Technische handreiking NTA 7516 voor e-mail dienstenleveranciers

Woord vooraf

NTA 7516[1] is een functionele norm voor ad-hoc berichten uitwisseling van persoonlijke gezondheidsinformatie via e-mail, chat, message applicaties, et cetera. NTA 7516 zal in de toekomst worden doorontwikkeld naar NEN 7516 of naar een Europese norm.

Aanbieders van e-mail communicatiediensten (leveranciers) hebben toegezegd binnen een jaar na publicatie (16 mei 2020) te voldoen aan NTA 7516. Een verplicht onderdeel van deze norm is het tot stand brengen van multikanaalcommunicatie en de daarmee samenhangende interoperabiliteitseisen tussen alle producten. Dit lukt alleen als de leveranciers hiervoor eenduidige (technische) keuzes maken. Deze technische handreiking doet suggesties aan de leveranciers om een technische invulling te geven aan dit criterium uit NTA 7516. Wanneer een leverancier voor een product claimt dat NTA 7516 wordt nageleefd, dan moet deze de interoperabiliteitseisen in deze technische handreiking aantoonbaar volledig naleven.

De technische handreiking kan op basis van veldafspraken of nieuwe inzichten worden geactualiseerd en / of aangescherpt. Dit houdt in dat naleving van de norm voortdurend moet worden gemonitord: na elke herziening van NTA 7516 of van deze technische handreiking dient er verbeterd te worden om aan de norm geconformeerd te blijven.

Dankwoord
Onze dank gaat uit naar de vele partijen die input hebben input aan deze technische handreiking. Onze speciale dank gaat hierbij uit naar het Nationaal Cyber Security Center voor hun bijdrage.

1 NEN, NTA 7516, https://www.nen.nl/Alles-over-NEN-7510/NTA-7516.htm, 16 mei 2019

Inhoud

Woord vooraf 2

Inhoud 3

1 Inleiding 5
1.1 Algemeen 5
1.2 (Optionele) Eisen en suggesties 5
1.3 Bericht encryptie 6
1.4 Basisbegrippen 6
1.5 Opbouw technische handreiking 7

2 Handreiking multikanaalcommunicatie-eisen 8
2.1 Multikanaalcommunicatie 8
2.2 Check geldigheid DNS record 12
2.3 Herkomstbevestiging 13
2.4 Data-integriteit 13
2.5 Onweerlegbaarheid verzender 13
2.6 Gegevensvertrouwelijkheid 14
2.7 Communicatievertrouwelijkheid 15
2.8 Internationaal ad-hocberichtenverkeer 15

3 Handreiking optionele eisen 17
3.1 Veilige informatievoorziening 17
3.2 Minimale beschikbaarheid, maximale uitvalduur en maximaal gegevensverlies 17
3.3 Toegangsvertrouwelijkheid 18
3.4 Continuïteit van ad-hocberichtenverkeer – beantwoorden 19
3.5 Continuïteit van ad-hocberichtenverkeer – doorsturen 19
3.6 Veiligheid als gemak 19
3.7 Leesbaarheid 20
3.8 Eigen kopie 20

4 Overige suggestie(s) 21
4.1 Dossierkoppeling 21

5 Implementatie technische standaarden 22
5.1 AES 22
5.2 CAdES 22
5.3 DANE 23
5.4 DKIM 23
5.5 DMARC 23
5.6 IMAP 24
5.7 SMTP 24
5.8 SPF 25
5.9 STARTTLS 25
5.10 TLS 25

Bijlage A Ongewenste headers 27

Bijlage B Veilig transport bij ontbreken DNSSEC 29
Verificatiestappen voor verzender 29
Inspanning voor ontvanger 30

Bijlage C Veilig transport bij ontbreken DANE 31
Introductie 31
Voorbeeldsituatie 31
Verificatiestappen voor verzender 32
Inspanning voor ontvanger 32
Controle 32

Bijlage D Wanneer is er sprake van interoperabiliteit? 34

1 Inleiding

1.1 Algemeen

NTA 7516 introduceert een aantal criteria die moeten worden vervuld door zogeheten professionals (beroepsmatige gebruikers en hun organisaties), voordat ad-hoc persoonlijke gezondheidsinformatie via e-mail, chat et cetera gecommuniceerd mag worden. Professionals moeten zelf in veel gevallen waardes toekennen aan elk van de criteria. NTA 7516 geeft daarbij grenswaardes aan, die in geen geval mogen worden geschonden. Voor professionals komt er een praktisch implementatiehandboek dat hen helpt bij het voldoen aan NTA 7516.

NTA 7516 stelt ook eisen aan communicatiediensten-leveranciers. Deze technische handreiking, behorende bij NTA 7516, beoogt de leveranciers te helpen om aan NTA 7516 te voldoen. Deze technische handreiking is bedoeld voor leveranciers van e-mail diensten die wensen te gaan voldoen aan NTA 7516. De handreiking zal op een later moment worden uitgebreid voor leveranciers van chat, message en andersoortige diensten waar ad-hoc berichten mee gecommuniceerd kunnen worden.

1.2 (Optionele) Eisen en suggesties

In de volgende tabel staat aangegeven hoe een leverancier aan NTA 7516 kan voldoen en hoe een professional aan NTA 7516 kan voldoen.

Groep	**Criterium**	**Communicatiedienst**	**Professional**
Beschikbaarheid	Minimale *beschikbaarheid* (6.1.2)	Optioneel	Eis
	Maximale uitvalduur (6.1.3)	Optioneel	Eis
	Maximaal gegevensverlies (6.1.4)	Optioneel	Eis
Integriteit	Herkomstbevestiging (6.1.5)	Optioneel[2]	Eis
	Data-*integriteit* (6.1.6)	Optioneel[2]	Eis
	Onweerlegbaarheid verzender (6.1.7)	Optioneel[2]	Eis
Vertrouwelijkheid	Gegevens*vertrouwelijkheid* (6.1.9)	Optioneel[2]	Eis
	Toegangs*vertrouwelijkheid* (6.1.10)	Optioneel	Eis
	Communicatie*vertrouwelijkheid* (6.1.11)	Optioneel[2]	Eis
	Internationaal *ad-hocberichtenverkeer* (6.1.13)	Optioneel[2]	Eis
Gebruiksvriendelijkheid	Continuïteit van *ad-hocberichtenverkeer* – beantwoorden (6.1.14)	Optioneel	Eis
	Continuïteit van *ad-hocberichtenverkeer* – doorsturen (6.1.15)	Optioneel	Eis
	Veiligheid als gemak (6.1.16)	Optioneel	Eis
	Leesbaarheid (6.1.17)	Optioneel	Eis
	Eigen kopie (6.1.18)	Optioneel	Eis
Interoperabiliteit	Dossierkoppeling (6.1.19)	Optioneel	Optioneel
	Multikanaalcommunicatie (7.2)	Eis	-

[2] Om aan de Multikanaalcommunicatie eis te voldoen zijn de criteria 6.1.5., 6.1.6., 6.1.7, 6.1.9, 6.1.11 en 6.1.13 ook verplicht.

De professional dient aan alle criteria (met uitzondering van de Dossierkoppeling) van NTA 7516 te voldoen. De professional voldoet automatisch aan alle criteria die worden afgedekt door de door de professional ingezette communicatiedienst. Wanneer een ingezette communicatiedienst niet voldoet aan alle criteria uit NTA 7516, dient de professional de resterende criteria uit NTA 7516 op andere wijze in te vullen.

Leveranciers dienen altijd te voldoen aan de multikanaalcommunicatie-eis en één van de andere criteria. Dit houdt in dat een communicatiedienst niet aan NTA 7516 voldoet indien deze niet interoperabel is met andere communicatiediensten die aan NTA 7516 voldoen. Uiteraard kan en mag de leverancier aan veel meer criteria voldoen om zo de professional te ontlasten.

In deze handreiking staan technieken en standaarden voor leveranciers om aan de interoperabiliteits-eisen van NTA 7516 te voldoen. Deze technische handreiking heeft daarbij geen verplichtend karakter. Voorwaarde is echter wel dat de leveranciers een gedragen keuze maken voor andere toe te passen technieken en standaarden om gezamenlijk aan de interoperabiliteitseisen van NTA 7516 te kunnen voldoen. Daarnaast bevat deze handreiking suggesties voor technieken en standaarden om aan de andere criteria van NTA 7516 te voldoen.

1.3 Bericht encryptie

In NTA 7516 staat in paragraaf 6.1.9 bij Gegevensvertrouwelijkheid aangegeven dat toegang tot opgeslagen berichten onmogelijk moet zijn. Er staat ook dat versleuteling met verantwoord sleutelbeheer hiervoor vaak wordt ingezet. Op dit moment bestaat er nog geen gedragen open standaard voor de encryptie van mail berichten. Overwogen is om hier S/MIME of PGP voor in te zetten. Beiden staan echter (nog) niet op de verplicht toe te passen lijst van open standaarden van Forum Standaardisatie en kennen nog beperkte adoptie.

Zodra er een open standaard voor de encryptie van mail berichten is vastgesteld door Forum Standaardisatie, zal worden overwogen om deze standaard aan de technische handreiking toe te voegen.

1.4 Basisbegrippen

Een e-mailbericht verloopt vanaf een verzender tot aan de ontvanger via een infrastructuur die als volgt kan worden geschetst.

transportrichting		→	→	→	→
softwarecomponent	MUA (mail user agent)	MSA (mail sub mission agent)	MTA (mail transfer agent(s))	MDA (mail delivery agent)	MRA (mail retrieval agent)
betekenis	client verzender	server verzender	gegevensdoorgifte	server ontvanger	client ontvanger
voorbeelden	Outlook	Exchange	(internet)	Google mail server	G suite client
voorbeeldprovider	Microsoft	Microsoft		Google	Google

De beheerder van de mail sub mission agent (MSA) respectievelijk mail delivery agent (MDA) is binnen dit document de mail service provider (MSP): een dienstverlener voor de verzender respectievelijk de ontvanger van een e-mail bericht. Waar wordt gesproken over «server» of «servers», dan worden zowel de MSA als de MDA bedoeld. Implementatie-items die betrekking hebben op servers en/of een MSP, zijn in het geel aangegeven.

Met client service provider (CSP) wordt in deze technische handreiking de beheerder van een beheerde client bedoeld, bijvoorbeeld Outlook binnen een ziekenhuis. Een organisatie kan het client beheer zelf uitvoeren, maar het kan het ook hebben uitbesteed. Onder onbeheerde clients worden clients verstaan waarbij geen zekerheid omtrent het beheer ervan kan worden geboden. Onbeheerde clients worden veelal aangetroffen bij particuliere burgers, maar ook bij zakelijke gebruikers die zelf een client op een smartphone installeren is sprake van een onbeheerde client.

Waar in dit document wordt gesproken over «client» of «clients», dan worden zowel de beheerde mail user agent (MUA) als de beheerde mail retrieval agent (MRA) bedoeld. Implementatie-items die betrekking hebben op beheerde clients en/of een CSP, zijn in het blauw aangegeven.

Voor een full service provider, die zowel de client als de zend- en ontvangstserver beheert, zijn zowel de items van toepassing voor de CSP als die voor de MSP.

1.5 Opbouw technische handreiking

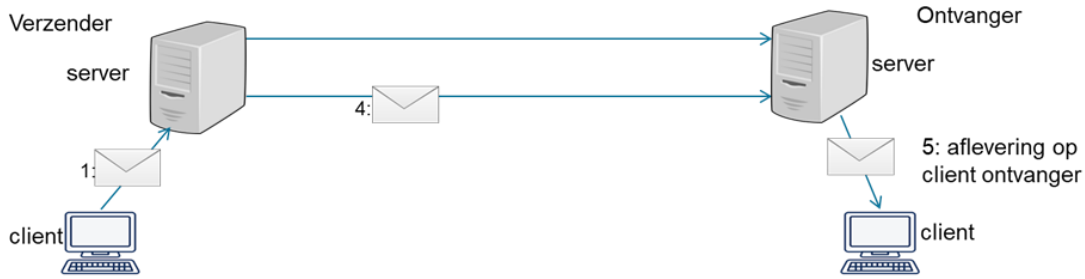
In deze handreiking wordt onderscheid gemaakt tussen de Multikanaalcommunicatie-eis (hoofdstuk 2), de ‘optionele eisen’ (hoofdstuk 3) en ‘overige suggesties’ (hoofdstuk 4). In hoofdstuk 5 staan de technische standaarden genoemd.

2 Handreiking multikanaalcommunicatie-eisen

De leveranciers dienen onderling vast te stellen welke technische keuzes zij maken om multikanaalcommunicatie-eis van NTA 7516 te voldoen. De gekozen technieken en standaarden dienen voor elke aanbieder van een communicatiedienst vrij toegankelijk en toe te passen zijn, zodat elke aanbieder van een communicatiedienst in staat is om aan NTA 7516 te kunnen voldoen. In deze technische handreiking zijn daarom alleen open standaarden opgenomen.

In dit hoofdstuk wordt een voorstel gedaan hoe aan deze eis te voldoen. Indien aanbieders van communicatiediensten onderling met een gedragen voorstel komen voor de invulling van de toe te passen technieken en standaarden dan staat het Informatieberaad daar open voor. Voorwaarde is wel dat de aangedragen technieken en standaarden voor elke aanbieder van een communicatiedienst vrij toegankelijk en toe te passen zijn.

In onderstaand schema staat aangeven hoe berichten veilig worden verzonden en opgeslagen. De omgeving van de verzender controleert eerst of de ontvangende omgeving aan NTA 7516 voldoet (Zie 2.1 multikanaalcommunicatie). Indien daar aan wordt voldaan, wordt er een TLS 1.2 of 1.3 verbinding opgezet waarover het bericht (zonder aanvullende berichtversleuteling) wordt verzonden. Wel dienen berichten (en bijlagen) versleuteld opgeslagen te worden op de (mail)servers (zie eis 2.4). De versleuteling van berichten tussen client en (mail)server (1 en 5 in het schema) mag op een door de communicatiedienst aanbieder gekozen manier plaatsvinden, mits deze voldoet aan de eisen zoals gesteld in eis 2.4.



- Handreiking stelt eisen aan type versleuteling in transport (dus 1 en 5) en opslag.
- Transport (4) op basis van versleuteling met TLS 1.2/1.3
- Overdracht van verzender naar ontvanger (onversleuteld) op de server van ontvanger

Voordeel:
- Gedeeltelijk vrije keuze leveranciers in encryptie
- Zekerheid ten aanzien van informatiebeveiliging voor alle partijen

Nadeel:
- Gebaseerd op vertrouwen dat certificering werkt en de ontvangende partij daarmee inderdaad sterke/goede encryptie toepast die garantie geeft op feit dat alleen beoogde ontvangers er bij kunnen
- Gebaseerd op vertrouwen dat overheden geen 'backdoor' hebben door kopie van private sleutel van CA.

2.1 Multikanaalcommunicatie

Het moet mogelijk zijn om berichten van één communicatiedienst verder te laten verwerken door een andere communicatiedienst en vice versa (zie NTA 7516 paragraaf 7.2.). Hierbij is de ontvangende communicatiedienst verantwoordelijk voor adequate en goed beschermde aflevering in de mailbox van de ontvanger. Indien de mailbox van de ontvanger voldoet aan NTA 7516, dan kan de ontvangende communicatiedienst een bericht in de mailbox afleveren zonder dat de ontvanger extra handelingen hoeft te verrichten voor het lezen van de inhoud. De ontvangende communicatiedienst neemt dan de

verantwoordelijkheid van de verzendende communicatie over conform de eisen in NTA 7516 en deze technische handreiking.

Reguliere uitwisseling van e-mailberichten is geen probleem zolang aansluiting bij reguliere mail-standaarden (zoals SMTP) wordt gezocht. NTA 7516 verlangt echter dat er tussen 'NTA-veilige' partijen op basis van 'multikanaalcommunicatie' wordt gecommuniceerd.

Hiervoor zijn twee DNS text records nodig:

- Eén text record bij de professional waarin deze zelf verklaart te voldoen aan NTA7516 en welke communicatiedienstaanbieder van Veilige mail gebruikt wordt. Dit text record heeft een geldigheid van 3 jaar;
- En een tekst record bij de mailprovider van de professional waarin de versie van het toegepaste normenkader staat. Deze zal uiteindelijk verwijzen naar een NEN-register. Dit text record heeft een geldigheid van 1 jaar.

Bij de professional wordt in het domein van de ontvangende professional een DNS TXT RR gepubliceerd om de verzendende server te laten weten dat NTA 7516-compliant ontvangst mogelijk is. De syntax van het NTA7516 TXT record dat bij een gecertificeerd domein aanwezig behoort te zijn is:
ntatxt = version ";" startdate ";" enddate ";" provider [";" ntamx]
waarbij de betekenis van de componenten als volgt is:

version	= "v=NTA7516-1"
	Wordt gewijzigd voor nieuwe versies van de norm.
startdate	= "startdate=" date
	Startdatum geldigheid van het record. Deze valt binnen de periode dat de NTA7516 certificering van het domein geldig is.
enddate	= "enddate=" date
	Einddatum (inclusief) geldigheid van het record. Deze valt binnen de periode dat de NTA7516 certificering van het domein geldig is, en is groter of gelijk aan startdate. Na de enddate is het resource record niet meer geldig.
provider	= "provider=" { character }
	character moet vallen onder '!' t/m '~' (ASCII 33 t/m 126): iedere CHAR behalve <SP> en "-teken en alle control characters (US-ASCII 0-31 en ook 127).
date	= year "-" month
	Alleen het formaat wordt hier gedefinieerd, niet welke waarden geldig zijn.
year	= digit digit digit digit
month	= digit digit
	januari=01, december=12
ntamx	= "ntamx=" prioriteit SP mailserver
prioriteit	= 2 * [digit] digit
	De mailservers met de laagste prioriteit worden als eerste geprobeerd.
mailserver	= { character }
	Een hostname conform RFC 1123 clause 2.1.

Legenda:

- [] mag herhaald voorkomen

- {} herhalend
- * maximum aantal herhalingen

Aandachtspunten:

- Het record mag geen "-teken bevatten.
- Er mogen maximaal 2 instanties van het ntatxt record aanwezig zijn.
- De startdate van het ene record moet groter zijn dan de enddate van het andere record (ofwel: de geldigheidperiode van de records mogen elkaar niet overlappen).
- De TTL waarde van elk record mag niet hoger zijn dan 86400 (1 etmaal).
- Indien de 'ntamx tag' niet wordt opgenomen, dan moeten e-mails verzonden worden naar de normale mailserver(s) van de organisatie.

Voorbeeld 1:

"v=NTA7516-1;startdate=2019-06;enddate=2020-09;provider=kenmerkNTAsysteem;ntamx=10 inc.webser.nl; ntamx=20 inc2.webser.nl"

Voorbeeld 2:

"v=NTA7516-1;startdate=2019-06;enddate=2020-09;provider=kenmerkNTAsysteem"

Contactpersoon NTA 7516: bij elke organisatie die voldoet aan NTA 7516 moet er een contactpersoon zijn die te bereiken is via het mail adres NTA7516@domeinnaam van de organisatie. Er wordt geen mailadres in het DNS bestand opgenomen.

In de mail header dient een tag opgenomen te worden die aangeeft dat het bericht een NTA 7516 bericht betreft. Voor deze mailberichten gelden onderstaande serveritems. Voor reguliere – niet NTA 7516 – mailberichten gelden onderstaande serveritems niet. Dit is van belang omdat er anders geen reguliere mail meer ontvangen kan worden op betreffende mailserver(s).

Tag in de header: 'X-NTA7516' met als content de 'provider' van de NTA dienst 'kenmerkNTAsysteem'.

Bij de communicatiedienst leverancier wordt een DNS TXT RR gepubliceerd met de volgende inhoud:
"version=NTA7516-1;startdate:2019-06;enddate:2020-09"

- **Aanvullende opmerkingen**

De waarden in het DNS TXT record en de header zijn hoofdlettergevoelig.

DNS hanteert de volgende regels voor hoofdlettergevoeligheid (Zie ook: https://tools.ietf.org/html/rfc4343):

- Host names (or 'labels'), such as example.com are case-insensitive
- DNS record types, such as 'A', and 'MX' are case sensitive
- Values in TXT and SPF records are case sensitive. All other DNS record types have case-insensitive values.

Een professional neemt een NTA record op en de communicatiedienst leverancier neemt ook een NTA record op. Indien een professional van meerdere communicatiedienst leveranciers diensten afneemt, elk met hun eigen NTA RR, dan beschikt de professional over meer dan één NTA RR. Het maakt voor de verzender echter niet uit welk record er geselecteerd wordt. Er hoeft daarom geen prioritiet in de records aangegeven te worden.

Als een certificering geforceerd beëindigd moet worden, dan dient de enddate aangepast te worden. Na een etmaal is deze aanpassing actief.

Een communicatiedienstleverancier kan ook mail voor professionals ontvangen. Bijvoorbeeld voor een bedrijfsarts. Dan is er een NTA professional RR en een NTA communicatiedienstleverancier RR. Afhankelijk van de rol die je hebt wordt dan het juiste NTA RR geselecteerd.

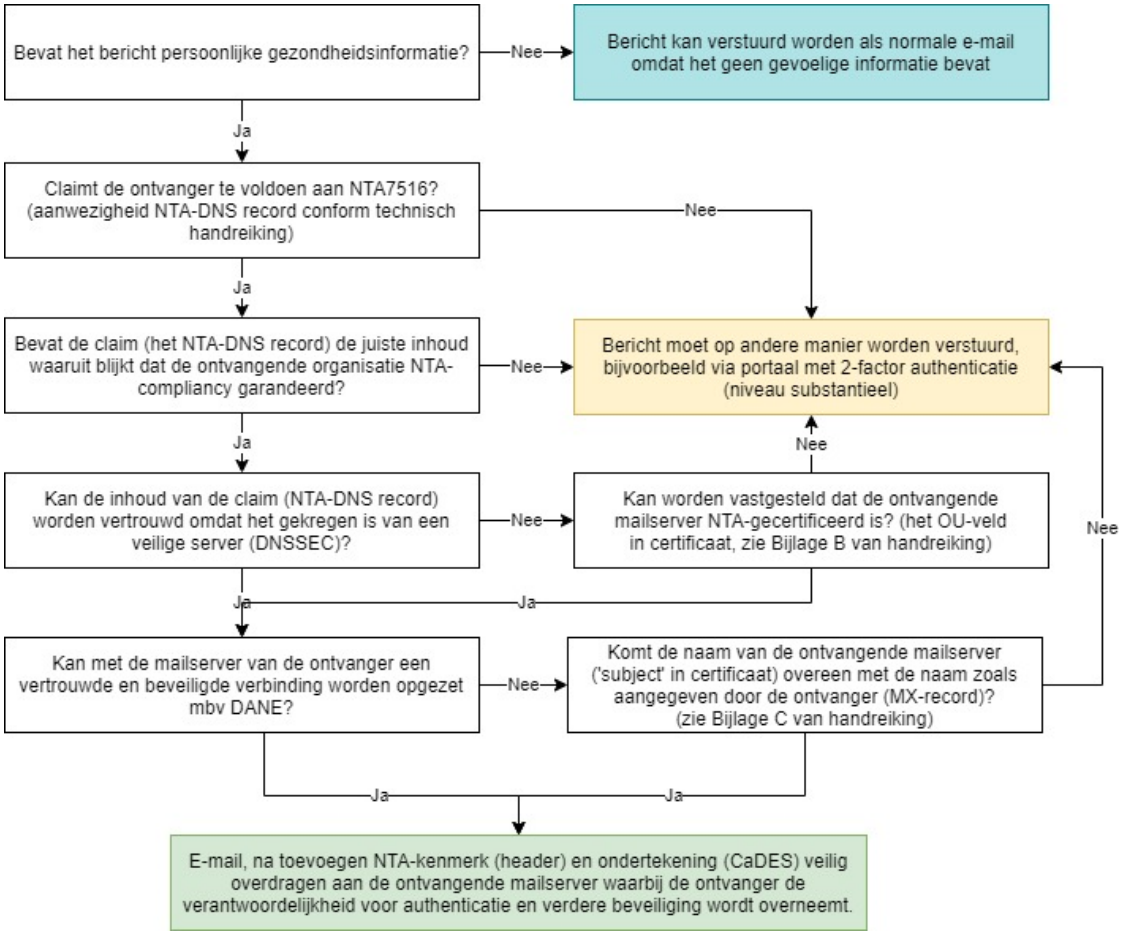
Serveritem 1	*De MSP van de verzendende server controleert of de beoogde ontvangende server het betreffende RR heeft gepubliceerd in diens DNS en of de geldigheid niet is verlopen. Als alles correct is, wordt het bericht naar de gespecificeerde server verzonden.*
Serveritem 2	*De MSP van de ontvangende server controleert of de beoogde verzendende server het betreffende RR heeft gepubliceerd in diens DNS en of de geldigheid niet is verlopen. Als alles correct is, wordt het bericht van de gespecificeerde server ontvangen.*

NB 1: Om het risico op het vervalsen van de resultaten van een DNS-verzoek te verkleinen, zorgen organisaties dat hun DNS is beveiligd met DNSSEC. Zie bijlage B voor een beschrijving van een tijdelijk alternatief voor organisaties waarvoor het (te) moeilijk is hun DNS met DNSSEC te beveiligen. Deze tijdelijke oplossing vormt een groeipad totdat er een volledige omarming van DNSSEC is.

NB 2: Omdat bij multikanaalcommunicatie de inhoud van een e-mailbericht niet in handen van een onbevoegde derde mag komen, zijn ook de standaarden van paragraaf *2.3 Gegevensvertrouwelijkheid* en de versleutelde opslag van berichten een vereiste. Daarnaast is ook het toepassen van CAdES voor digitale handtekening in paragraaf 2.4 verplicht, zodra er consensus over de implementatie van CAdES is.

Schema multikanaalcommunicatie

Om multikanaalcommunicatie te realiseren wordt het onderstaande logisch schema aangehouden door de MSA (verzendende mailserver). Dit sluit aan bij de beschrijving over multikanaalcommunicatie in dit hoofdstuk en Bijlage B en D.



2.2 *Check geldigheid DNS record*

De verzendende communicatiedienstaanbieder mag een bericht alleen maar ‘direct leesbaar’ overdragen aan de mailserver als de inhoud van het DNS-record aanwezig is en de inhoud geldig is. Dit betekent dat parsing volledig juist kan plaatsvinden, de *enddate* niet verstreken is en de ontvangende partij gebruik maakt van een dienst die NTA 7516 gecertificeerd is.

Hoe dit laatste moest worden uitgevoerd wordt uitgewerkt en op een later moment vastgesteld. Voorlopig wordt gebruik gemaakt van een certificatenlijst:

- Er wordt aan de DNS-record een signing toegevoegd, waarschijnlijk (indirect) gesigned met een (private) sleutel van een certificerende partij of de NEN. De verzendende dienst dient dan met de corresponderende publieke sleutel vast te stellen of het kenmerk juist ondertekend is en dus geldig is.
- Alle NTA leveranciers bieden hun certificaat voor mutual TLS aan op 1 plek (webpagina GitHub) en later via de DNS.
- De organisatorische en technische certificering wordt door de NEN beheerd.

Medio mei 2020 dienen alle communicatiediensten die meedoen met het project Veilige Mail gecertificeerd te zijn. Tot die tijd zal de publicatie van een DNS TXT record plaatsvinden zoals beschreven in paragraaf 2.1.

2.3 Herkomstbevestiging

Aan kunnen tonen dat verzender daadwerkelijk degene is die zich als zodanig uitgeeft (zie NTA 7516 paragraaf 6.1.5.).

Serveritem 3	*De MSP heeft DKIM en DMARC ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 zijn toegelicht.*
Clientitem 1	*De CSP heeft CAdES[3] geïmplementeerd op de wijze die in de betreffende passage van hoofdstuk 5 is toegelicht.*

DKIM maakt het mogelijk om het afzendadres van een e-mail te koppelen aan een domein/organisatie, op een manier die is te valideren door de ontvanger van de e-mail.

DMARC maakt het mogelijk om misbruik van domeinnamen bij e-mail te voorkomen.

CAdES biedt ondertekening door middel van een geavanceerde elektronische handtekening, wat vereist is op basis van het eIDAS betrouwbaarheidsniveau 'substantieel'.[4] Met de elektronische handtekening door CAdES worden de ‘bron en de integriteit’ van het bericht gewaarborgd.

2.4 Data-integriteit

De inhoud van het e-mailbericht (ook wel als body aangeduid) wordt volledig ongewijzigd afgeleverd bij de ontvanger met uitzondering van zogeheten meta-data of header records (zie NTA 7516 paragraaf 6.1.6.).

Serveritem 4	*De MSP heeft TLS ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 is toegelicht.*
Clientitem 2	*De CSP heeft TLS ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 is toegelicht.*

TLS realiseert een beveiligde verbindingen op de transportlaag van netwerkverkeer (zoals internet).

2.5 Onweerlegbaarheid verzender

De verzender kan niet ontkennen een door hem verzonden e-mailbericht te hebben verzonden (zie NTA 7516 paragraaf 6.1.7.).

Serveritem 5	*De MSP heeft DKIM, DMARC en SPF ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 zijn toegelicht.*

3 Zodra er consensus over de implementatie van CAdES is.

4 Uitvoeringsbesluit (EU) 2015/1506 van de Commissie van 8 september 2015 tot vaststelling van specificaties betreffende formaten van geavanceerde elektronische handtekeningen en geavanceerde zegels die door openbare instanties moeten worden erkend overeenkomstig respectievelijk artikel 27, lid 5, en artikel 37, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Clientitem 3	*De CSP van de verzendende client heeft CAdES[3] geïmplementeerd op de wijze die in de betreffende passage van hoofdstuk 5 is toegelicht.*

DKIM maakt het mogelijk om het afzendadres van een e-mail te koppelen aan een domein/organisatie, op een manier die is te valideren door de ontvanger van de e-mail.

DMARC en SPF maken het mogelijk om misbruik van domeinnamen bij e-mail te voorkomen.

CAdES biedt ondertekening door middel van een geavanceerde elektronische handtekening, wat vereist is op basis van het eIDAS betrouwbaarheidsniveau 'substantieel'.[5] Met de elektronische handtekening door CAdES worden de 'bron en de integriteit' van het bericht gewaarborgd.

2.6 *Gegevensvertrouwelijkheid*

De inhoud van een e-mailbericht mag niet in handen van een onbevoegde derde komen; beveiliging in storage (zie NTA 7516 paragraaf 6.1.9.).

Serveritem 6	*De MSP heeft TLS, SMTP, IMAP, STARTTLS en DANE ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 zijn toegelicht.*
Clientitem 4	*De CSP heeft TLS, SMTP, IMAP en DANE[6] ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 zijn toegelicht.*
Clientitem 5	*Indien het beheer van een verzendende client is uitbesteed aan een derde partij, moet de uitbestedende partij een verwerkersovereenkomst (als bedoeld in de AVG) met die CSP sluiten.*

TLS realiseert een beveiligde verbindingen op de transportlaag van netwerkverkeer (zoals internet).

IMAP wordt aanbevolen voor synchronisatie tussen e-mailserver en ontvangende e-mailclient.

STARTTLS maakt het mogelijk om SMTP-verkeer over een met TLS versleutelde verbinding te laten lopen.

DANE voorkomt aanvallen waarbij een aanvaller zich uitgeeft voor de ontvangende e-mailserver en STARTTLS blokkeert om zo toegang tot de niet versleutelde berichten te krijgen of berichten te vervalsen. Zie bijlage C voor een tijdelijk alternatief om veilig transport te realiseren als het voor organisaties niet mogelijk is hun inkomende mailserver te beveiligen met DANE. Deze tijdelijke oplossing vormt een groeipad totdat er een volledige omarming van DANE is.

- **Versleutelde opslag berichten**

De berichten dienen versleuteld opgeslagen te worden op de servers van de (verzendende en ontvangende) communicatiedienstaanbieder. Hierbij kan de communicatiedienstaanbieder of professional zelf kiezen voor een versleutelings-/encryptiemethodiek, mits de versleutelde opslag

5 Uitvoeringsbesluit (EU) 2015/1506 van de Commissie van 8 september 2015.

6 Enkel indien de client direct middels SMTP communiceert. Dit zal veelal niet het geval zijn. Dan is DANE alleen een serveritem.

gebeurt conform een standaard die op de lijst van het Forum Standaardisatie staat[7]. Op dit moment is dit voor encryptie Advanced Encryption Standard **(**AES). De AES biedt de mogelijkheid om sleutellengtes van 128, 192 of 256 bits te kiezen.

Indien gekozen is voor een andere encryptiestandaard dient aangetoond te worden door de communicatiedienstaanbieder dat deze minimaal gelijke veiligheid biedt als de standaarden op de lijst van het Forum Standaardisatie.

Een essentieel onderdeel van goede versleuteling is verantwoord sleutelbeheer. Het is sterk aanbevolen om berichten te versleutelen met een unieke sleutel, waarbij deze sleutel niet (leesbaar) bewaard/opgeslagen wordt door de communicatiedienstenaanbieder. Bij een afwijkende implementatie dient beschreven te worden hoe invulling wordt gegeven aan de gegevensvertrouwelijkheidseis uit NTA 7516 paragraaf 6.1.9.

2.7 Communicatievertrouwelijkheid

Informatie *over* een e-mailbericht (zogenaamde meta-data) mag niet in handen van een onbevoegde derde komen. Beveiliging in transit (zie NTA 7516 paragrafen 6.1.11. en 6.2.2.2.).

Serveritem 7	*De MSP heeft TLS, SMTP en IMAP ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 zijn toegelicht.*
Clientitem 6	*De CSP heeft TLS, SMTP en IMAP ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 zijn toegelicht.*
Clientitem 7	*Indien header-informatie onbeschermd wordt verzonden, verwijdert de CPS ten minste de headers genoemd in bijlage A.*

TLS realiseert een beveiligde verbindingen op de transportlaag van netwerkverkeer (zoals internet).

SMTP dient om e-mails uit te wisselen tussen e-mailservers en tussen de verzendende client en de bijbehorende server.

IMAP wordt aanbevolen voor synchronisatie tussen e-mailserver en ontvangende e-mailclient.

Als de informatie uit te verwijderen headers gewenst is, dan kan deze aan de body worden toegevoegd en zo (beveiligd) worden verzonden.

2.8 Internationaal ad-hocberichtenverkeer

Communicatie en informatie over communicatie mag niet (onbeschermd) buiten de Europese Economische Ruimte (EER) en zogeheten adequate landen geraken (zie NTA 7516 paragraaf 6.1.13.).

Serveritem 8	*De MSP heeft STARTTLS, SPF, DKIM en CAdES[8] ten behoeve van de e-maildienst geïmplementeerd op de wijze die in de betreffende passages van hoofdstuk 5 zijn toegelicht.*

7 https://www.forumstandaardisatie.nl/open-standaarden/lijst

8 Zodra er consensus over de implementatie van CAdES is.

Persoonsgegevens worden beschermd door onder andere de AVG. Die biedt – zonder aanvullende maatregelen – de ruimte om persoonsgegevens te verwerken binnen de EER en landen met een zogenaamd wettelijk adequaat beschermingsniveau.[9]

De AVG verlangt daarom passende maatregelen. De Autoriteit Persoonsgegevens heeft aangegeven STARTTLS-SPF-DKIM als passend te beschouwen.[10]

STARTTLS maakt het mogelijk om SMTP-verkeer over een met TLS versleutelde verbinding te laten lopen.

SPF controleert of de mailserver die een e-mail wil versturen namens een domein deze e-mail mag verzenden.

DKIM maakt het mogelijk om het afzendadres van een e-mail te koppelen aan een domein/organisatie, op een manier die is te valideren door de ontvanger van de e-mail.

CAdES maakt het mogelijk de onweerlegbaarheid van de verzender vast te stellen.

9 De EER bestaat uit de lidstaten van de EU, Noorwegen, IJsland en Liechtenstein. Tot de (ongeclausuleerde) adequate landen behoren (medio 2019): Andorra, Argentinië, Faeroer Eilanden, Guernsey, Israël, Japan, Jersey, het eiland Man, Nieuw-Zeeland, Uruguay en Zwitserland. Met Zuid-Korea zijn onderhandelingen gaande.
Voor de Verenigde Staten geldt dat de betreffende partij(en) deelnemer moeten zijn aan het Privacy Shield raamwerk, waardoor het in het licht van NTA 7516 niet als de andere adequate landen kan worden behandeld. Iets vergelijkbaars geldt voor Canada, waar de adequaatheidsbeslissing slechts geldt voor private partijen.

10 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens?qa=starttls

3 Handreiking optionele eisen

In dit hoofdstuk worden voorstellen gedaan om aan de resterende eisen van NTA 7516 te voldoen. Naast de eis in 3.1, dient een communicatiedienst aan minimaal één van de eisen in 3.2 tot en met 3.13 te voldoen.

3.1 Veilige informatievoorziening

De aangeboden dienst zal aantoonbaar veilig zijn. (Zie NTA 7516 paragraaf 7.5.)

Serveritem 9	*De MSP heeft een geldig certificaat volgens ISO/IEC 27001:2017 [11] dan wel NEN 7510-1:2017 [12], die betrekking heeft op de aangeboden e-maildiensten, wat blijkt uit de bij het certificaat behorende verklaring van toepasselijkheid, gebaseerd op de maatregelen set uit ISO/IEC 27002[13] dan wel NEN 7510-2[14].*
Clientitem 8	*De CSP heeft een geldig certificaat voor ISO/IEC 27001:2017 dan wel NEN 7510:2017, die betrekking heeft op de aangeboden e-maildiensten, wat blijkt uit de bij het certificaat behorende verklaring van toepasselijkheid, gebaseerd op de maatregelen set uit ISO/IEC 27002 dan wel NEN 7510-2.*

De dienstafnemer wil zekerheid hebben dat de gegevens in goede handen zijn bij de MSP respectievelijk CSP. Het ISO/IEC 27001-certificaat biedt daarvoor een goed houvast. ISO/IEC 27002 behandelt algemene beveiligingsmaatregelen, ISO/IEC 27017 bevat aanvullende maatregelen voor clouddiensten.

3.2 Minimale beschikbaarheid, maximale uitvalduur en maximaal gegevensverlies

E-mailcommunicatie is een bepaalde hoeveelheid van de tijd mogelijk. Uitval van e-mailcommunicatie mag niet langer dan een bepaalde periode duren en er mag over een periode geen e-mailcommunicatie verloren raken (niet aankomen bij de beoogde ontvanger). (Zie NTA 7516 paragrafen 6.1.2, 6.1.3 en 6.1.4.)

Serveritem 10	*De MSP heeft aantoonbaar Service continuity and availability management van ISO/IEC 20000 (of vergelijkbaar) geïmplementeerd, wat blijkt uit een ten hoogste twee jaar eerder gegeven verklaring van een ter zake deskundige derde partij, of heeft een geldig certificaat voor ISO/IEC 20000 met een bij het certificaat behorende verklaring van toepasselijkheid.*
Clientitem 9	*De CSP heeft aantoonbaar Service continuity and availability management van ISO/IEC 20000 (of vergelijkbaar) geïmplementeerd, wat blijkt uit een ten hoogste twee jaar eerder gegeven verklaring van een ter zake deskundige derde partij, of heeft een geldig certificaat voor ISO/IEC 20000 met een bij het certificaat behorende verklaring van toepasselijkheid.*

11 NEN-EN-ISO/IEC 27001:2017 Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen

12 NEN 7510-1:2017 Medische informatica – Informatiebeveiliging in de zorg – Deel 1: Managementsysteem

13 NEN-EN-ISO/IEC 27002:2017 Informatietechnologie – Beveiligingstechnieken – Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging

14 NEN 7510-2:2017 Medische informatica – Informatiebeveiliging in de zorg – Deel 2: Beheersmaatregelen

Serveritem 11	*De MSP kan beredeneerd aantonen dat de gerealiseerde implementatie in staat is om de door de dienstafnemer vastgestelde beschikbaarheidscriteria te realiseren.*
Clientitem 10	*De CSP kan beredeneerd aantonen dat de gerealiseerde implementatie in staat is om de door de dienstafnemer vastgestelde beschikbaarheidscriteria te realiseren.*

ISO/IEC 20000 (of vergelijkbaar) komt overeen met ITIL Service Management. Onderdeel hiervan is *Service continuity and availability management*. Naleving hiervan is instrumenteel in het kunnen behalen van de beschikbaarheidscriteria die de dienst afnemende professional heeft gesteld.

3.3 Toegangsvertrouwelijkheid

De ontvanger kan een bericht uitsluitend lezen nadat een passende authenticatie van diens identiteit heeft plaatsgevonden. (Zie NTA 7516 paragraaf 6.1.10.)

Clientitem 11	*De CSP dwingt bij ontvangst van een e-mailbericht authenticatie van de identiteit van de geadresseerde op basis van eIDAS af.*
Clientitem 12	*Bij verstrekking van de authenticatiemiddelen aan gebruikers moet de CSP eIDAS substantieel toepassen.*
Clientitem 13	*Verstrekking van authenticatiemiddelen aan (werknemers van) professionals moet aan eIDAS hoog voldoen.*

Authenticatie van een identiteit (met andere woorden: inloggen) kan op basis van single sign-on mechanismen, mits de oorspronkelijke inlogwijze aan de genoemde eisen voldoet.

Twee factor authenticatie (2FA) houdt in dat ten minste twee verificatiemethoden moeten gebruikt van de drie mogelijke methoden: op basis van iets wat iemand weet (bijvoorbeeld een wachtwoord), op basis van iets wat iemand heeft (bijvoorbeeld een pasje of een token) en op basis van iets wat iemand is (met name biometrie[15]). Een veel gebruikt oplossing is een wachtwoord (wat je weet) en een sms-token op een mobiele telefoon (wat je hebt). Het token dat via sms wordt verstuurd, is dan uniek bij elke volgend gebruik (een zogenaamde one time passcode). De mobiele telefoon moet wel normaliter worden beveiligd (minimaal met een pincode) en het token mag niet worden getoond zonder de telefoon te hebben ontgrendeld. Laptops kunnen in toenemende mate op vergelijkbare wijze worden ingezet.

Identiteitsverificatie bij verstrekking van authenticatiemiddelen mag op afstand plaatsvinden. DigiD met betrouwbaarheidsniveau substantieel (controle identiteitsbewijs) is hiervoor geschikt.[16] Indien dit voor partijen nog niet beschikbaar is, kan verificatie-op-afstand niet plaatsvinden.

Identiteitsverificatie bij verstrekking van authenticatiemiddelen hoeft niet door de CSP zelf te worden uitgevoerd, maar mag ook door een andere partij namens haar worden gedaan. Bijvoorbeeld tijdens het aannameproces bij de afdeling personeelszaken van de gebruikende partij (ziekenhuis, gemeente etc.), die de dienst van de CSP afneemt.

15 Biometrie wordt, onder meer vanwege het onveranderlijke karakter, ook wel gebruikt ter identificatie.

16 Zie https://www.digid.nl/over-digid/app/controle-identiteitsbewijs/

One time password (OTP)

Verzenders dienen zelf de afweging te maken of zij gebruik willen maken van een wachtwoord dat op een specifiek device voor een beperkte periode, bijvoorbeeld een dag of een week, geldig blijft (OTP). In geval van een eventueel datalek zal worden getoetst of door verzender voldoende maatregelen zijn genomen om het datalek te voorkomen in relatie tot de ernst van het datalek. Indien gebruik wordt gemaakt van een OTP dienen de volgende punten meegenomen te worden:

- vanuit de Zorgkoepels geldt hier dat de professional moet kunnen bepalen of deze optie wel of niet wordt aangeboden;
- vanuit Patiëntenfederatie Nederland geldt daarnaast dat een patiënt zelf moet kunnen kiezen of hij / zij van de geboden optie gebruik wil maken.

3.4 Continuïteit van ad-hocberichtenverkeer – beantwoorden

Communicatie gestart door een professional moet door een ontvangende persoon veilig kunnen worden beantwoord (zie NTA 7516 paragraaf 6.1.14.).

Clientitem 14	*De CSP biedt een mogelijkheid waarmee een veilig ontvangen en gelezen bericht, veilig kan worden beantwoord en teruggezonden naar de oorspronkelijke verzender, die het veilig door hem ontvangen bericht ook veilig kan lezen.*

3.5 Continuïteit van ad-hocberichtenverkeer – doorsturen

Communicatie gestart door een professional moet door een ontvangende persoon veilig kunnen worden voortgezet. (Zie NTA 7516 paragraaf 6.1.15.)

Clientitem 15	*Afhankelijk van de eis ter zake van de professional, moet de CSP een mogelijkheid bieden waarmee een veilig ontvangen en gelezen bericht, veilig kan worden doorgestuurd naar een derde die het veilig door hem ontvangen bericht ook veilig kan lezen.*

3.6 Veiligheid als gemak

Security by default (zie NTA 7516 paragraaf 6.1.16.).

Serveritem 12	*De MSP draagt er zorg voor dat als verschillende opties/instelmogelijkheden beschikbaar zijn, standaard is gekozen voor de optie/instelmogelijkheid die leidt tot de grootste veiligheid, ook wanneer aanvullende mogelijkheden worden gebruikt.*
Clientitem 16	*De CSP draagt er zorg voor dat als verschillende opties/instelmogelijkheden beschikbaar zijn, standaard is gekozen voor de optie/instelmogelijkheid die leidt tot de grootste veiligheid, ook wanneer aanvullende mogelijkheden worden gebruikt.*

Security by default gaat standaard uit van de veiligste instellingen, zodat elke minder veiligere instelling het gevolg moet zijn van (bewust) menselijk handelen.

3.7 Leesbaarheid

Verzonden bericht worden door de ontvanger direct binnen zijn client (of binnen een portaal) gelezen, zonder gebruik te hoeven maken van (te installeren) viewers en dergelijke; hieruit volgt het gebruik van open, breed gebruikte standaarden (zie NTA 7516 paragraaf 6.1.17.).

Clientitem 17	*De CSP die communicatie verzorgt met personen, past EN 301 549[17] toe.*

EN 301 549 is een standaard die toegankelijkheid bevordert tot IT-diensten voor mensen met een functiebeperking.

3.8 Eigen kopie

De ontvanger van een bericht kan een bericht en/of haar bijlagen opslaan (a) op een zelfgekozen locatie en (b) in een breed toegankelijk formaat. (Zie NTA 7516 paragraaf 6.1.18.)

Clientitem 18	*De CSP biedt de mogelijkheid om een bericht of een bijlage op te slaan op een zelfgekozen locatie en in een breed toegankelijk formaat.*

Tot zelfgekozen locaties kan ook een PGO of een andere cloud-gebaseerde of netwerklocatie horen.

Forum Standaardisatie hanteert een aantal documentformaten als zogenaamd ‘open’ formaten,[18] waarvan de volgende breed worden gebruikt: PDF (voor ‘traditionele’ documenten), SVG (voor afbeeldingen),en XML en CSV (voor gestructureerde gegevensverzamelingen).

17 EN 301 549 – Accessibility requirements suitable for public procurement of ICT products and services in Europe, zie: https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf

18 https://www.forumstandaardisatie.nl/open-standaarden/lijst?f%5B0%5D=field_standard_domain%3A6&f%5B1%5D=field_keywords%3A65

4 Overige suggestie(s)

4.1 Dossierkoppeling

Berichten kunnen eenvoudig aan een dossier worden toegevoegd: met minimale inspanning van de professional kan een bericht geschikt worden gemaakt voor opname in een dossier. (Zie NTA 7516 paragraaf 6.1.19.)

Clientitem 19	*De CSP van professional is in staat om (a) te herkennen of een bericht mogelijk persoonsgebonden medisch-inhoudelijke informatie bevat, (b) de identiteit van de betreffende persoon te suggereren (waarna deze die identiteit kan accepteren, wijzigen of afwijzen) en (c) na geaccepteerde of gewijzigde identiteit het bericht naar een daemon (of vergelijkbaar) te versturen die zorgt draagt voor de feitelijke toevoeging aan het betreffende dossier.*

Ad (a): Herkenning kan geschieden door een bepaalde hoeveelheid medisch jargon te detecteren, alsmede attributen die een persoon kunnen identificeren (zoals naam, adres, BSN, patiëntnummer, geboortedatum et cetera).

Ad (b): De suggestie zal normaliter in de vorm van een pop-up worden gepresenteerd, waarbij de professional zijn/haar keuze moet aangeven.

Ad (c): De CSP is niet verantwoordelijk voor opname in een dossiersysteem, het moet uitsluitend de geselecteerde en geïdentificeerde berichten aan het dossiersysteem kunnen aanbieden.

In hoeverre gekoppeld wordt met een dossiersysteem (bijvoorbeeld door de ad b-keuze te koppelen aan reeds bekende identiteiten) is aan marktpartijen zelf.

5 Implementatie technische standaarden

Een aantal van de volgende standaarden zijn beschreven in zogeheten RFCs. De vindplaats daarvan is https://tools.ietf.org/html/rfcNNNN, waarbij 'NNNN' staat voor de viercijferige identificatie van de betreffende RFC. Wanneer een RFC verwijst naar updates ("Updated by:"), dan behoren die updates ook tot die standaard.

5.1 AES

Standaard: FIPS 197

Volledige naam: *Advanced Encryption Standard*

Betreft: Server.

Werking: De AES-standaard is een versleutelingstechniek voor de bescherming van de vertrouwelijkheid van opgeslagen en verzonden data en is de vervanger van de verouderde DES standaard. AES wordt zowel binnen Nederland als wereldwijd zeer veel en op zeer veel verschillende wijzen gebruikt. AES is ontwikkeld door het National institute of technology and standards (NIST), een federaal agentschap binnen het U.S. Departement of Commerce en is inmiddels ook opgenomen door ISO.

Implementatie: AES is een versleutelingstechniek voor de bescherming van de vertrouwelijkheid van de opgeslagen en verzonden data.

5.2 CAdES

Standaard: ETSI TS 101 733 (versie 2.2.1)

Volledige naam: *CMS Advanced Electronic Signatures (CAdES is afkomstig van ETSI en kan worden gevonden via https://www.etsi.org/standards).*

Betreft: Client.

Werking: CAdES biedt een geavanceerde elektronische handtekening conform eIDAS, waardoor een bericht uniek wordt gekoppeld aan de ondertekenaar, de ondertekenaar kan worden geïdentificeerd, de ondertekenaar (met uitsluiting van alle anderen) kan besluiten over ondertekening en wijzigingen in een bericht ná ondertekening kunnen worden vastgesteld. De ontvangende client moet controleren op de aanwezigheid van een geldige ondertekening.

Implementatie: CAdES-BES (Basic Electronic Signature) wordt toegepast op verzendende en ontvangende clients.

5.3 DANE

Standaard: RFC 7672

Volledige naam: *SMTP Security via Opportunistic DNS-Based Authentication of Named Entities*

Betreft: Server.

Werking: Bij het maken van een veilige verbinding naar een onbekende partij is een onlinecontrole op de authenticiteit van de verzendende partij en de eindbestemming vereist. Dit geschiedt door middel van (gepubliceerde) certificaten. DANE maakt authenticatie van de eindbestemming mogelijk, doordat de eigenaar van een domein via een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline certificaten aan te reiken. Hierdoor kan real-time een controle worden gedaan op de authenticiteit van de eindbestemming en of de server-to-server-verbinding legitiem is en niet wordt gemanipuleerd.

Implementatie: DANE moet worden toegepast op alle domeinservers van de ontvangende organisatie. Zie voor details https://www.forumstandaardisatie.nl/standaard/starttls-en-dane. Publicatie in DNS TLSA RR moet gebruik maken van DANE-EE(3) SPKI(1) SHA2-256(1).

5.4 DKIM

Standaard: RFC 6367

Volledige naam: *DomainKeys Identified Mail Signatures*

Betreft: Server.

Werking: DKIM koppelt een e-mailbericht aan een domeinnaam met behulp van een digitale handtekening. Het stelt de ontvanger in staat om te bepalen welke domeinnaam (en daarmee welke achterliggende organisatie) verantwoordelijk is voor het zenden van de e-mail.

Met behulp van DKIM wordt een bericht getekend, waarbij verificatie mogelijk is door middel van de publieke sleutel die op een mailserver staat.

Implementatie: DKIM wordt toegepast op alle verzendende en ontvangende e-mailservers. Het DKIM-record moet de strings «a=rsa-sha256» en «c=simple/simple» bevatten.

5.5 DMARC

Standaard: RFC 7489

Volledige naam: *Domain-based Message Authentication, Reporting and Conformance*

Betreft: Server en domeinen (zie hieronder).

Werking: DMARC maakt het mogelijk om misbruik van domeinnamen bij e-mail te voorkomen door beleid in te stellen over de manier hoe een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie.

Een DMARC-policy stelt een verzender in staat aan te geven dat berichten zijn beschermd met SPF of DKIM (zie aldaar) en meldt de ontvanger wat te doen als één van deze authenticatiemethoden faalt. DMARC biedt tevens een methode om de ontvanger aan de verzender te laten rapporteren of de verzending is gelukt of niet. DMARC-policies worden gepubliceerd in de DNS als text resource records en vertellen de ontvanger wat te doen met berichten die niet door middel van DKIM en SPF (zie aldaar) kunnen worden geauthentiseerd.

Implementatie: DMARC wordt toegepast op alle relevante domeinnamen (inclusief domeinen waarmee niet wordt gemaild), én op alle ontvangende e-mailservers. Het DMARC-record moet de string «P=reject» of «p=quarantaine» bevatten.

5.6 IMAP

Standaard: RFC 3501 en RFC 8314

Volledige naam: *Internet Message Access Protocol*

Betreft: Client en server.

Werking: IMAP draagt zorg voor synchronisatie tussen e-mailserver en e-mail client en dat het e-mailbericht op de server aanwezig blijft.

Implementatie: IMAP4 revisie 1 moet zijn geïmplementeerd op de clients en de servers. Normaal IMAP-verkeer verloopt via poort 143, eventueel SSL-versleuteld IMAP-verkeer verloopt via poort 993.

5.7 SMTP

Standaard: RFC 5321 en RFC 2487

Volledige naam: *Simple Mail Transfer Protocol*

Betreft: Client en server.

Werking: SMTP zorgt voor het versturen van een e-mail bericht tussen e-mailservers en tussen de verzendende client en de bijbehorende server.

Implementatie: SMTP wordt gebruikt over verbindingen die met TLS (zie aldaar) zijn beveiligd. Bij client authentication wordt gebruik gemaakt van het EHLO-commando en gedurende authenticatie moet het mechanisme CRAM-MD5 worden gebruikt.

5.8 SPF

Standaard: RFC 7208

Volledige naam: *Sender Policy Framework*

Betreft: Server en domeinen (zie hieronder).

Werking: SPF controleert of de mailserver die een e-mail wil versturen namens een domein deze e-mail mag verzenden, door de authenticiteit van de domeinnaam in het afzenderadres van de ontvangen mail herleidbaar te maken via de in DNS gepubliceerde IP-adressen van de verzendende mailserver(s).

Implementatie: SPF wordt toegepast op alle relevante domeinnamen (inclusief domeinen waarmee niet wordt gemaild), én op alle ontvangende e-mailservers (meer precies: op elk domein met een A-record of een MX-record). Het SPF-record moet het(de) domeinnaam + ip-adres(sen) van de verzendende server(s) en de string «-all» bevatten.

5.9 STARTTLS

Standaard: RFC 3207 en RFC 3848

Volledige naam: *SMTP Service Extension for Secure SMTP over Transport Layer Security* en *ESMTP and LMTP Transmission Types Registration* respectievelijk.

Betreft: Server.

Werking: E-mails worden door de e-mailserver van de verzendende partij verstuurd naar de e-mailserver van de ontvangende partij met de SMTP-standaard. STARTTLS maakt het mogelijk om SMTP-verkeer over een met TLS versleutelde verbinding te laten lopen.

Implementatie: Alle verzendende e-mailservers en ontvangende e-mailservers moeten STARTTLS ondersteunen. STARTTLS kent een zwakheid die met behulp van DANE (zie aldaar) wordt afgedicht; DANE moet dus ook worden geïmplementeerd.

5.10 TLS

Standaard: TFC 5246 en RFC 8446

Volledige naam: *The Transport Layer Security (TLS) Protocol Version 1.2* en *Transport Layer Security (TLS) Protocol Version 1.3* respectievelijk.

Betreft:	Client en server.
Werking:	TLS zorgt voor beveiligde verbindingen op de transportlaag van een netwerk (zoals internet) en biedt een beveiligde basis, waar applicatie protocollen als IMAP (mailuitwisseling) op kunnen bouwen en gebruik van kunnen maken. Het maakt gebruik van certificaten om zekerheid te bieden over de identiteit van beide communicerende partijen voordat die communicatie plaatsvindt.
Implementatie:	MSP respectievelijk CSP gebruikt TLS conform de meest recente beveiligingsrichtlijnen van het NCSC, waarbij uitsluitend opties met de status 'goed' worden gebruikt.[19]

19 Op het moment van schrijven is de meest recente versie 2.0 dd. 23 april 2019. Relevante opties daarin met de status 'goed' zijn:

sleuteluitwisseling	ECDHE
certificaatsverificatie	ECDSA of RSA,
bulkversleuteling	AES_256_GCM, CHACHA20_POLY1305 of AES_128_GCM
hashing	(HMAC-)SHA-512, (HMAC-)SHA-384 of (HMAC-)SHA-256
RSA sleutellengte	3072 bit of meer
compressie	geen
renogation	uit
0-RTT	uit
OCSP stapling	aan
cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 OF TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Bijlage A Ongewenste headers

(prescriptief)

Mail-berichten bevatten, naast de inhoud zelf, headers die uiteenlopende doelen mogelijk kunnen maken. Maar tegelijk kunnen ze zaken weergeven die de vertrouwelijkheid van het berichtenverkeer kunnen bedreigen. Om die reden moeten ten minste onderstaande headers door de verzendende CSP worden geschrapt (de gronden zijn in de tweede kolom weergegeven). Zie Clientitem 7. Dit is alleen van toepassing header-informatie van op e-mails die onbeschermd worden verzonden.

Header	*grond voor verwijdering*
Accept-Language	taal (onnodig binnen NTA 7516)
Apparently-To	voorlopige header, niet in normaal gebruik
ARC-Authentication-Results	voorlopige header, niet in normaal gebruik
ARC-Message-Signature	voorlopige header, niet in normaal gebruik
ARC-Seal	voorlopige header, niet in normaal gebruik
Base	ingetrokken
Content-Base	ingetrokken
Content-Language	taal (onnodig binnen NTA 7516)
DL-Expansion-History	mailing lists (buiten scope)
Downgraded-Bcc	ingetrokken
Downgraded-Cc	ingetrokken
Downgraded-Disposition-Notification-To	ingetrokken
Downgraded-From	ingetrokken
Downgraded-Mail-From	ingetrokken
Downgraded-Rcpt-To	ingetrokken
Downgraded-Reply-To	ingetrokken
Downgraded-Resent-Bcc	ingetrokken
Downgraded-Resent-Cc	ingetrokken
Downgraded-Resent-From	ingetrokken
Downgraded-Resent-Reply-To	ingetrokken
Downgraded-Resent-Sender	ingetrokken
Downgraded-Resent-To	ingetrokken
Downgraded-Return-Path	ingetrokken
Downgraded-Sender	ingetrokken
Downgraded-To	ingetrokken
EDIINT-Features	voorlopige header, niet in normaal gebruik
Eesst-Version	voorlopige header, niet in normaal gebruik
Errors-To	voorlopige header, niet in normaal gebruik
Form-Sub	voorlopige header, niet in normaal gebruik
Jabber-ID	voorlopige header, niet in normaal gebruik
Language	taal (onnodig binnen NTA 7516)
List-Archive	mailing lists (buiten scope)
List-Help	mailing lists (buiten scope)
List-ID	mailing lists (buiten scope)

Header	*grond voor verwijdering*
List-Owner	mailing lists (buiten scope)
List-Post	mailing lists (buiten scope)
List-Subscribe	mailing lists (buiten scope)
List-Unsubscribe	mailing lists (buiten scope)
List-Unsubscribe-Post	mailing lists (buiten scope)
MMHS-Acp127-Message-Identifier	bedoeld voor militair gebruik
MMHS-Authorizing-Users	voorlopige header, niet in normaal gebruik
MMHS-Codress-Message-Indicator	bedoeld voor militair gebruik
MMHS-Copy-Precedence	bedoeld voor militair gebruik
MMHS-Exempted-Address	bedoeld voor militair gebruik
MMHS-Extended-Authorisation-Info	bedoeld voor militair gebruik
MMHS-Handling-Instructions	bedoeld voor militair gebruik
MMHS-Message-Instructions	bedoeld voor militair gebruik
MMHS-Message-Type	bedoeld voor militair gebruik
MMHS-Originator-PLAD	bedoeld voor militair gebruik
MMHS-Originator-Reference	bedoeld voor militair gebruik
MMHS-Other-Recipients-Indicator-CC	bedoeld voor militair gebruik
MMHS-Other-Recipients-Indicator-To	bedoeld voor militair gebruik
MMHS-Primary-Precedence	bedoeld voor militair gebruik
MMHS-Subject-Indicator-Codes	bedoeld voor militair gebruik
Organization	informational, dus niet vereist
Privicon	voorlopige header, niet in normaal gebruik
Resent-Reply-To	ingetrokken
SIO-Label	voorlopige header, niet in normaal gebruik
SIO-Label-History	voorlopige header, niet in normaal gebruik
X-Archived-At	voorlopige header, niet in normaal gebruik
X-Mittente	voorlopige header, niet in normaal gebruik
X-Ricevuta	voorlopige header, niet in normaal gebruik
X-Riferimento-Message-ID	voorlopige header, niet in normaal gebruik
X-TipoRicevuta	voorlopige header, niet in normaal gebruik
X-Trasporto	voorlopige header, niet in normaal gebruik
X-VerificaSicurezza	voorlopige header, niet in normaal gebruik
X400-Content-Identifier	X400 is vervangen door SMTP
X400-Content-Return	X400 is vervangen door SMTP
X400-Content-Type	X400 is vervangen door SMTP
X400-MTS-Identifier	X400 is vervangen door SMTP
X400-Originator	X400 is vervangen door SMTP
X400-Received	X400 is vervangen door SMTP
X400-Recipients	X400 is vervangen door SMTP
X400-Trace	X400 is vervangen door SMTP

Bijlage B Veilig transport bij ontbreken DNSSEC

Deze bijlage beschrijft een manier om een veilig transport tussen de verzendende en ontvangende mailservers van de organisatie te realiseren als het voor de ontvangende organisatie (te) moeilijk is om de DNS van de organisatie te beveiligen met DNSSEC. Hoewel meer dan de helft van .nl[20] domeinen al DNSSEC heeft en aanzetten van of overstappen naar een registrar die DNSSEC ondersteunt relatief eenvoudig geregeld kan worden[21], zijn er signalen uit het veld dat DNSSEC voor met name kleine organisaties een (te) grote inspanning vraagt om toe te passen.

Zonder DNSSEC is het niet mogelijk zeker te weten dat het antwoord van het DNS op het verzoek niet vervalst is. Daarmee kan de authenticiteit van de inhoud van het opgevraagde TXT-record zoals beschreven in paragraaf 2.1 niet gegarandeerd worden. Dit vormt alleen een risico voor het antwoord in de 'ntamx' velden, waarbij het niet zeker is dat de opgegeven mailserver in het antwoord de juiste mailserver betreft.

Om dit risico te mitigeren wordt tijdelijk een alternatieve implementatie ondersteund voor organisaties die (nog) geen DNSSEC hebben. Hiervoor moeten zij wel gebruik maken van een NTA 7516-gecertificeerde communicatiedienstenaanbieder voor de afhandeling van inkomende e-mail. Deze aanbieder dient namelijk een certificaat te hebben dat, in het Organizational Unit veld (OU-veld), een kenmerk bevat waarmee gevalideerd kan worden dat deze ontvangende server ook daadwerkelijk een gecertificeerde dienst betreft. Hoe dit kenmerk er uit ziet en hoe de geldigheid hiervan gevalideerd kan worden, wordt op een later moment vastgesteld.

Verificatiestappen voor verzender

De verzendende mailserver dient de volgende stappen zorgvuldig te controleren en te volgen.

1. De verzender bevraagt de DNS van de ontvanger op aanwezigheid van het NTA-record zoals beschreven in paragraaf 2.1;
2. De verzender maakt verbinding met de mailserver zoals opgegeven in antwoord van de vorige stap;
3. De verbinding moet altijd gebruik maken van STARTTLS;
4. Het servercertificaat moet geldig zijn. Dat wil zeggen: volgens gangbare X.509 validatiestappen zoals inachtneming van vervaldatum en chain of trust naar een vertrouwd rootcertificaat;
5. De waarde in het OU-veld van het servercertificaat moet worden gevalideerd op geldigheid (zoals eerder aangegeven, wordt later vastgesteld hoe dit dient te gebeuren).

Veilige communicatie volgens de voorgestelde methode kan niet worden opgezet indien een van bovenstaande stappen faalt.

[20] https://stats.sidnlabs.nl/nl/dnssec.html
[21] https://www.sidn.nl/faq/dnssec

Inspanning voor ontvanger

De ontvanger dient een dienst af te nemen bij een NTA 7516-gecertificeerde communicatiedienstenaanbieder en in de DNS van de organisatie de informatie op te nemen zoals aangegeven in paragraaf 2.1.

Bijlage C Veilig transport bij ontbreken DANE

Deze bijlage beschrijft een manier om de authenticiteit van mailservers vast te stellen in gevallen waar DANE niet beschikbaar is. Deze situatie komt veelvuldig voor bij organisaties die bijvoorbeeld G Suite of Office 365 gebruiken. Het organisatiedomeinnaam is veelal met DNSSEC beveiligd (meer dan de helft van de gevallen voor .nl[22]), maar de mailserver van Google of Microsoft publiceert geen DNSSEC beveiligd TLSA-record (DANE). Een combinatie van een DNSSEC beveiligde MX-lookup en een traditionele controle van mailservercertificaten schept toch de mogelijkheid een veilige connectie op te zetten. Deze methode vereist enkel DNSSEC op het organisatiedomein. De mailserver hoeft niet te worden beveiligd met DNSSEC/DANE en hoeft enkel een geldig certificaat te tonen.

De hierna beschreven methode is een efficiënt alternatief, indien DANE niet mogelijk is door het ontbreken van DNSSEC op het mailserverdomein.

Introductie

Veelal besteden organisaties hun e-mailbeheer uit aan email service providers. Deze providers bieden vaak enkel opportunistische-, of “trust on first use” TLS-encryptie aan. Niet-opportunistische methoden (DANE) ontbreken helaas, waardoor veilige overdracht van versleutelde e-mail niet kan worden gegarandeerd. Gelukkig is het in sommige gevallen mogelijk toch de authenticiteit van de mailserver vast te stellen indien DANE niet is ingeregeld.

Voorbeeldsituatie

Een organisatie met het domeinnaam `example.org` laat het e-mailverkeer afhandelen door een externe partij (`provider_example.com`). Zodoende publiceert `example.org` het volgende MX-record:

```
example.org.   3600   IN     MX     mx1.provider_example.com.
```

De zone `example.org` is beveiligd met DNSSEC.
Het A-record van mx.provider_example.com is als volgt gepubliceerd:

```
mx1.provider_example.com.    3600   IN     A      192.0.2.1
```

De zone provider_example.com is niet met DNSSEC beveiligd, maar de mailserver ondersteunt STARTTLS en presenteert een geldig TLS-certificaat met een chain of trust naar een geldig X.509 rootcertificaat.

```
openssl s_client -starttls smtp -crlf -connect mx1.provider_example.com:25
…
Verification: OK
```

De authenticiteit van de server kan nu onomstotelijk worden aangetoond omdat:

[22] https://stats.sidnlabs.nl/nl/dnssec.html

- De integriteit van het MX-lookup vast staat dankzij DNSSEC-beveiliging van het ontvangende domein.
- Het subject van het mailservercertificaat overeenstemt met de servernaam uit het MX-record.
- Het mailservercertificaat geldig is door ondertekening van een vertrouwde certificate authority.

Verificatiestappen voor verzender

De verzendende mailserver dient de volgende stappen zorgvuldig te controleren en te volgen.

6. De MX-lookup gebiedt te gebeuren met een DNSSEC-enabled DNS resolver. Dit betekent dat de resolver geen antwoorden doorgeeft indien de DNSSEC-validatie niet slaagt. Ter controle kan de zone `dnssec-failed.org` worden geraadpleegd. Dit domein is met opzet onjuist geconfigureerd. Een correcte resolver zal dus geen antwoord mogen geven op DNS-verzoeken op dit domein.
7. De verbinding moet altijd gebruik maken van STARTTLS.
8. Het servercertificaat moet geldig zijn. Dat wil zeggen: volgens gangbare X.509 validatiestappen zoals inachtneming van vervaldatum en chain of trust naar een vertrouwd rootcertificaat.
9. Het certificaat-subject of de alternative names van het certificaat stroken met de mx hostname zoals gevonden in stap 1.

Veilige communicatie volgens de voorgestelde methode kan niet worden opgezet indien een van bovenstaande stappen faalt.

Inspanning voor ontvanger

Veel organisaties zullen reeds ondersteuning hebben voor deze verificatiemethode, al realiseren de meesten zich dit waarschijnlijk niet. Populaire domain registrars in Nederland zoals TransIP hebben vaak al standaard DNSSEC geactiveerd voor klanten. Praktisch alle email service providers ondersteunen STARTTLS en presenteren een geldig TLS-certificaat.

Controle

Aan onderstaande voorwaarden moet worden voldaan om dit alternatief voor het (tijdelijk) ontbreken van DANE mogelijk te maken.

- Voorwaarde 1: Controle DNSSEC op organisatiedomein
  Het is eenvoudig te controleren of de MX-lookup beveiligd is met DNSSEC door gebruik van Google's DNS lookup tool:

  https://dns.google.com/query?name=example.org&type=MX&dnssec=true

  De controle gaat als volgt: 1) Vervang example.org door het te testen domeinnaam. 2) Klik op "Resolve" 3) Controleer of in de output staat **`"AD": true`**. AD staat voor 'Authenticated Data', hetgeen betekent dat Google de controle op DNSSEC-geldigheid heeft gedaan en dat het record geldig is.

- Voorwaarde 2: Geldig STARTTLS-certificaat op de mailserver
  De website check tls (https://www.checktls.com/TestReceiver) biedt de mogelijkheid de TLS-certificaten van mailservers op geldigheid te controleren. Vul in het veld 'eMail Target' het organisatiedomeinnaam in. De tool zal zelf de MX-records opzoeken en alle vermelde mailservercertificaten controleren.

Bijlage D Wanneer is er sprake van interoperabiliteit?

Onderstaande casussen beschrijven wanneer er sprake is van interoperabiliteit.

Casus A: beide leveranciers zijn gecertificeerd en verzender heeft **geen** zelfverklaring (zelfverklaring vindt plaats in DNS TXT record):

- Effect = Leverancier zou moeten weten dat een klant niet voldoet en mag de header NTA 7516 niet zetten.
  Aan de ontvangende kant is dus sprake van de ontvangst van een reguliere mail waarop normale maatregelen van toepassing zijn.
- Risico = Leveranciers zetten de header wel.
- Maatregel = Leveranciers moeten vaststellen of klanten voldoen aan de NTA 7516. Dat kan technisch (DNS), maar ook contractueel. Mocht een leverancier haar product willen inzetten bij een klant die niet voldoet aan de NTA, dan moet de leverancier er bij deze klant voor zorgen dat in de header geen NTA wordt gezet.

Casus B: ontvangende leverancier is **wel** gecertificeerd en ontvanger heeft **geen** zelfverklaring:

- Effect = Mail mag niet interoperabel worden afgeleverd en volgt het stroomschema in § 2.1 van de technische handreiking.
- Risico = Geen.
- Maatregel = Geen extra maatregelen nodig.

Casus C: verzendende leverancier is **niet** gecertificeerd en verzender heeft **wel** zelfverklaring, de ontvanger is **wel** gecertificeerd en **met** zelfverklaring:

- Effect = Er vanuit gaande dat de leverancier van de verzender zich aan de regels houdt (zie volgende casus in situatie dat dit niet zo is), dan wordt de mail in de reguliere mailserver bij de ontvanger afgeleverd. Dit is niet interoperabel.
- Risico = Geen.
- Maatregel = Geen extra maatregelen nodig.

Casus D: verzendende leverancier is **niet** gecertificeerd maar heeft de technische handreiking gevolgd en verzender heeft **onterecht** een zelfverklaring, de leverancier van ontvanger is **wel** gecertificeerd en de ontvanger heeft **wel** een zelfverklaring:

- Effect = Dit betreft fraude door zowel de verzendende leverancier, als de verzender zelf. Omdat DKIM verplicht is en SPF zijn er voldoende maatregelen om de oorsprong te duiden. Daarnaast moet TLS gebruikt worden. Enige wat ontbreekt is DNSsec en certificaat. Het bericht kan interoperabel worden afgeleverd zonder extra verantwoordelijkheid bij de ontvanger.
- Risico = Ondermijning van de NTA 7516. Risico voor de ontvanger is beperkt, gezien de andere maatregelen (DKIM, SPF, TLS) die al zijn genomen.
- Maatregel = Geen extra maatregelen nodig. Het staat de ontvanger uiteraard vrij om aanvullende maatregelen te nemen, bijvoorbeeld door te checken of de verzendende leverancier voorkomt in het NEN register.