.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals, zoals niet steeds opnieuw in moeten loggen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

B.4. Conclusie

Een verplichting tot E2E-beveiliging kan resulteren in een hogere mate van informatiebeveiliging waarbij alleen de verzendende en ontvangende partij inzicht hebben in de gedeelde gegevens. Echter, vereist een dergelijke verplichting grote aanpassingen aan de manier waarop gegevens op dit moment gedeeld worden en de methode waarop zorgverleners zich kunnen authenticeren. Het

voldoen aan deze vereisten zal structurele aanpassingen vereisen van gegevensuitwisseling binnen de BgZ. Het is daarbij van belang om de afweging te maken of de toegenomen mate aan informatiebeveiliging van de gedeelde gegevens onder de vereisten tot E2E-beveiliging in deze context opwegen tegen de gevolgen.

C. Analyse “Beeldbeschikbaarheid”

C.1. Huidige status

Beeldbeschikbaarheid bevat de uitwisseling van beeldvormende diagnostiek (zoals röntgenfoto’s, MRI, echo, CT, mammografie) en de bijhorende verslagen daarvan. Bij gegevensuitwisseling wordt altijd de combinatie van het beeld en het bijbehorende verslag gedeeld. De beelden voldoen aan de wereldwijde DICOM-standaard waarbij verslagen gestructureerd of ongestructureerd kunnen zijn. Daarnaast verplicht het AMvB instellingen en zorgverleners binnen de medisch specialistische zorg om bij de uitwisseling van beelden alleen gebruik te maken van gecertificeerde beeldmanagementsystemen (voldoen aan de NEN-norm). In de huidige situatie vinden er twee manieren van gegevenstuitwisseling plaats:

I. Gegevensuitwisseling via CD en DVD
In de huidige situatie vindt een deel van de gegevensuitwisseling met betrekking tot beeldbeschikbaarheid plaats door beelden en verslagen te delen via CD’s en DVD’s.

II. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert:
In de huidige situatie wordt er veelal geleund op gegevensuitwisseling via een derde partij, zoals het Twiin portaal (VZVZ) en EVOCS. Deze derde partijen leveren een netwerk/platform-oplossing om beelduitwisseling te faciliteren. In de huidige situatie worden deze oplossingen voornamelijk gebruikt voor het delen van beelden als onderdeel van een verwijzing. Daarnaast verschillen deze oplossingen in de mate waarin ze geïntegreerd zijn met de PACS van de zorginstelling. Een drietal oplossingen uit de huidige situatie worden hieronder verder toegelicht.

1. Gegevensuitwisseling via het Twiin portaal in de browser. In deze situatie vindt er tijdelijke centrale dataopslag plaats binnen het Twiin portaal, gehost door Twiin. Het Twiin Portaal wordt gebruikt via de webbrowser voor het uploaden en downloaden van beelden en verslagen. Er is geen integratie met het eigen PACS-systeem. Daarnaast bevat het portaal de mogelijkheid om verslagen te converteren naar het gewenste format.
2. Gegevensuitwisseling via een lokale gateway van het Twiin portaal. Het Twiin portaal is geïntegreerd in het PACS. In deze situatie vindt er decentrale dataopslag plaats, lokaal binnen de eigen instelling. Hierdoor kan het proces van het versturen van beelden op de gateway plaatsvinden. Voor de communicatie wordt gebruikgemaakt van de internationale IHE XDM standaard, de DICOM Mail standaarden en versleuteling op basis van PGP. Ook het adresboek staat decentraal op de gateways en wordt regelmatig gesynchroniseerd. Daarnaast bevat Gateway de mogelijkheid om verslagen te converteren naar het gewenste format.
3. Gegevensuitwisseling via de EVOCS webapplicatie. De EVOCS webapplicatie ontsluit patiëntdata vanuit verschillende informatiebronnen, zoals PACS en ZIS en integreert ze met (DICOM-)modaliteiten. Voor de communicatie wordt gebruikgemaakt van de internationale IHE HL7 en DICOM-standaarden.

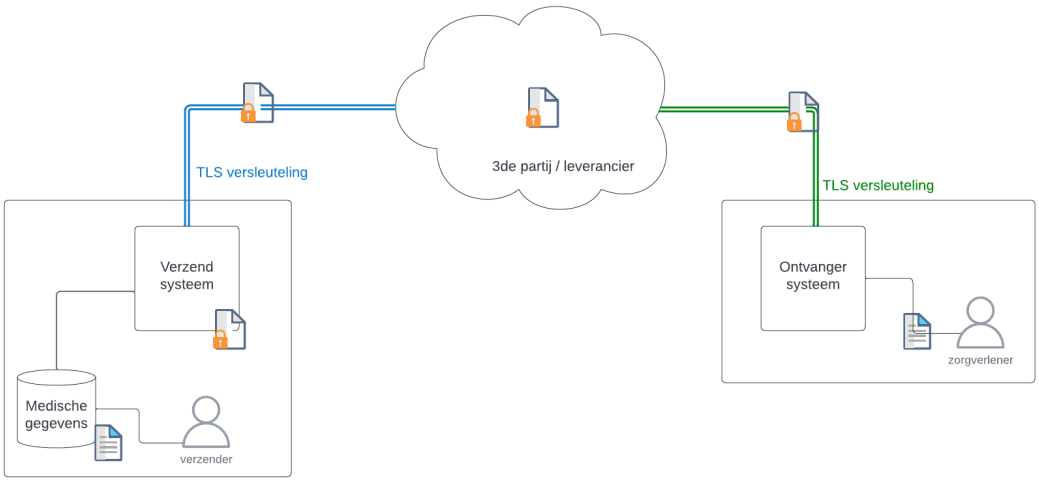
C.2. E2E-versleuteling voor beeldbeschikbaarheid

E2E-versleuteling voor beeldbeschikbaarheid wordt uitgewerkt aan de hand van twee scenario’s. Binnen deze scenario’s wordt een striktere (sectie 2.1: Scenario 1) en een iets flexibelere interpretatie (sectie 2.2: Scenario 2) van E2E-versleuteling gehanteerd. Elk van deze scenario’s wordt uitgezet tegen de huidige manier van gegevensuitwisseling en vervolgens worden de technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden voor het scenario uitgewerkt.

C.2.1. Scenario 1: Een strikte interpretatie van E2E-versleuteling

De strikte interpretatie van E2E-versleuteling vereist dat de gegevensuitwisseling van verzendende systeem tot aan het ontvangende systeem versleuteld is, wat betekend dat eventuele tussenpartijen het bericht niet in kunnen zien. Binnen dit scenario zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen het versturende en ontvangende

systeem inzicht hebben in de informatie die wordt uitgewisseld.



Figuur 12: Schematische weergave van de strikte interpretatie van E2E-versleuteling

C.2.1.1. Scenario 1 in relatie tot de huidige situatie

Binnen Scenario 1 zijn versleutelingsmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. In de huidige situatie zijn er twee manieren van gegevensuitwisseling: gegevensuitwisseling middels DVD en CD en gegevensuitwisseling die gefaciliteerd wordt door een derde partij.

I. Gegevensuitwisseling via CD en DVD

In de huidige situatie vindt een deel van de gegevensuitwisseling met betrekking tot beeldbeschikbaarheid plaats door beelden en verslagen te delen via CD's en DVD's. Deze manier van gegevensuitwisseling voldoet niet standaard aan de vereisten van E2E-versleuteling en de Wegiz. Onder de Wegiz is de huidige manier van uitwisselen via CD en DVD niet langer geschikt wat vereist dat er alternatieve methoden geïmplementeerd dienen te worden.

II. Gegevensuitwisseling via een derde partij die de uitwisseling faciliteert

In de huidige situatie wordt er veelal geleund op gegevensuitwisseling via een derde partij, zoals het Twiin portaal (VZVZ) en EVOCS. Deze derde partijen leveren een netwerk/platform-oplossing om beelduitwisseling te faciliteren en indien nodig een translatieslag uit te voeren.

Veelal wordt er gebruikgemaakt van een portaal in de browser. Binnen Scenario 1 is het delen van gegevens via een dergelijke derde partij veelal geen optie meer, omdat berichtversleuteling betekent dat er geen tussentijdse translatie plaats kan vinden. Dit betekent dan ook dat in situaties waar een tussentijdse translatieslag uitgevoerd dient te worden, deze manier van uitwisselen niet langer geschikt zal zijn en er alternatieve methoden geïmplementeerd dienen te worden. Daarnaast komen er ook situaties voor waar wel berichtversleuteling wordt toegepast, echter gebeurt dit in die gevallen vaak door de derde partij zelf (geen E2E-berichtversleuteling), zoals bij het gebruik van een portaal in de browser. Deze manier van gegevensuitwisseling is niet mogelijk in scenario 1 wat betekent dat aanpassingen noodzakelijk zijn om aan deze vereisten van E2E-versleuteling te voldoen. Daarnaast is er een tweede reden waarom gegevensuitwisseling middels een applicatie in de browser veelal niet uitvoerbaar is onder een verplichting tot E2E-versleuteling. Indien de ontvangende organisatie zelf geen bronsysteem heeft waar de gegevens ontvangen in kunnen worden is er geen spraken van een "end" bij de ontvangende zorginstelling. Om die reden is een dergelijke use case niet langer geschikt.

Er zijn ook situaties waarbij het portaal volledig geïntegreerd is met de PACS van de zorginstelling waardoor de gegevens decentraal opgeslagen zijn, zoals bij de Twiin Portaal Gateway. In deze situatie vindt de translatie in de gateway zelf plaats alvorens het verzenden. Voor verzending wordt er op berichtniveau versleuteling toegepast op basis van de sleutel van de ontvanger (PGP).

Wanneer de gegevensuitwisseling van een gateway bij de zorginstelling naar een gateway van een andere zorginstelling loopt is er sprake van E2E-versleuteling. Deze manier van gegevensuitwisseling voldoet aan de vereisten. Echter, indien een van de zorgaanbieders geen gebruik maakt van de gateway, maar in plaats daarvan het Twiin portaal in de browser hanteert, is er geen sprake meer van E2E-versleuteling, zoals reeds hierboven toegelicht.

C.2.1.2. Gevolgen van Scenario 1 op de huidige manier van uitwisseling

Uitgaande van Scenario 1 heeft een vereiste tot E2E-beveiliging van gegevensuitwisseling tot gevolg dat gegevensuitwisseling die door een derde partij gefaciliteerd worden vaak niet langer een optie zijn omdat er geen E2E-berichtversleuteling kan worden toegepast. Dit vereist dat in dergelijke situaties alternatieve methoden voor gegevensuitwisseling dienen te worden gedefinieerd en geïmplementeerd.

Zo kan er wanneer er E2E-berichtversleuteling moet plaatsvinden geen translatie meer uitgevoerd worden, wat betekent dat zorginstellingen die verschillende type beelden hanteren deze niet meer kunnen uitwisselen. Wanneer de translatie niet meer uitgevoerd kan worden door een derde partij betekent dit dat ofwel translatie plaats moet vinden bij de bron, wat aanpassingen aan de bronsystemen vereist, ofwel dat er een uniforme standaard voor gegevens geïmplementeerd dient te worden.

Een tweede gevolg is dat wanneer gegevensuitwisselingen via een portaal in de browser lopen een aantal bestaande use cases niet meer uitgevoerd kunnen worden. Zoals reeds toegelicht worden er ook beelden gedeeld met zorginstellingen die niet een eigen bronsysteem hebben zoals een PACS en dus niet beschikken over een eigen “end”. Deze zorgverleners zijn dus afhankelijk van een derde partij om de beelden te kunnen zien. Onder het vereiste van E2E-versleuteling is deze usecase niet mogelijk meer. Een oplossing zou zijn om alle zorginstellingen die beelden moeten kunnen inzien een PACS te laten aanschaffen, echter dit is zeker voor de kleinere instellingen een erg dure en onpraktische oplossing.

Voor situaties waarbij er gebruik wordt gemaakt van een in de PACS geïntegreerde gateway met decentrale opslag en berichtversleuteling op basis van PGP zijn geen additionele maatregelen nodig. Dit kan gezien worden als een situatie waar E2E-versleuteling plaatsvindt.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- Aanpassingen aan bronsystemen om translatie bij de bron te bewerkstelligen of het implementeren van een uniforme standaard voor gegevens.
- PACS-systemen dienen eventueel aangepast te worden om versleuteling van de beelden zelf – aan de bron – te voorzien.
- Sleutelbeheer moet ingericht worden.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Beelden kunnen alleen nog gedeeld worden met zorginstellingen die een eigen PACS hebben.
- Overstappen op andere methode van gegevensuitwisseling is een langdurend proces.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.

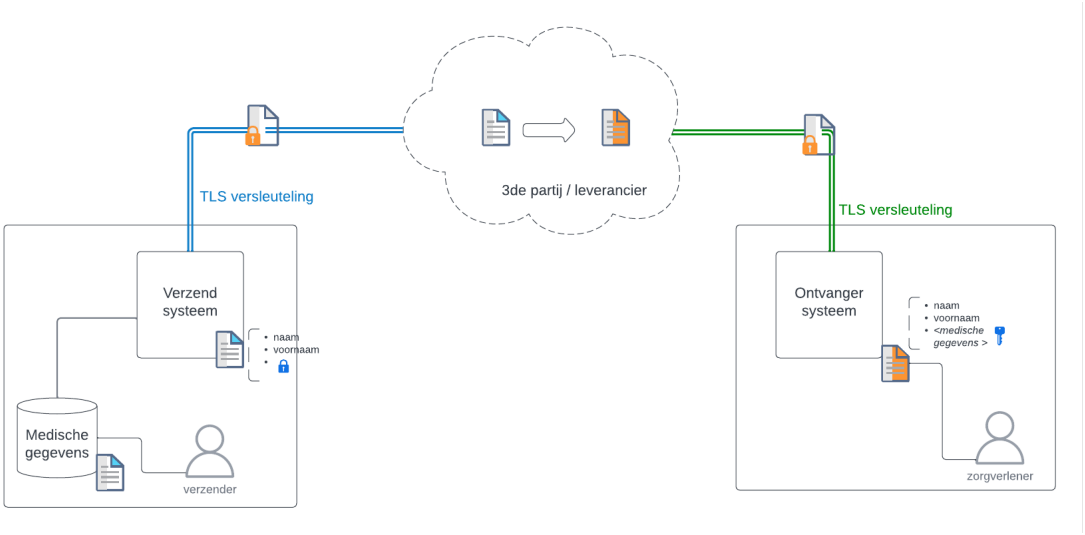
- Kosten gerelateerd aan het aanschaffen van een PACS voor zorginstellingen die momenteel geen eigen PACS hebben maar wel beelden moeten inzien om zorg te leveren.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals. Integratie in huidige systemen is noodzakelijk.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

C.2.2. Scenario 2: Een flexibelere interpretatie van E2E-versleuteling

De flexibelere interpretatie van E2E-versleuteling vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er in plaats van versleuteling van het volledige bericht (berichtversleuteling) zoals bij Scenario 1, versleuteling binnen het bericht plaatsvindt (element versleuteling) waardoor de gevoelige (medische) informatie binnen het bericht versleuteld zijn. Daarnaast wordt kanaalversleuteling toegepast. Op de gegevenselementen kunnen dus ook nog bepaalde bewerkingen of mappings op uitgevoerd worden, gezien de derde partij de metadata kan uitlezen. Hierdoor kan de derde partij het bericht eventueel in het juiste formaat en vorm zetten om vervolgens door te zenden naar de ontvanger.



Figuur 13: Schematische weergave van de flexibele interpretatie van E2E-versleuteling

C.2.2.1. Scenario 2 in relatie tot de huidige situatie

In de huidige situatie wordt er veelal geleund op gegevensuitwisseling via een derde partij, zoals het Twiin portaal (VZVZ) en EVOCS. Deze derde partijen leveren een netwerk/platform-oplossing om beeldduitwisseling te faciliteren en indien nodig een translatieslag uit te voeren.

Scenario 2 vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er bijvoorbeeld in plaats van versleuteling van het volledige bericht (berichtversleuteling) versleuteling binnen het bericht plaatsvindt (element versleuteling). De gevoelige (medische) informatie binnen het bericht zijn dan versleuteld naast de kanaal versleuteling die toegepast wordt wanneer het bericht verstuurd wordt. Echter is het niet mogelijk om in de context van beeldduitwisseling elementversleuteling toe te passen. Om deze reden zal ook uitgaande van Scenario 2 alleen berichtversleuteling een optie zijn. Dit betekent dus ook dat de relatie tot de huidige situatie en de gevolgen identiek zijn aan de uitwerkingen van Scenario 1.

C.2.2.2. Gevolgen van Scenario 2 op de huidige manier van uitwisseling

Uitgaande van Scenario 1 heeft een vereiste tot E2E-beveiliging van gegevensuitwisseling tot gevolg dat gegevensuitwisseling die door een derde partij gefaciliteerd worden vaak niet langer een optie zijn omdat er geen E2E-berichtversleuteling kan worden toegepast. Dit vereist dat in dergelijke situaties alternatieve methoden voor gegevensuitwisseling dienen te worden gedefinieerd en geïmplementeerd.

Zo kan er wanneer er E2E-berichtversleuteling moet plaatsvinden geen translatie meer uitgevoerd worden, wat betekent dat zorginstellingen die verschillende type beelden hanteren deze niet meer kunnen uitwisselen. Wanneer de translatie niet meer uitgevoerd kan worden door een derde partij betekent dit dat ofwel translatie plaats moet vinden bij de bron, wat aanpassingen aan de bronsystemen vereist, ofwel dat er een uniforme standaard voor gegevens geïmplementeerd dient te worden.

Een tweede gevolg is dat wanneer gegevensuitwisselingen via een portaal in de browser lopen een aantal bestaande use cases niet meer uitgevoerd kunnen worden. Zoals reeds toegelicht worden er ook beelden gedeeld met zorginstellingen die niet een eigen bronsysteem hebben zoals een PACS en dus niet beschikken over een eigen “end”. Deze zorgverleners zijn dus afhankelijk van een derde partij om de beelden te kunnen zien. Onder het vereiste van een E2E-versleuteling is deze usecase niet mogelijk meer. Een oplossing zou zijn om alle zorginstellingen die beelden moeten kunnen inzien een PACS te laten aanschaffen, echter dit is zeker voor de kleinere instellingen een erg dure en onpraktische oplossing.

Voor situaties waarbij er gebruik wordt gemaakt van een in de PACS geïntegreerde gateway met decentrale opslag en berichtversleuteling op basis van PGP zijn geen additionele maatregelen nodig. Dit kan gezien worden als een situatie waar E2E-versleuteling plaatsvindt.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- Aanpassingen aan bronsystemen om translatie bij de bron te bewerkstelligen of het implementeren van een uniforme standaard voor gegevens.
- PACS-systemen dienen eventueel aangepast te worden om versleuteling van de beelden zelf – aan de bron – te voorzien.
- Sleutelbeheer moet ingericht worden.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Beelden kunnen alleen nog gedeeld worden met zorginstellingen die een eigen PACS hebben.
- Overstappen op een andere methode van gegevensuitwisseling is een langdurend proces.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.
- Kosten gerelateerd aan het aanschaffen van een PACS voor zorginstellingen die momenteel geen eigen PACS hebben maar wel beelden moeten inzien om zorg te leveren.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.

- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals. Integratie in huidige systemen is noodzakelijk.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

C.3. E2E-authenticatie voor beeldbeschikbaarheid

E2E-authenticatie kan op verscheidene manieren bewerkstelligd worden. De belangrijkste uitgangspunten daarbij zijn dat er onderling vertrouwen tussen IAM-oplossingen dient te zijn en dat de methode voor authenticatie eIDAS Hoog moeten classificeren, in verband met de gevoeligheid van de gegevens die uitgewisseld worden. Een voorbeeld van een inlogmiddel met een hoog betrouwbaarheidsniveau is de UZI-pas.

C.3.1.1. E2E-authenticatie in relatie tot de huidige situatie

In de huidige situatie vindt er authenticatie plaats door middel van 2-factor authenticatie. Echter, voldoet deze methode van authenticatie niet aan de eIDAS Hoog vereiste die vanuit het principe van E2E-authenticatie verwacht zou worden. Daarnaast worden er momenteel ook beelden automatisch opgehaald gedurende de nacht. Indien een vereiste tot E2E-authenticatie wordt doorgevoerd is dit proces niet langer mogelijk.

C.3.1.2. Gevolgen van E2E-authenticatie op de huidige manier van uitwisseling

Een vereiste van E2E-authenticatie heeft tot gevolg dat de huidige manier van authenticatie niet langer mogelijk zijn. Dit vereist dat alternatieve methoden voor authenticatie dienen te worden gedefinieerd en geïmplementeerd.

Technische gevolgen:

- Alternatieve methoden voor authenticatie dienen gedefinieerd en geïmplementeerd te worden conform betrouwbaarheidsniveau eIDAS Hoog.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Definiëren van andere methoden voor authenticatie is een langdurend proces.
- Overstappen op andere methoden voor authenticatie is een langdurend proces.
- Geautomatiseerd ophalen van beelden is niet langer mogelijk.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor authenticatie.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van authenticatie die wel voldoet aan het vereiste van betrouwbaarheidsniveau eIDAS Hoog.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals, zoals niet steeds opnieuw in moeten loggen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

C.4. Conclusie

Een verplichting tot E2E-beveiliging kan resulteren in een hogere mate van informatiebeveiliging waarbij alleen de verzendende en ontvangende partij inzicht hebben in de gedeelde gegevens. Echter, vereist een dergelijke verplichting aanpassingen aan de manier waarop gegevens op dit

moment gedeeld worden. Daarnaast vereist een verplichting tot E2E-beveiliging grote aanpassingen in de methode waarop zorgverleners zich kunnen authenticeren. Het is daarbij van belang om de afweging te maken of de toegenomen mate aan informatiebeveiliging van de gedeelde gegevens onder een vereisten tot E2E-beveiliging in deze context opwegen tegen de gevolgen.

D. Analyse “Verpleegkundige overdracht (eOverdracht)”

D.1. Huidige status

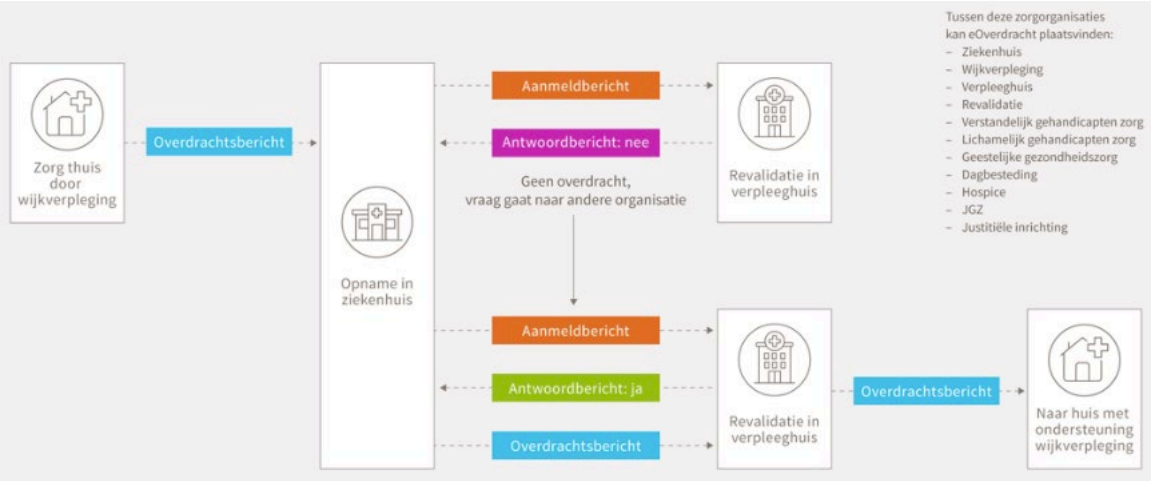
Verpleegkundige overdracht omvat de verplaatsing van de gegevens (verpleegkundig dossier) van een patiënt of cliënt naar een andere zorgverlener. Het gaat hierbij onder andere over administratieve gegevens, informatie over de achtergrond van de patiënt, medische informatie, het zorgplan en de gezondheidstoestand van de patiënt/cliënt.

In de context van elektronische gegevensuitwisseling wordt er bij verpleegkundige overdracht gesproken van de eOverdracht. De eOverdracht is een informatiestandaard gericht op de eenduidige en volledige overdracht van verpleegkundige patiëntgegevens. Deze informatiestandaard faciliteert de veilige, gestandaardiseerde, gestructureerde en geautomatiseerde overdracht van informatie tussen verpleegkundigen/verzorgenden op basis van zorginformatiebouwstenen (hierna: zibs) van bron naar bron.

In de praktijk vinden er als onderdeel van de verpleegkundige overdracht vier informatiestromen plaats:

- Overdracht van thuiszorg naar ziekenhuis
- Aanmelding en overdracht van ziekenhuis naar revalidatie of verpleeghuis
- Overdracht van revalidatie of verpleeghuis naar thuiszorg
- Opname van verpleeghuis naar ziekenhuis

De eOverdracht wordt momenteel nog niet in al deze informatiestromen gehanteerd omdat er veel sprake is van overdracht van ongestructureerde informatie, zoals telefonisch of door het opsturen van pdf’s. Daarnaast is er ook nog sprake van een papierenoverdracht. Momenteel wordt pas een beperkt deel van de zibs uitgevoerd.



Figuur 14 – overzicht van gegevensuitwisselingen bij eOvedracht. bron: Nictiz

Op dit moment vindt gegevensuitwisseling plaats langs 3 stromen:

- Ongestructureerde gegevensuitwisseling.
- Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.
- Gegevensuitwisseling via een broker.

Deze drie stromen worden hieronder kort toegelicht aan de hand van enkele voorbeelden:

I. Ongestructureerde gegevensuitwisseling

In de huidige situatie worden gegevens veelal ongestructureerd uitgewisseld, bijvoorbeeld aan de hand van (beveiligde) email, fax en telefonisch. Ongestructureerde gegevens worden bijvoorbeeld uitgewisseld aan de hand van ZorgMail, een beveiligde email waarbij gegevens worden beveiligd

met kanaalversleuteling en in enkele gevallen ook met berichtversleuteling, wanneer systemen dat ondersteunen (S/MIME, PGP).

II. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.
Gegevensuitwisseling die uitgevoerd wordt door directe uitwisseling tussen de zorgsystemen. Zorgaanbieders kunnen aansluiten op het netwerk om zo onderling gegevens uit te wisselen. Vanuit hun eigen systeem kunnen zorgaanbieders rechtstreeks met elkaar communiceren zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Deze methode voor gegevensuitwisseling is gebaseerd op de Nuts Standaarden, waar verschillende leveranciers voor de verpleegkundige overdracht bij aangesloten zijn. Zo kunnen er bijvoorbeeld vanuit het Ons elektronisch cliënten dossier (ECD van Nedap) gegevens uitgewisseld worden met andere partijen uit het Nuts-netwerk.

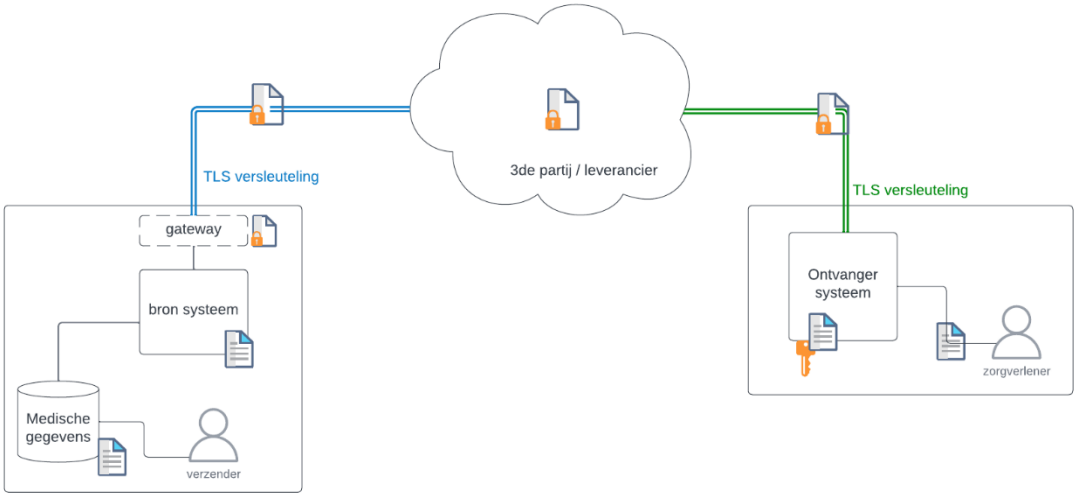
III. Gegevensuitwisseling via een broker
Gegevensuitwisseling vindt plaats door gebruik te maken van een broker zoals een platform dat gegevensuitwisseling rondom de verpleegkundige overdracht regelt. Een zogenoemde makelaars-applicatie. Zo wordt bijvoorbeeld de Transfer oplossing van het ZorgDomein gebruikt voor de overdracht van gegevens over een patiënt vanuit een ziekenhuis dat werkt met HiX (Chipsoft) naar een Verpleeg-, Verzorgingshuizen en Thuiszorg (VVT)-instelling. De gegevens worden vanuit het bronsysteem verstuurd naar het ZorgDomein waar deze worden gebundeld in een FHIR-document en vervolgens aangeboden worden bij het ontvangende systeem. Daarnaast wordt het ZorgDomein gebruikt om de aanmelding van de patiënt te coördineren met andere zorgaanbieders. ZorgDomein slaat in sommige gevallen ook de gegevens van patiënten op. Eenzelfde soort functionaliteit heeft het platform POINT. Dit platform wordt gebruikt voor de samenwerking rondom het transferproces van de patiënt. POINT biedt continu inzicht in de transferstatus, met een up-to-date transferdossier dat voldoet aan de landelijke normen. Ook hier worden zibs uitgewisseld op basis van de HL7 FHIR standaard. Hierbij moet opgemerkt worden POINT en ZorgDomein ook geïmplementeerd kan worden als in een gedistribueerd netwerk. Hierbij gaan de gegevens direct van bronsysteem tot ontvangende systeem zonder tussenkomst van een broker.

D.2. E2E-versleuteling voor verpleegkundige overdracht

E2E-versleuteling voor de verpleegkundige overdracht wordt uitgewerkt aan de hand van twee scenario's. Binnen deze scenario's wordt een striktere (sectie 2.1: Scenario 1) en een iets flexibelere interpretatie (sectie 2.2: Scenario 2) van E2E-versleuteling gehanteerd. Elk van deze scenario's wordt uitgezet tegen de huidige manier van gegevensuitwisseling en vervolgens worden de technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden voor het scenario uitgewerkt.

D.2.1. Scenario 1: Een strikte interpretatie van E2E-versleuteling

De strikte interpretatie van E2E-versleuteling vereist dat de gegevensuitwisseling van het verzendende systeem tot aan het ontvangende systeem versleuteld is, wat betekend dat eventuele tussenpartijen het bericht niet in kunnen zien. Binnen dit scenario zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen het versturende en ontvangende systeem inzicht hebben in de informatie die wordt uitgewisseld.



Figuur 15: Schematische weergave van de strikte interpretatie van E2E-versleuteling

D.2.1.1. Scenario 1 in relatie tot de huidige situatie

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld.

I. Gegevensuitwisseling via de email en fax

In de huidige situatie worden gegevens veelal uitgewisseld via (beveiligde) email en fax. Deze manier van gegevensuitwisseling voldoet niet standaard aan de vereisten van E2E-versleuteling en de Wegiz. Onder de Wegiz is de huidige manier van uitwisselen via de fax niet langer geschikt wat vereist dat er alternatieve methoden geïmplementeerd dienen te worden. Om aan een vereiste tot E2E-versleuteling te voldoen voor email zijn aanpassingen noodzakelijk, zoals het versleutelen van het bericht met S/MIME of PGP. Er moet zorggedragen worden dat E2E-versleuteling plaatsvindt. Dit kan betekenen dat een zorginstelling zijn huidige infrastructuur met betrekking tot email volledig moet omgooien of over moet stappen op alternatieve methode voor gegevensuitwisseling.

II. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals bijvoorbeeld kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. Voor gegevensuitwisseling via een gedistribueerd netwerk worden de gegevens rechtstreeks vanuit het systeem van de zorgaanbieder gecommuniceerd naar het systeem van de ontvangende zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Daarnaast worden er versleutelingmaatregelen genomen om te bewerkstelligen dat alleen de versturende en de ontvangende partij de gegevens in kunnen zien. Deze manier van uitwisseling voldoet aan de vereisten van E2E-versleuteling.

III. Gegevensuitwisseling via een broker

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. In de huidige situatie worden gegevens uitgewisseld door gebruik te maken van een broker dat deze uitwisseling faciliteert, zoals ZorgDomein en POINT. Alhoewel er wel kanaalversleuteling wordt toegepast vindt er geen berichtversleuteling plaats. ZorgDomein, in deze configuratie, dient namelijk de gegevens nog te bundelen in de juiste FHIR format alvorens deze uit te wisselen. Om deze bundeling te maken kunnen de gegevens niet versleuteld zijn. Dit heeft tot gevolg dat de derde partij toegang heeft tot de niet-versleutelde berichten wanneer deze via de broker lopen. Dit betekent dan ook dat de huidige manier van uitwisselen niet langer geschikt zal zijn en er alternatieve methoden geïmplementeerd dienen te worden.

D.2.1.2. Gevolgen van Scenario 1 op de huidige manier van uitwisseling

Uitgaande van Scenario 1 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolg dat een aantal methoden die momenteel toegepast worden om gegevens uit te wisselen niet langer mogelijk zijn. Zo kunnen gegevens niet meer uitgewisseld worden wanneer deze over een broker lopen zoals ZorgDomein en Point, omdat hier geen berichtversleuteling op toegepast kan worden. Dit vereist dat in situaties waar deze methoden toegepast worden alternatieve methoden voor gegevensuitwisseling dienen te worden gedefinieerd. Hierbij kan gedacht worden aan de implementatie volgens de nuts standaarden.

Technische gevolgen:

- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste tot E2E-versleuteling te voldoen.
- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- De bestaande infrastructuur moet opnieuw ingericht worden.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Overstappen op andere methode van gegevensuitwisseling is een langdurend proces.
- Kleinere zorgaanbieders kunnen mogelijk niet mee met de verandering.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.

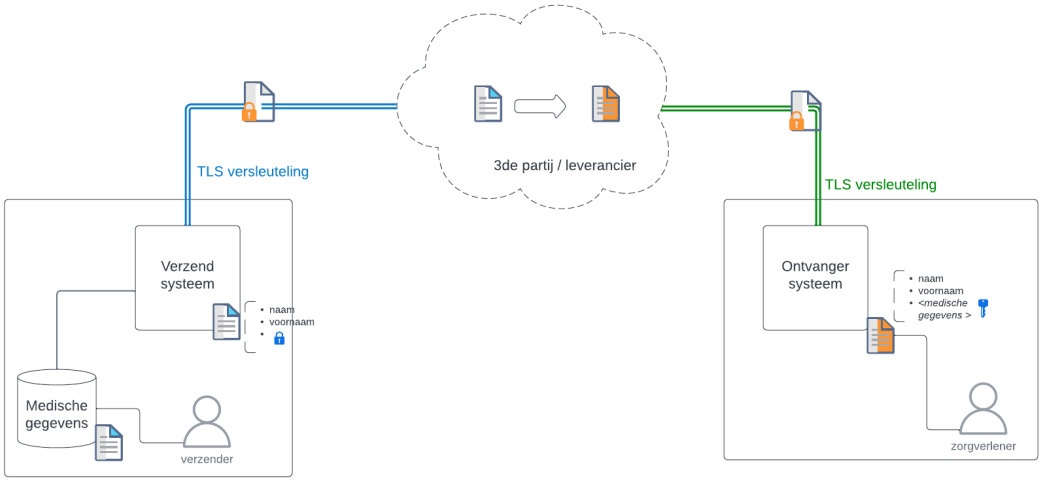
***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau waarbij de voordelen van E2E-beveiliging duidelijk moeten zijn én er uniformiteit over de verschillende gegevensuitwisselingen moet plaatsvinden.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Veranderingen moeten werkbaar en behapbaar blijven voor de verschillende partijen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.
- Uniformiteit in zorgdossiers en terminologie.
- De methoden voor gegevensuitwisseling moeten in lijn blijven met internationale standaarden.

D.2.2. Scenario 2: Een flexibelere interpretatie van E2E-versleuteling

De flexibelere interpretatie van E2E-versleuteling vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er in plaats van versleuteling van het volledige bericht (berichtversleuteling) zoals bij Scenario 1, versleuteling binnen het bericht plaatsvindt (element versleuteling) waardoor gevoelige (medische) informatie binnen het bericht versleuteld zijn. Daarnaast wordt kanaalversleuteling toegepast. Op de gegevenselementen kunnen dus ook nog bepaalde bewerkingen of mappings op uitgevoerd worden, gezien de derde partij de metadata kan uitlezen. Hierdoor kan de derde partij het bericht

eventueel in het juiste formaat en vorm zetten om vervolgens door te zenden naar de ontvanger.



Figuur 16: Schematische weergave van de strikte interpretatie van E2E-versleuteling

D.2.2.1. Scenario 2 in relatie tot de huidige situatie

Binnen Scenario 2 kunnen alleen de versturende en de ontvangen partij de (medische) gegevens zien die gedeeld worden.

I. Gegevensuitwisseling via de email en fax

In de huidige situatie worden gegevens veelal uitgewisseld via (beveiligde) email en fax. Deze manier van gegevensuitwisseling voldoet niet standaard aan de vereisten van E2E-versleuteling en de Wegiz. Onder de Wegiz is de huidige manier van uitwisselen via de fax niet langer geschikt wat vereist dat er alternatieve methoden geïmplementeerd dienen te worden. Om aan een vereiste tot E2E-versleuteling te voldoen voor email zijn aanpassingen noodzakelijk, zoals het versleutelen van het bericht met S/MIME of PGP. Er moet zorggedragen worden dat E2E-versleuteling plaatsvindt. Dit kan betekenen dat een zorginstelling zijn huidige infrastructuur met betrekking tot email volledig moet omgooien of over moet stappen op alternatieve methode voor gegevensuitwisseling.

II. Gegevensuitwisseling door directe uitwisseling tussen zorgsystemen.

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals bijvoorbeeld kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. Voor gegevensuitwisseling via een gedistribueerd netwerk worden de gegevens rechtstreeks vanuit het systeem van de zorgaanbieder gecommuniceerd naar het systeem van de ontvangende zonder systeem specifieke koppelingen of verplichte tussenkomst van een centrale dienstverlener. Daarnaast worden er versleutelingmaatregelen genomen om te bewerkstelligen dat alleen de versturende en de ontvangende partij de gegevens in kunnen zien. Deze manier van uitwisseling voldoet aan de vereisten van E2E-versleuteling.

III. Gegevensuitwisseling via een broker

In de huidige situatie worden gegevens uitgewisseld door gebruik te maken van een platform dat deze uitwisseling faciliteert, zoals ZorgDomein en Point. Om aan de vereisten van E2E-beveiliging te voldoen betekent dit dat deze derde partij de inhoud van dit bericht niet mag zien. Echter is het noodzakelijk om de gegevens om te zetten naar de juiste format (HL7 FHIR) zodat deze uitgewisseld kunnen worden. De enige werkbare oplossing waarbij de huidige manier van uitwisselen kan blijven bestaan is door versleuteling toe te passen binnen het bericht zelf. Op deze manier is de derde partij nog wel in staat de gegevens in de juiste format te zetten, echter zijn de daadwerkelijke (medische) gegevens niet meer zichtbaar. Om aan een vereiste tot E2E-versleuteling te voldoen zijn aanpassingen noodzakelijk.

D.2.2.2. Gevolgen van Scenario 2 op de huidige manier van uitwisseling

Uitgaande van Scenario 2 heeft een vereiste tot E2E-beveiliging van gegevensuitwisseling tot gevolg dat een aantal grote aanpassingen gedaan moeten worden. Zo kunnen gegevens alleen uitgewisseld worden via een broker wanneer er verdere standaardisatie van berichtdefinities

plaatsvindt en additionele maatregelen worden geïmplementeerd. Daarnaast is het goed om te benadrukken dat zulke aanpassingen niet van de een op de andere dag doorgevoerd kunnen worden. Het proces van het verder standaardiseren van berichtdefinities gaat tijd en afstemming tussen verscheidene partijen vereisen. Hierbij moet ook onderzocht worden in welke mate het technisch haalbaar is aangezien sommige bericht elementen ook bewerkt moeten worden, zoals het opdelen van een volledige naam in voor- en achternaam. Overigens kan er in dit scenario ook voor gekozen worden aan de implementatie volgens de Nuts-standaarden.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- De bestaande infrastructuur moet opnieuw ingericht worden.
- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste tot E2E-versleuteling te voldoen.
- Berichtdefinities dienen geformaliseerd te worden.
- Versleuteling binnen de berichten aan de hand van de berichtdefinities dienen geïmplementeerd te worden.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Er dient afstemming plaats te vinden tussen verscheidene partijen met betrekking tot de berichtdefinities.
- Alle partijen dienen de geformaliseerde berichtdefinities over te nemen voor gegevensuitwisseling die via een derde partij loopt.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Overstappen op andere methode van gegevensuitwisseling is een langdurend proces.
- Kleinere zorgaanbieders kunnen mogelijk niet mee met de verandering.

Financiële gevolgen:

- Kosten gerelateerd aan het implementeren van additionele maatregelen.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.
- Kosten gerelateerd aan het ontwikkelen van berichtdefinities.
- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau waarbij de voordelen van E2E-beveiliging duidelijk moeten zijn én er uniformiteit over de verschillende gegevensuitwisselingen moet plaatsvinden.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Veranderingen moeten werkbaar en behapbaar blijven voor de verschillende partijen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.
- Uniformiteit in zorgdossiers en terminologie.
- De methoden voor gegevensuitwisseling moeten in lijn blijven met internationale standaarden.

D.3. E2E-authenticatie voor acute zorg

E2E-authenticatie kan op verscheidene manieren bewerkstelligd worden. De belangrijkste uitgangspunten daarbij zijn dat er onderling vertrouwen tussen IAM-oplossingen dient te zijn en dat de methode voor authenticatie eIDAS Hoog moeten classificeren, in verband met de gevoeligheid van de gegevens die uitgewisseld worden. Een voorbeeld van een inlogmiddel met een hoog betrouwbaarheidsniveau is de UZI-pas.

D.3.1. E2E-authenticatie in relatie tot de huidige situatie

In de huidige situatie vindt er geen gegevensuitwisseling plaats conform betrouwbaarheidsniveau eIDAS Hoog. Op dit moment wordt er voor verpleegkundige overdracht gebruikgemaakt van SSO, 2-factor authenticatie en Yivi (self-sovereign identity).

Inlogmiddelen die voldoen aan eIDAS betrouwbaarheidsniveau Hoog voorzien in de hoogste mate van zekerheid over iemands identiteit. In bijvoorbeeld het geval van de UZI-pas wordt het gehele uitgifteproces van de UZI-pas met grote waarborgen voorzien. Zo is de pas gelinkt aan de BIG-registratie van de zorgprofessional en vindt er bij uitgifte van de pas een fysieke controle van het ID-bewijs plaats. Daarnaast hebben niet alle medewerkers in bijvoorbeeld de VVT toegang tot een UZI-pas aangezien hiervoor een BIG-registratie benodigd is. SSO, 2-factor authenticatie en Yivi voldoen op dit moment niet aan deze vereisten.

D.3.2. Gevolgen van E2E-authenticatie op de huidige manier van uitwisseling

Een vereiste van E2E-authenticatie heeft tot gevolg dat de huidige manier van authenticatie niet langer mogelijk is. Dit vereist dat alternatieve methoden voor authenticatie dienen te worden gedefinieerd en geïmplementeerd. Hierbij is het van belang om te benoemen dat eindgebruikers hierbij betrokken zijn. De manier van hoe zij zich authenticeren zal aangepast worden. Al eerder afgeronde projecten hebben er veel moeite mee ondervonden om gebruikers hier in mee te nemen. Daarnaast zal het ook betekenen dat het aantal certificaten in aantallen zal toenemen.

Technische gevolgen:

- Alternatieve methoden voor authenticatie dienen gedefinieerd en geïmplementeerd te worden conform betrouwbaarheidsniveau eIDAS Hoog.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Naast algemene kennis op informatiebeveiliging betekent dit dat er meer gespecialiseerde kennis nodig is op de concepten van sleutel- en certificaatbeheer. In de huidige situatie is de al gesignaleerd als een beheer probleem.
- Definiëren van andere methode voor authenticatie is een langdurend proces.
- Overstappen op andere methode voor authenticatie is een langdurend proces.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor authenticatie.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van authenticatie die wel voldoet aan het vereiste van betrouwbaarheidsniveau eIDAS Hoog.

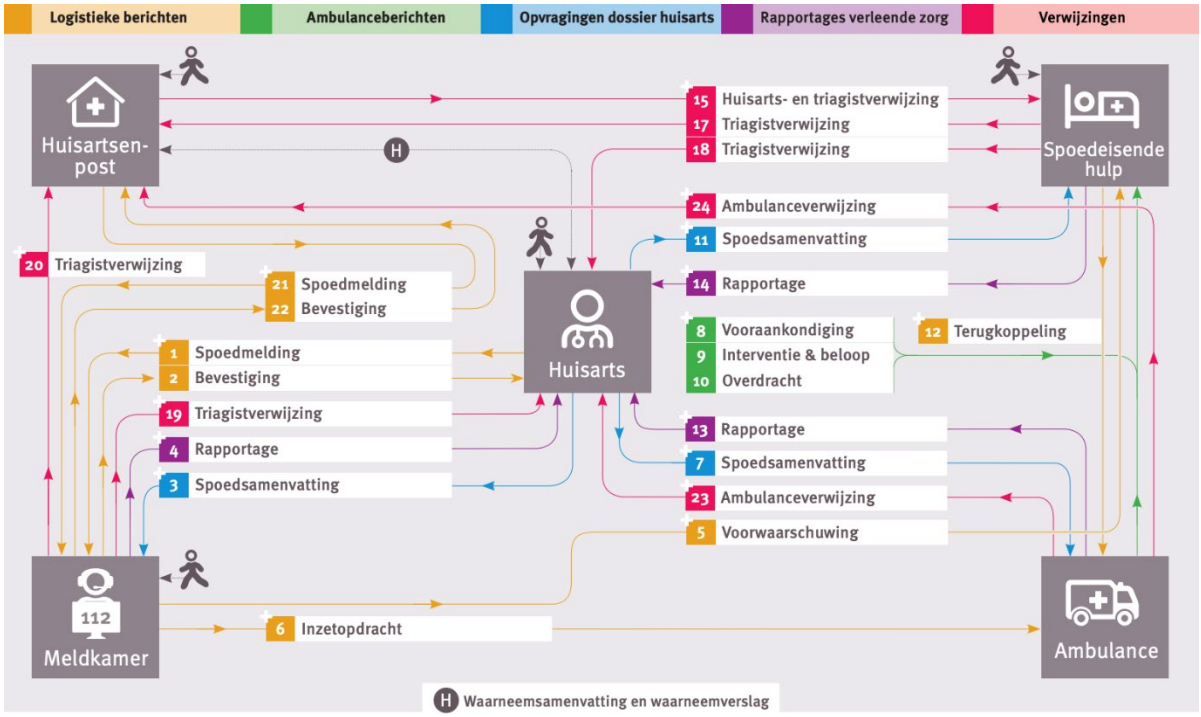
***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals, zoals niet steeds opnieuw in moeten loggen.
- Oplossingen dienen gebruiksvriendelijk te zijn. Zo weinig mogelijk belemmeringen.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

E. Analyse “Acute Zorg”

E.1. Huidige status

Gegevensuitwisseling omtrent de acute zorg omvat elektronische uitwisseling binnen de acutezorgketen: meldkamer ambulancezorg, ambulance, spoedeisende hulp, huisarts, en de huisartsenpost. Deze wisselen gegevens uit met betrekking tot: ambulanceberichten, logistiek berichten, opvraging dossier huisarts, rapportages verleende zorg en verwijzingen. Deze gegevens worden uitgewisseld op basis van de Richtlijn Acute Zorg. Deze richtlijn identificeert 22 type gegevensuitwisselingen gerelateerd aan de acutezorgketen en zijn weergegeven in het volgende figuur. Er kan hierbij dus ook niet gesproken worden van één gegevensuitwisseling, omdat er meerdere partijen betrokken zijn, met verschillende gegevensstromen, via verschillende uitwisselsystemen en leveranciers.



Figuur 17 – Overzicht van de diverse gegevensuitwisselingen bij Acute zorg. Bron: Nictiz

Voor de acute zorg is het van belang dat in een kort tijdsbestek verschillende zorgverleners betrokken kunnen zijn bij de zorg voor een patiënt. Snelle en betrouwbare gegevensuitwisseling is een randvoorwaarde zodat actuele medische gegevens tijdig gedeeld kunnen worden.

Voor gegevensuitwisseling binnen de acute zorg wordt zo veel mogelijk een uniform proces gehanteerd, gebaseerd op de Nictiz-standaarden. Gegevensuitwisseling verloopt op dit moment veelal over een besloten verbinding waar kanaalversleuteling op is toegepast. De gegevens zelf worden in de meeste gevallen niet nogmaals versleuteld waardoor er geen berichtversleuteling plaatsvindt. De gegevensuitwisseling verloopt veelal over verschillende VPN-verbindingen waarbij gegevens tussentijds verder verrijkt worden. Hierdoor is het van belang dat verschillende partijen informatie aan de gegevens toe kunnen voegen en dat de gegevens op die momenten dus niet versleuteld zijn. In enkele gegevensuitwisselingen (bijvoorbeeld van de meldkamer naar de huisartsenpost) worden berichten tussen de systemen van dezelfde leveranciers zelf wel versleuteld. Daarnaast wordt er ook gebruikgemaakt van beveiligde zorgmail, echter komt dit steeds minder voor. Een bestaande belemmering is dat niet alle relevante zorgaanbieders op dit moment aangesloten zijn op (dezelfde) uitwisselprogramma's, daarnaast is het niveau van volwassenheid van deze uitwisselprogramma's erg uiteenlopend.

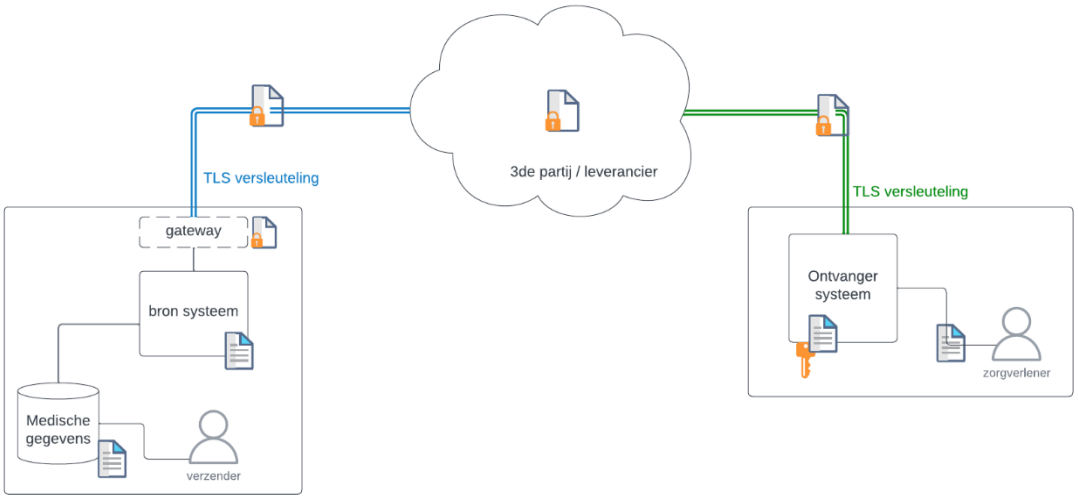
Een groot deel van de gegevensuitwisselingen loopt **via een centrale voorziening**. Zo wordt het LSP onder andere gebruikt voor gegevensuitwisseling tussen de huisartsenposten en de spoedeisende hulp, spoedmeldingen van de huisarts naar de meldkamer en het opvragen van een ICA-samenvatting bij de huisarts. Door de Regionale Ambulancevoorzieningen (RAV-en) wordt veelal gebruikgemaakt van het Landelijk Systeem-Digitale Vooraankondiging (LS-DV), een centraal koppelpunt mogelijk gemaakt door AZN. Hier is ook het LSP aan gekoppeld. Binnen het LS-DV wordt (medische) informatie die door ambulanceteams in het veld wordt verzameld beschikbaar gemaakt voor andere zorgaanbieders.

E.2. E2E-versleuteling voor acute zorg

E2E-versleuteling voor de acute zorg wordt uitgewerkt aan de hand van twee scenario's. Binnen deze scenario's wordt een striktere (sectie 2.1: Scenario 1) en een iets flexibelere interpretatie (sectie 2.2: Scenario 2) van E2E-versleuteling gehanteerd. Elk van deze scenario's wordt uitgezet tegen de huidige manier van gegevensuitwisseling en vervolgens worden de technische, organisatorische en financiële gevolgen en eventuele randvoorwaarden voor het scenario uitgewerkt.

E.2.1. Scenario 1: Een strikte interpretatie van E2E-versleuteling

De strikte interpretatie van E2E-versleuteling vereist dat de gegevensuitwisseling van het verzendende systeem tot aan het ontvangende systeem versleuteld is, wat betekend dat eventuele tussenpartijen het bericht niet in kunnen zien. Binnen dit scenario zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen het versturende en ontvangende systeem inzicht hebben in de informatie die wordt uitgewisseld.



Figuur 18: Schematische weergave van de strikte interpretatie van E2E-versleuteling

E.2.1.1. Scenario 1 in relatie tot de huidige situatie

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. In de huidige situatie wordt er veel gebruikgemaakt van gegevensuitwisseling via een centrale voorziening.

E.2.1.2. Gegevensuitwisseling via een centrale voorziening

Binnen Scenario 1 zijn versleutelingmaatregelen verplicht, zoals kanaal- en berichtversleuteling, waardoor alleen de versturende en ontvangende partij inzicht hebben in de informatie die wordt uitgewisseld. In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een centrale voorziening voor de uitwisseling van gegevens, zoals het LSP en de LSDV. Hoewel er meerdere lagen aan versleuteling worden toegepast zoals het gebruik van een afgesloten

netwerk en kanaalversleuteling zijn de berichten zelf niet versleuteld. Dit heeft tot gevolgen dat de derde partij toegang heeft tot de niet-versleutelde berichten wanneer deze over de centrale voorziening lopen. Dit betekent dan ook dat de huidige manier van uitwisselen niet langer geschikt voor een aanzienlijk deel van de uitwisselingen zal zijn en er alternatieve methoden geïmplementeerd dienen te worden.

E.2.1.3. Gevolgen van Scenario 1 op de huidige manier van uitwisseling

Uitgaande van Scenario 1 heeft een vereiste tot E2E-versleuteling van gegevensuitwisseling tot gevolg dat een aantal methoden die momenteel toegepast worden om gegevens uit te wisselen niet langer mogelijk zijn. Zo kunnen gegevens niet meer uitgewisseld worden wanneer deze over een centrale voorziening lopen zoals het LSP en het LSDV, omdat hier geen berichtversleuteling op toegepast kan worden. Dit vereist dat in situaties waar deze methoden toegepast worden alternatieve methoden voor gegevensuitwisseling dienen te worden gedefinieerd. Daarnaast kan er geen tussentijdse verrijking van gegevens meer plaatsvinden.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- De bestaande infrastructuur moet opnieuw ingericht worden.
- Berichtversleuteling moet toegevoegd worden.

***Organisatorische* gevolgen:**

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Kans op overbevraging van zorgaanbieders doordat het onduidelijk is waar gegevens zich bevinden (lokalisatie probleem).
- Overstappen op andere methode van gegevensuitwisseling is een langdurend proces.
- Verrijking gedurende gegevensuitwisseling is niet mogelijk.
- Lokalisatie en adressering moet op een andere manier gefaciliteerd worden.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Hoge kostbaar in verband met het herinrichten van de technische infrastructuur.

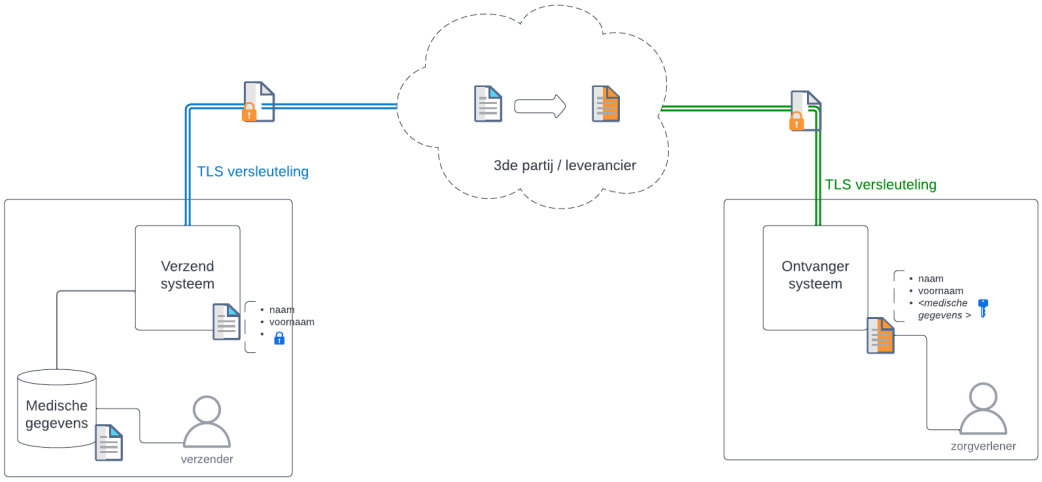
Randvoorwaarden:

- Duidelijke sturing op landelijk niveau, door bijvoorbeeld AZN, waarbij de voordelen van E2E-beveiliging duidelijk moeten zijn én er uniformiteit over de verschillende gegevensuitwisselingen moet plaatsvinden.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Veranderingen moeten werkbaar en behapbaar blijven voor de verschillende partijen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- De gegevensuitwisselingen moeten zo uniform mogelijk worden ingericht.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

E.2.2. Scenario 2: Een flexibelere interpretatie van E2E-versleuteling

De flexibelere interpretatie van E2E-versleuteling vereist dat de daadwerkelijke gevoelige gegevens die gedeeld worden door middel van de gegevensuitwisseling E2E-versleuteld zijn. Dit betekent dat er in plaats van versleuteling van het volledige bericht (berichtversleuteling) zoals bij Scenario 1, versleuteling binnen het bericht plaatsvindt (element versleuteling) waardoor de gevoelige (medische) informatie binnen het bericht versleuteld zijn. Daarnaast wordt kanaalversleuteling

toegepast. Op de gegevenselementen kunnen dus ook nog bepaalde bewerkingen of mappings op uitgevoerd worden, gezien de derde partij de metadata kan uitlezen. Hierdoor kan de derde partij het bericht eventueel in het juiste formaat en vorm zetten om vervolgens door te zenden naar de ontvanger.



Figuur 19: Schematische weergave van de flexibele interpretatie van E2E-versleuteling

E.2.2.1. Scenario 2 in relatie tot de huidige situatie

Binnen Scenario 2 kunnen alleen de versturende en de ontvangen partij de (medische) gegevens zien die gedeeld worden.

E.2.2.2. Gegevensuitwisseling via een centrale voorziening

In de huidige situatie wordt veel informatie uitgewisseld door gebruik te maken van een centrale voorziening van een derde partij die deze uitwisseling faciliteert door een translatieslag uit te voeren. Om aan de vereisten van E2E-beveiliging te voldoen betekent dit dat deze derde partij de inhoud van dit bericht niet mag zien. Echter is het voor de translatie noodzakelijk om het bericht te kunnen inzien, waardoor berichtversleuteling geen oplossing is (Scenario 1). De enige werkbare oplossing waarbij de huidige manier van uitwisselen kan blijven bestaan is door versleuteling toe te passen binnen het bericht zelf. Op deze manier is de derde partij nog wel in staat het format te identificeren, echter zijn de daadwerkelijke (medische) gegevens niet meer zichtbaar. Om aan een vereiste tot E2E-versleuteling te voldoen zijn aanpassingen noodzakelijk.

E.2.2.3. Gevolgen van Scenario 2 op de huidige manier van uitwisseling

Uitgaande van Scenario 2 heeft een vereiste tot E2E-beveiliging van gegevensuitwisseling tot gevolg dat een aantal grote aanpassingen gedaan moeten worden. Zo kunnen gegevens alleen uitgewisseld worden via een centrale voorziening wanneer er verdere standaardisatie van berichtdefinities plaatsvindt en additionele maatregelen worden geïmplementeerd. Daarnaast is het goed om te benadrukken dat zulke aanpassingen niet van de een op de andere dag doorgevoerd kunnen worden. Het proces van het verder standaardiseren van berichtdefinities gaat tijd en afstemming tussen verscheidene partijen vereisen. Daarnaast kan er, door het doorvoeren van deze aanpassingen, geen tussentijdse verrijking van gegevens meer plaatsvinden. Dit heeft dus impact op de efficiëntie waarmee belangrijke informatie gedeeld kan worden. Dit zou betekenen dat er of maatregelen doorgevoerd dienen te worden waardoor verrijking niet meer mogelijk is of er dient een andere methode voor gegevensuitwisseling geïmplementeerd te worden.

Technische gevolgen:

- Alternatieve methoden voor gegevensuitwisseling dienen gedefinieerd en geïmplementeerd te worden.
- De bestaande infrastructuur moet opnieuw ingericht worden.

- Technische maatregelen dienen geïmplementeerd te worden om aan de vereiste tot E2E-versleuteling te voldoen.
- Berichtdefinities dienen geformaliseerd te worden.
- Versleuteling binnen de berichten aan de hand van de berichtdefinities dienen geïmplementeerd te worden.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Er dient afstemming plaats te vinden tussen verscheidene partijen met betrekking tot de berichtdefinities.
- Alle partijen dienen de geformaliseerde berichtdefinities over te nemen voor gegevensuitwisseling die via een derde partij loopt.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Kans op overbevraging van zorgaanbieders doordat het onduidelijk is waar gegevens zich bevinden (lokalisatie probleem).
- Overstappen op andere methode van gegevensuitwisseling is een langdurend proces.
- Verrijking gedurende gegevensuitwisseling is niet mogelijk.
- Lokalisatie en adressering moet op een andere manier gefaciliteerd worden.

Financiële gevolgen:

- Kosten gerelateerd aan het implementeren van additionele maatregelen.
- Kosten gerelateerd aan het ontwikkelen van berichtdefinities.
- Kosten gerelateerd aan het beheren en in stand houden van de additionele maatregelen.
- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor uitwisseling.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van gegevensuitwisseling die wel voldoet aan de vereisten.
- Hoge kostbaar in verband met het herinrichten van de technische infrastructuur.

Randvoorwaarden*:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals.
- Veranderingen moeten werkbaar en behapbaar blijven voor de verschillende partijen.
- Oplossingen dienen gebruiksvriendelijk te zijn.
- De gegevensuitwisselingen moeten zo uniform mogelijk worden ingericht.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

E.3. E2E-authenticatie voor acute zorg

E2E-authenticatie kan op verscheidene manieren bewerkstelligd worden. De belangrijkste uitgangspunten daarbij zijn dat er onderling vertrouwen tussen IAM-oplossingen dient te zijn en dat de methode voor authenticatie eIDAS Hoog moeten classificeren, in verband met de gevoeligheid van de gegevens die uitgewisseld worden. Een voorbeeld van een inlogmiddel met een hoog betrouwbaarheidsniveau is de UZI-pas.

E.3.1. E2E-authenticatie in relatie tot de huidige situatie

In de huidige situatie vindt een deel van de gegevensuitwisselingen plaats conform betrouwbaarheidsniveau eIDAS Hoog, namelijk door middel van de UZI-pas. Echter is tijdens de gesprekken vastgesteld dat deze methode niet altijd leidt tot de juiste toepassing in de praktijk. Zo is het niet voor alle zorgverleners mogelijk een UZI-pas te verkrijgen en is dit authenticatiemiddel erg kostbaar. Daarnaast wordt de huidige toepasbaarheid van de UZI-pas niet als gebruiksvriendelijk ervaren waardoor er soms naar workarounds binnen het authenticatie proces gezocht wordt. Additioneel wordt authenticeren op het niveau van de gebruiker niet als gewenst gezien omdat dit niet bruikbaar is in de praktijk. Dit resulteert in belemmering voor het leveren van acute zorg.

E.3.2. Gevolgen van E2E-authenticatie op de huidige manier van uitwisseling

Een vereiste van E2E-authenticatie heeft tot gevolg dat in sommige situaties de huidige manier van authenticatie niet langer mogelijk zijn. Dit vereist dat alternatieve methoden voor authenticatie dienen te worden gedefinieerd en geïmplementeerd.

Technische gevolgen:

- Alternatieve methoden voor authenticatie dienen gedefinieerd en geïmplementeerd te worden conform betrouwbaarheidsniveau eIDAS Hoog.

Organisatorische gevolgen:

- Mogelijke weerstand tegen deze verandering vanuit leveranciers en zorgaanbieders als onvoldoende is aangetoond dat deze verplichting een toegevoegde waarde met betrekking tot informatiebeveiliging heeft.
- Kennis op het gebied van informatiebeveiliging is bij een groot deel van de zorgaanbieders niet hoog genoeg om dit zelfstandig te kunnen implementeren. Verantwoordelijkheid komt bij de leverancier te liggen en/of implementatie ondersteuning moet geboden worden.
- Definiëren van andere methode voor authenticatie is een langdurend proces.
- Overstappen op andere methode voor authenticatie is een langdurend proces.

Financiële gevolgen:

- Kosten gerelateerd aan het ontwikkelen van nieuwe methoden voor authenticatie.
- Kosten gerelateerd aan het overstappen naar een alternatieve manier van authenticatie die wel voldoet aan het vereiste van betrouwbaarheidsniveau eIDAS Hoog.

***Randvoorwaarden**:*

- Duidelijke sturing op landelijk niveau.
- Veranderingen mogen geen (grote) gevolgen hebben voor de huidige workflow van de zorgprofessionals, zoals niet steeds opnieuw in moeten loggen.
- Oplossingen dienen gebruiksvriendelijk te zijn. Zo weinig mogelijk belemmeringen.
- Zorgaanbieders moeten hun basishygiëne op het gebied van informatiebeveiliging op orde hebben.

F. Geraadpleegde documenten en betrokken onderzoekers

F.1. Geraadpleegde documenten

Wij hebben de beschikbaar gestelde documentatie nauwkeurig doorgenomen. Dit bestond uit de volgende documenten:

Tabel 2: overzicht geraadpleegde documenten

Domein	
VRHT	- NEN 7503 - Beantwoording IAK-vragen – VRHT. - Nota van toelichting concept Begiz - Wijziging Besluit elektronische gegevensuitwisseling in de zorg - Website Topicus - Website LSP - Website LHV
Basisgegevensset Zorg	- NEN 7540 - Concept besluit elektronische gegevensuitwisseling in de zorg - Beantwoording IAK-vragen – overdracht cliëntgegevens tussen instellingen voor medisch specialistische zorg. - Conceptrapport regeldrukonderzoek AMvB's BgZ en Beeldbeschikbaarheid en Begiz (SIRA Consulting) - Website Nictiz - Website Chipsoft - Website Hinq
Beeldbeschikbaarheid	- NEN 7541, NEN 7510, NEN 7512, NEN 7513 - Nota van toelichting – aanwijzing gegevensuitwisseling ten behoeve van beeldbeschikbaarheid tussen instellingen voor medisch-specialistische zorg en bevolkingsonderzoek naar kanker - Conceptrapport regeldrukonderzoek AMvB's BgZ en Beeldbeschikbaarheid en Begiz (SIRA Consulting) - Beeldbeschikbaarheid samenvatting - Website Alphatron - Website Twiin - Website NVvR
Verpleegkundige overdracht	- NEN 7545 - Eindrapport Verkenning Implementatieondersteuning Verpleegkundige Overdracht (VIVO) - eOverdracht samenvatting - Whitepaper Interoperabiliteit eOverdracht Zorgdomein Transfer - Website Nedap - Website Nuts - Website ICTU
Acute zorg	- Met spoed beschikbaar – architectuur acute zorg infrastructurele verbindingen per zorgaanbiedertype - Website Topicus - Website AZN - Website RAVU
Afsprakenstelsels	- Website MedMij - Website AORTA-LSP - Website Twiin - Website Koppeltaal - Website VZVZ
Overkoepelend	- Wettekst Wegiz, inclusief amendement Hijnk & Van den Berg - Meerjarenagenda Wegiz

	- Integraal zorgakkoord: Samen werken aan gezonde zorg - Kamerbrief “voortgang op elektronische gegevensuitwisseling” - Besluit elektronische gegevensuitwisseling in de zorg (Begiz) - Besluit elektronische gegevensverwerking door zorgaanbieders - NEN 7510-01, NEN 7510-02, NEN 7512 en NEN 7513. - Architectuurdocumenten behorend bij de DIZRA en ZiRA. - European Health Data Space (EHDS). - Andere beschrijvingen van processen, systeemlandschap en use cases. - Algemene website Rijksoverheid

F.1.1. Geïnterviewde partijen

Wij hebben per gegevensuitwisseling een desbetreffende leverancier, aanbieder uitwisselingssysteem en zorgorganisatie geïnterviewd om zo een holistisch overzicht te krijgen en kennis te vergaren van de zes aandachtsgebieden. Zo fuseerde wij de technische, organisatorische en financiële perspectieven van E2E-beveiliging. Per interview hanteerden wij een vaste set aan vragen specifiek gericht op het adresseren van de zes aandachtsgebieden volgens het Transformatiemodel. Tijdens elk interview werden er aantekeningen gemaakt van bevindingen die vervolgens zijn verwerkt in het eindrapport.

Tabel 3: overzicht geïnterviewde partijen

Domein	**Partijen**	
VRHT	Leverancier	Topicus
	Uitwisselingsysteem	LSP (VZVZ)
	Organisatie	Landelijke Huisartsen Vereniging (LHV)
Basisgegevensset Zorg	Leverancier	Chipsoft
	Uitwisselingssysteem	Hinq
	Organisatie	Maastricht Universitair Medisch Centrum (MUMC)
Beeldbeschikbaarheid	Leverancier	Alphatron
	Uitwisselingssysteem	TWIIN (VZVZ)
	Organisatie	Nederlandse Vereniging voor Radiologie (NVvR)
Verpleegkundige overdracht	Leverancier	Nedap (ONS)
	Uitwisselingssysteem	Nuts
	Organisatie	ICTU
Acute zorg	Leverancier	Topicus
	Uitwisselingssysteem	Ambulancezorg Nederland (AZN)
	Organisatie	Regionale Ambulance Voorziening Utrecht (RAVU)
Overkoepelend en andere relevante organisaties.	MedMij	
	NEN (Nederlandse normalisatie-instituut)	
	Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ)	
	WhiteBox Systems	