Bastion 365

WHITE PAPER

NTA 7516 compliant

met Microsoft 365 en Bastion 365

Versie 2.0

04-06-2021

INHOUD

INLEIDING

In dit White Paper geven we u een overzicht van de benodigde technische configuratie van uw domein en hoe Bastion 365 past binnen uw architectuur. Houd er rekening mee dat Bastion 365 de beveiligingsinstellingen voor uw domein (-en) niet configureert of onderhoudt maar deze wel nodig heeft om correct te werken. Deze technische gids legt de basisconcepten van de beveiligde e-mailconfiguratie uit en verwijst u waar nodig naar meer informatie.

Deze white paper is bijgewerkt tot en met release 1.4 van Bastion 365.

Mocht u vragen of opmerkingen hebben, raadpleeg onze kennisbank op bastion365.nl of neem contact op met onze Support afdeling via gsc@fenestrae.com.

WAAROM GEWONE E-MAIL NIET VEILIG IS

Hoewel e-mail een van de oudste vormen van communicatie op internet is en overal in applicaties op diverse apparaten is geïntegreerd, waren veiligheid en privacy nooit onderdeel van het ontwerp. Zorgen over privacy hebben een tijdje geduurd om serieus te worden genomen door wetgevers en er is eindelijk wetgeving geïmplementeerd in 2018 om de veiligheid van onze privacy te waarborgen. Strenge definities en hoge boetes voor niet-naleving hebben nu de aandacht van organisaties getrokken en e-mail is nu geïdentificeerd als een groot probleem en (hoogstwaarschijnlijk) grootste privacy lek in hun proces.

In principe is het artikel 32 van de Algemene Verordening Gegevensbescherming (AVG) die eist dat er zorgzamer om wordt gegaan met persoonsgegevens:

*"De verantwoordelijke legt passende **technische** en **organisatorische** maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een **passend beveiligingsniveau** gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen."*

Op Europees niveau is er een norm ontwikkeld voor wat er minimaal moet gebeuren bij digitale identificatie. Dit is de Europese eIDAS norm. De NEN – het Nederlandse orgaan voor het opstellen van normen en certificaties – heeft specifiek voor de zorgsector o.a. de NEN 7510 norm ontwikkeld voor informatiebeveiliging in de Zorg en ook de mate waarin acties moeten worden gelogd, de NEN 7513.

Om aan al deze eisen te voldoen is de norm voor veilig e-mailen in de zorg-sector geformuleerd: de NTA 7516.

VEILIGE E-MAIL STANDAARDEN

Veilig e-mailen is meer dan encryptie. Encryptie maakt alleen de overdracht tussen twee eindpunten veiliger. Als een van de twee eindpunten kan worden misleid of vervalst, zullen de gegevens beveiligd naar een onbedoeld kanaal stromen en nog steeds in verkeerde handen vallen. Dit betekent dat beveiligde e-mail niet alleen om beveiliging gaat maar ook om het valideren dat de twee eindpunten (zender en ontvanger) zijn wie ze beweren te zijn. Dit wordt bereikt door een combinatie van een aantal beveiligings- / authenticatiemaatregelen:

DNSSEC (Domain Name System Security Extensions)

De DNS van een domein wordt gebruikt om “mensvriendelijke” domeinnamen (zoals microsoft.com) te vertalen naar “machinevriendelijke” IP-adressen (zoals 192.0.578.4) die via internet kunnen worden gerouteerd. De authenticatie van beiden is onmogelijk in een gewone DNS.

DNSSEC maakt gebruik van digitale handtekeningen om de herkomst en integriteit van de ontvangen gegevens te verifiëren. Bastion 365 controleert dan ook als eerste of het domein van de ontvanger DNSSEC heeft zodat het zeker weet dat informatie verkregen van dat DNS ook betrouwbaar is, zoals bijvoorbeeld het NTA 7516 record.

STARTTLS

Met STARTTLS laat de e-mailclient de e-mailserver weten dat de verbinding moet worden opgeschaald naar een beveiligde verbinding via TLS.

DANE (DNS-based Authentication of Named Entities)

DANE maakt het mogelijk om een extra verificatiebron te zoeken door een TLSA-certificaat te publiceren waarmee klanten kunnen verifiëren dat de TLS-informatie overeenkomt met de informatie die via HTTPS wordt gepubliceerd. Als het overeenkomt, kan de afzender er zeker van zijn dat het eindpunt correct is en dat de gegevens kunnen worden overgedragen. DANE wordt afgehandeld via Bastion 365.

De combinatie DNSSEC / DANE / STARTTLS zorgt er in hoge mate voor dat een veilige verbinding tussen verzender en ontvanger van een e-mail tot stand kan worden gebracht door het domein te valideren en pas het e-mailbericht te verzenden als de validatie slaagt.

SPF (Sender Policy Framework)

Met SPF kan de e-mailserver van de ontvanger controleren of een e-mail die beweert afkomstig te zijn van een specifiek domein, is verzonden door een IP-adres dat is geautoriseerd door de beheerders van dat domein. De lijst met geautoriseerde mailservers voor het domein wordt gepubliceerd in een zgn. SPF-record.

DKIM (Domain Keys Identified Mail)

Met DKIM wordt een handtekening in de e-mail geplaatst waarmee de ontvanger kan controleren of een e-mail inderdaad is verzonden en geautoriseerd door de eigenaar van dat domein. Bastion 365 ondertekent een NTA 7516 bericht voordat deze wordt verstuurd.

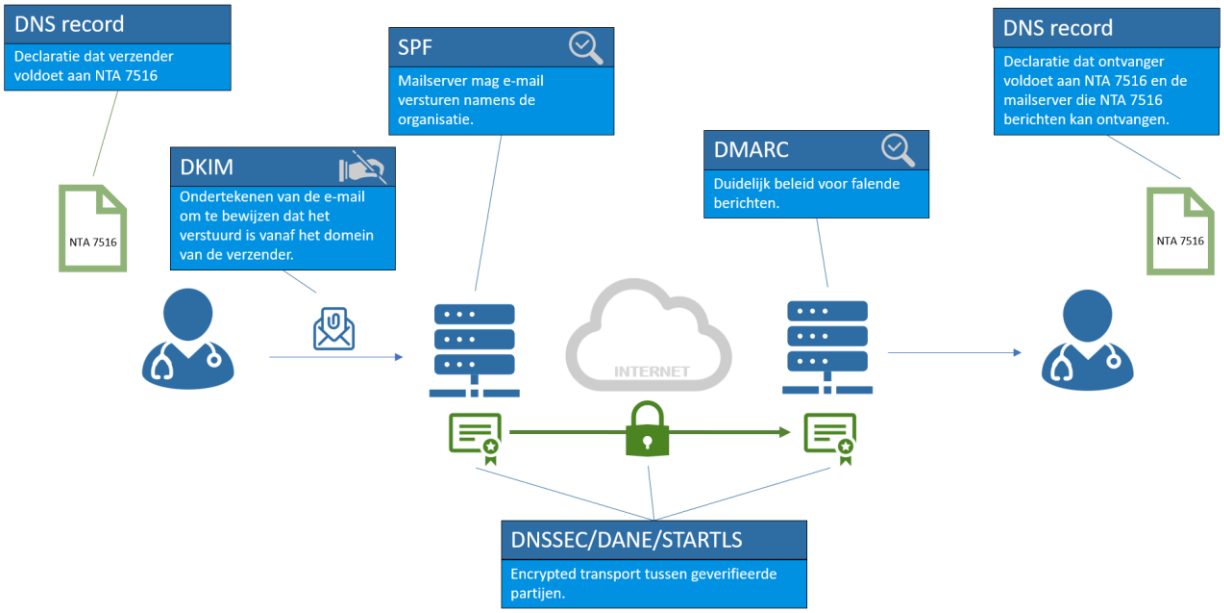
DMARC (Domain-based Message Authentication, Reporting & Conformance)

Een DMARC-beleid stelt de afzender in staat om aan te geven dat hun berichten worden beschermd door SPF en / of DKIM en vertelt een ontvanger wat te doen als geen van deze authenticatiemethoden slaagt. Om als veilig te worden beschouwd, moet dit beleid worden ingesteld op ‘reject’ (zorgt ervoor dat alle potentieel schadelijke e-mail wordt gestopt) of ‘quarantaine’ (ontvangt de e-mail die de DMARC-verificatiecontrole niet doorstaat, maar behandelt deze met extra voorzichtigheid).

Als alle bovenstaande standaarden correct zijn geïmplementeerd, kunnen de e-mails die worden verzonden en ontvangen door een mailprovider die ze valideert als veilig worden beschouwd.

HOE WERKT NTA 7516?

NTA 7516 heeft de vijf veilige e-mail standaarden als technische basis en voegt daaraan toe dat de twee NTA 7516 compliant partijen ook een zgn. NTA 7516 record moeten hebben in hun DNS, waarmee de zender en ontvanger declareren te voldoen aan NTA 7516 en wat de mailserver is die NTA 7516 berichten kan verzenden of ontvangen.



Indien bijde partijen voldoen, kan de e-mail veilig worden afgeleverd in de inbox van de ontvanger. Het bericht is dan voorzien van een NTA 7516 header die het bericht herkenbaar maakt als zodanig.

Door te declareren aan NTA 7516 te voldoen, moeten beide organisaties ook multi-factor authenticatie hebben toegepast op de werkplek.

Als de e-mail niet conform NTA 7516 kan worden verstuurd, dan moet er een alternatieve methode zijn om het bericht af te leveren. Deze moet ook gebruik maken van een geldige multi-factor authenticatie, maar moet ook zo gebruiksvriendelijk mogelijk blijven.

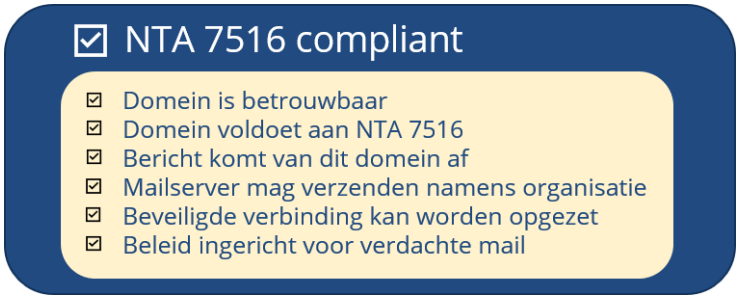
De NTA 7516 richt zich op de volgende doelgroepen:

Doelgroep	Mailprovider	
 Professionals die voldoen aan NTA 7516	zivver, zorgmail, SMARTLOCKR, PINEWOOD, E-Zorg, Bastion 365, Cryptshare, SecuMailer	Ontvangen de mail in hun inbox
 Professionals die niet voldoen aan NTA 7516	Exchange	Ontvangen de mail via MFA portaal
 Patiënten en mantelzorgers	Gmail, yahoo!, Outlook.com	Ontvangen de mail via MFA portaal

1.) De zorgprofessionals die voldoen aan NTA 7516. Deze hebben een NTA 7516 gecertificeerde mailprovider en ontvangen de NTA 7516 berichten in hun e-mail inbox
2.) De zorgprofessionals die (nog) niet voldoen aan NTA 7516. Deze hebben nog geen NTA 7516 gecertificeerde mailprovider of voldoen om een andere reden (nog) niet aan NTA 7516. Deze hebben in ieder geval Microsoft Exchange als mailprovider. Zij kunnen de persoonsgebonden berichten niet direct in hun mailbox ontvangen en moeten eerst via MFA geauthentiseerd worden.
3.) Patiënten kunnen niet voldoen aan NTA 7516 en hebben vaak een mailaccount bij een gratis mailprovider zoals Gmail, Hotmail or Outlook or Yahoo!. Zijn moeten ook eerst via MFA worden geauthentiseerd voordat zij het bericht met persoonsgebonden informatie kunnen lezen.

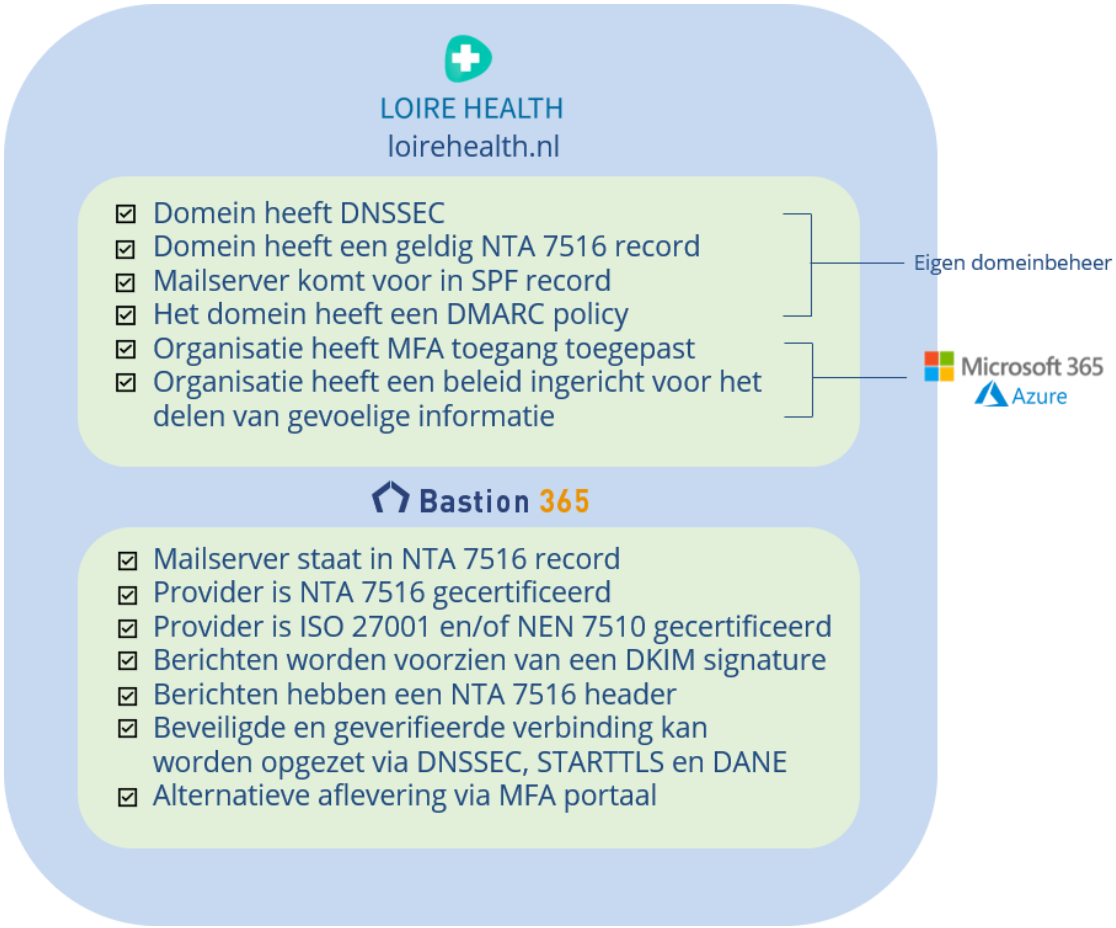
HOE WORDT JE NTA 7516 COMPLIANT?

Een NTA 7516 compliant domein voldoet aan de volgende voorwaarden:



In ons voorbeeld moet de zorgorganisatie *Loirehealth* op het eigen domein een aantal zaken inrichten. Dit moet men zelf doen of via een geautoriseerde partner, omdat de mailprovider over het algemeen geen toegang heeft tot het hoofddomein.

Naast het inrichten van de veilige e-mail standaarden, moet men ook MFA toegang tot de werkplek hebben geregeld. De zorgorganisatie moet ook een beleid hebben ingericht voor toegang en delen van gevoelige informatie.

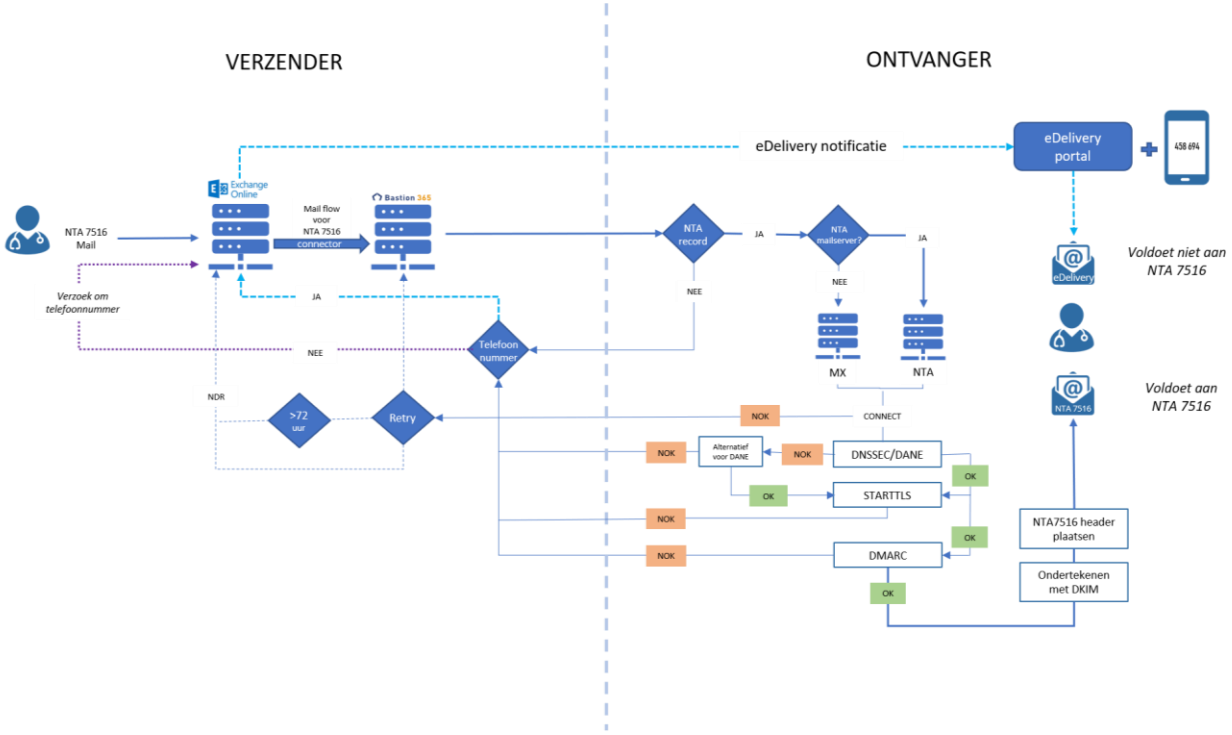


De mailprovider van de zorgprofessional moet NTA 7516 zijn gecertificeerd en heeft daarvoor ook als basis een ISO 27001 of NEN 7510 certificaat nodig om aan te tonen dat hij informatie beveiliging goed op orde heeft. De provider zal de DKIM handtekening plaatsen en het bericht van een NTA 7516 header voorzien zodat het als zodanig kan worden verstuurd. De provider moet ervoor zorgen dat de beveiligde en geverifieerde verbinding kan worden opgezet.

Omdat we niet willen dat berichten niet worden verzonden als de ontvangende partij niet aan NTA 7516 voldoet, moet er ook een alternatieve aflevermethode zijn in de vorm van een portaal voorzien van MFA. Dat gaat nu per SMS omdat dit op dit moment de meest beschikbare methode is voor iedereen. Vrijwel iedereen heeft een mobiele telefoon en kan SMS berichten ontvangen. Dit portaal moet eenvoudig en gebruiksvriendelijk zijn. Wat daarmee met name wordt bedoeld is dat de gebruiker naast de multi-factor authenticatie niet nog andere handelingen moet verrichten om bij het bericht te kunnen in het portaal zoals een aparte login of installatie van plug-ins.

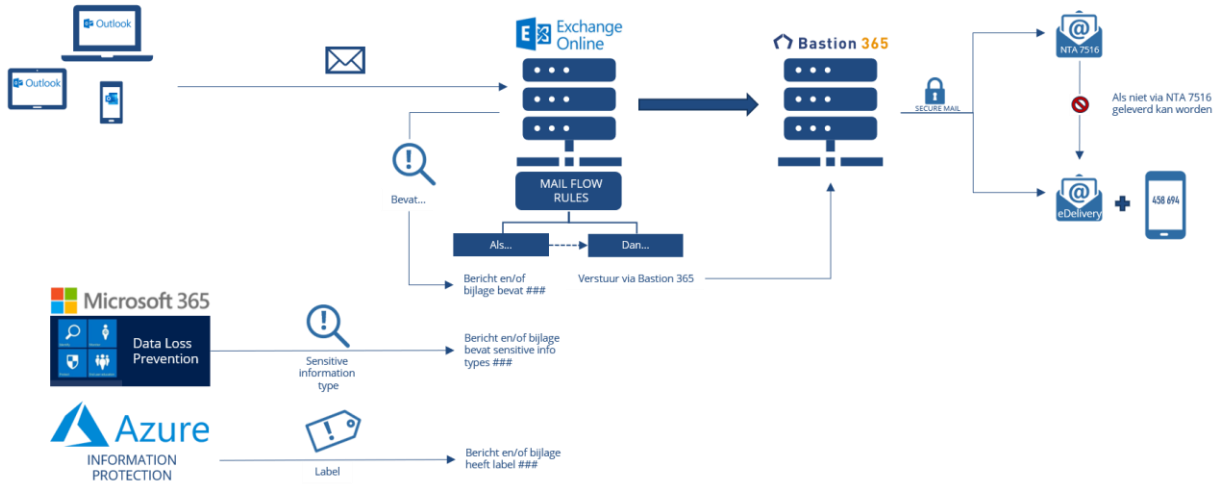
WAT DOET BASTION 365?

Bastion 365 functioneert als een MTA (message transfer agent). Uw organisatie gebruikt de Exchange-server van Microsoft 365 als e-mailserver om berichten te verzenden, maar Exchange Online kan de hierboven genoemde vereiste beveiligingsvalidaties niet (volledig) uitvoeren. Bastion 365 functioneert als een verlengstuk van Exchange Online en voert de nodige technische validaties uit en zorgt voor een veilig transport van de berichten en documenten.



WELKE E-MAIL BERICHTEN WORDEN VIA NTA 7516 VERZONDEN?

Microsoft 365 biedt verschillende oplossingen voor het identificeren van gevoelige inhoud in uw organisatie en applicaties (zie ook volgende hoofdstuk). Nadat deze zijn ingericht, geeft u Exchange Online opdracht om alle gevoelige inhoud via Bastion 365 te routeren zodat een veilige levering gegarandeerd is.



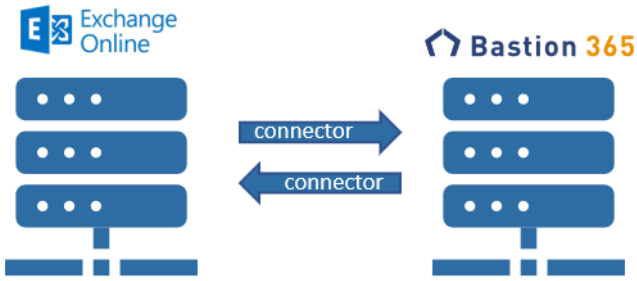
Onze oplossing biedt de verificatie of de ontvanger voldoet aan de veilige e-mailnormen en als hij dat niet doet, wordt het bericht afgeleverd via een twee-factor authenticatieservice (eDelivery) met een extra beveiliging via een unieke code per SMS.

De mail flow rules moeten de berichten voorzien van een header ‘X-Fen-SDX-NTA7516’ zodat Bastion 365 weet dat de berichten via deze weg moeten worden verstuurd.

MICROSOFT 365 CONFIGUREREN OM MET BASTION 365 TE WERKEN

Connectors aanmaken in Microsoft 365

Om ervoor te zorgen dat Bastion 365 e-mails van Microsoft 365 kan ontvangen, moet u een veilige verbinding tussen hen opzetten. Dit gebeurt via *connectors* in Exchange.



U moet een connector instellen om berichten naar Bastion 365 te verzenden en een om berichten van respectievelijk Bastion 365 te ontvangen. U kunt dit handmatig doen of met een script.

Nadat u de connectoren heeft ingesteld, kunt u zgn. 'mail flow rules' maken waarmee u kunt bepalen welke berichten moeten worden gerouteerd via Bastion 365 of hoe u berichten in Exchange Online die door Bastion 365 worden ontvangen, moet afhandelen.

Wat zijn 'mail flow rules' en waarom hebben we deze nodig?

Met een mail flow rule kunt u e-mailberichten in Exchange Online identificeren op basis van hun inhoud, ontvangers of andere identificatiegegevens en beslissen wat er met de berichten gebeurt. In ons geval moeten we e-mails identificeren die naar Bastion 365 moeten worden gerouteerd omdat ze gevoelige gegevens bevatten en met maximale bescherming en validatie moeten worden verzonden.

Omdat deze regels voor het identificeren van inhoud behoorlijk complex kunnen worden, biedt Microsoft verschillende methoden om gevoelige inhoud op het hele platform te identificeren. Deze worden gebruikt om gevoelige inhoud te labelen, zodat deze gemakkelijk kan worden gekoppeld aan een e-mailstroomregel in Exchange Online.

Identificatie van gevoelige inhoud in Microsoft 365

Veel sectoren die te maken hebben met gevoelige persoonlijke informatie zijn wettelijk verplicht om deze te beschermen en te kunnen bewijzen dat ze dat deden. Tegelijkertijd is het delen van informatie en interoperabiliteit van organisaties vereist voor efficiënte samenwerking en betere service. Er zijn verschillende methoden om inhoud op het Microsoft 365-platform te identificeren, zodat u berichten en documenten met de nodige zorg kunt beheren.

Alle opties voor gegevensbescherming werken ook goed samen, afhankelijk van hoe ingewikkeld uw beleid is of hoe u labels wilt toewijzen en beheren.

Lees de brochure for Microsoft Information Protection voor een overzicht van het brede scala aan services die Microsoft biedt voor gegevensbescherming. De beschikbaarheid van de producten voor gegevensbescherming kan afhankelijk zijn van uw Microsoft 365-abonnement.

Exchange Online

Exchange Online zal altijd een rol spelen bij het maken van mail flow rules, ongeacht de methode van gegevensbescherming die u toepast, aangezien in Exchange Online wordt gespecificeerd welke berichten naar Bastion 365 worden gerouteerd om met maximale veiligheid te worden afgeleverd.

In Exchange Online kunt u aangeven wat er gebeurt met berichten die zijn geclassificeerd als gevoelige informatietypes. Met Exchange Online kunt u ook een (combinatie van) regel (s) maken waarvoor Exchange Online een specifieke actie moet ondernemen. Aangezien deze regels erg complex kunnen worden, wordt het aanbevolen om de detectie en classificatie van de gevoelige gegevens te beheren met behulp van een van de onderstaande methoden. Ze kunnen allemaal door Exchange Online worden gebruikt om acties te ondernemen.

Microsoft 365's Data Loss Prevention

Met DLP van Microsoft kunt u een geïndexeerde tekstzoekopdracht uitvoeren op het hele Microsoft-platform (Sharepoint Online, OneDrive, Exchange Online en alle Office toepassingen) en gegevensbeleid inrichten dat het gebruik van gevoelige gegevens in documenten en toepassingen bewaakt. De belangrijkste bedoeling is om u in staat te stellen datalekken te identificeren en te voorkomen.

Een beleid kan elke tekstinhoud identificeren die u opgeeft. Dit kunnen de ingebouwde indexen van Microsoft 365 zijn voor burgerservicenummers of creditcardnummers, maar ook lijsten met specifieke termen die, indien vermeld in een bericht of document, worden geïdentificeerd als (potentieel) gevoelig zodat u acties kunt toewijzen die moeten worden ondernomen. In ons geval wordt het onder meer gebruikt door Exchange Online om het bericht via Bastion 365 te routeren.

DLP van Microsoft 365 biedt een brede set aan beheer- en rapportagetools waarmee u de gegevensbescherming in uw hele organisatie kunt beheren.

Microsoft 365's Advanced Data Governance

Microsoft 365 Advanced Data Governance past machine-learning toe om klanten te helpen bij het vinden en behouden van belangrijke informatie, terwijl triviale, overtollige en verouderde informatie die bij compromittering risico's kan opleveren, wordt verwijderd. Met ADG kunt u documenten classificeren en labelen voor het toepassen van bewaar-, verloop- en verwijderingsbeleid voor gevoelige informatie.

Azure Information Protection

Met Azure Information Protection kunt u berichten en documenten labelen. Dit label blijft bij het bericht of document, ongeacht waar het wordt opgeslagen of gebruikt op het Microsoft Azure-platform. Het belangrijkste verschil tussen Microsoft's DLP en de AIP is dat gebruikers met AIP actief een bericht of document kunnen labelen en dat alle regels voor gegevensbescherming kunnen worden toegepast wanneer het label is ingesteld.

Een gelabeld bericht en document kunnen vervolgens worden versleuteld of hebben beperkte toegang. In ons geval wordt het label gebruikt om berichten te identificeren die via Bastion 365 moeten worden gerouteerd.

Samenvatting

In de onderstaande tabel vindt u een overzicht van de relevante functies voor gegevensbescherming die elk Microsoft-product biedt.

	Azure	Exchange online	Data Loss Prevention	Advanced Data Governance	Azure Information Protection
Multi-factor authenticatie op de werkplek	① ✓				
Mail flow rules		② ✓			
Regels en voorwaarden definiëren		③ ✓	✓	✓	✓
Gevoelige inhoud detecteren		✓	✓	✓	
Bewaar-, verloop- en verwijderingsbeleid instellen			✓		✓
Gebruik en distributie van gevoelige gegevens bewaken			✓		✓
Gebruikers labels laten toekennen aan documenten					✓
Automatisch documenten en berichten labelen				✓	
Visuele markering van documenten met PGI					✓

Deze drie stappen zijn belangrijk:

① De toegang tot de werkplek die conform NTA 7516 met een twee factor authenticatie moet worden voorzien. Het is natuurlijk lastig voor een verzender om dit te controleren, maar het is wel voorwaarde voor uw organisatie om te claimen aan NTA 7516 te voldoen.

② Er moeten zgn. Mail Flow Rules worden gedefinieerd. Daarmee geeft u aan welke berichten (met of zonder bijlagen) moeten worden verstuurd via NTA 7516. Dit is inrichtbaar in Exchange en wordt hoogstwaarschijnlijk al gebruikt door uw Exchange beheerder in een of andere vorm. Minimaal moet er voor deze oplossing worden ingericht dat mailverkeer naar buiten de organisatie via Bastion 365 veilig moet worden verstuurd. Omdat men natuurlijk ook nog graag normaal wil kunnen e-mailen buiten de organisatie is het wellicht wel nodig om bepaalde regels en voorwaarden te definiëren.

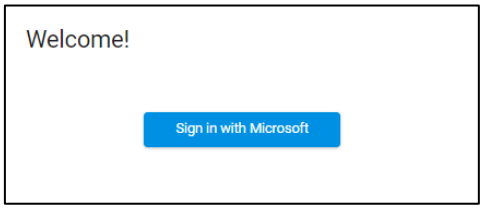
③ Is nodig om ervoor te zorgen dat er alleen bepaalde e-mails via Bastion 365 moeten kunnen worden verstuurd. Een eenvoudige manier is om de gebruiker de mogelijkheid te geven om aan te geven dat de e-mail via NTA 7516 moet worden verstuurd in Outlook. Probleem hierbij is natuurlijk dat dit kan worden vergeten.

UW DOMEIN CONFIGUREREN VOOR NTA 7516

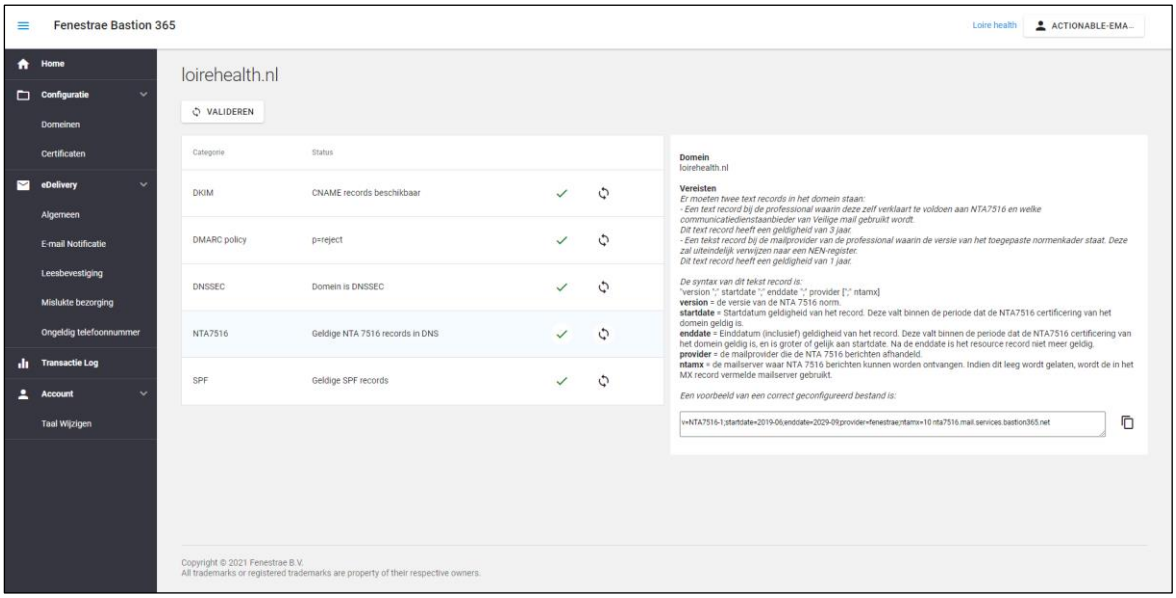
In het configuratieportaal van Bastion 365 richt u uw domein(-en) in voor het zenden en ontvangen van veilige mail, bepaalt u de settings van de eDelivery mailberichten en kunt u de transactie logs bekijken.

Na activeren van uw organisatie voor het werken met Bastion 365, bereikt u het portaal via uw webbrowser: *bastion365.com*

U kunt via single sign-on inloggen met uw Microsoft 365 account.



Ondersteuning bij het juist inrichten van uw domein(-en)



Voor elk domein moet u valideren of deze voldoet aan de veiligheidseisen en -normen van NTA 7516. U wordt ook geholpen met voorbeelden van hoe de DNS records juist geconfigureerd moeten worden.

DNSSEC

Uw hoofddomein moet beveiligd zijn met DNSSEC zodat informatie verkregen vanaf uw DNS gevalideerd kan worden. Dit wordt over het algemeen ondersteund door de DNS providers, maar moet misschien wel aangevraagd worden.

SPF

Om een consistent beleid te garanderen, moet SPF worden geïmplementeerd op alle domeinen en alle ontvangende e-mailservers die met Bastion 365 worden gebruikt.

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.

Het SPF-record dient de volgende elementen te bevatten:

- *de email servers voor uw domein*
- *de lijst van servers van Bastion 365, middels de volgende include:* ***include:_spf.mail.services.bastion365.net***
- *eindigen op -all*

het resultaat ziet er dan zo uit:

v=spf1 <uw mail-servers> include:_spf.mail.services.bastion365.net -all

DKIM

Bastion 365 plaatst een DKIM-handtekening op het bericht wanneer het wordt verzonden. Hierdoor is het voor de ontvanger verifieerbaar dat het bericht vanuit uw organisatie is verzonden.

Om dit te doen, moet u twee nieuwe CNAM- records maken voor elk domein dat door Bastion 365 zal worden gebruikt om de uitgaande berichten te ondertekenen.

Als u DKIM-handtekeningen in Exchange Online gebruikt, heeft u al twee CNAME-records (selector1 en selector2) voor Microsoft in uw DNS staan. Laat deze alstublieft ongewijzigd.

Uw CNAME-records moeten er als volgt uitzien:

Host = fen-selector-1._domainkey. {formattedDomainName}.mail.services.bastion365.net
Host = fen-selector-2._domainkey. {formattedDomainName}.mail.services.bastion365.net

DMARC

DMARC staat voor Domain-based Message Authentication, Reporting and Conformance. Het is een DNS TXT-record dat in uw domein is gepubliceerd en waarmee u kunt specificeren welk authenticatiemechanisme wordt gebruikt bij het verzenden van e-mails vanuit uw domein (DKIM, SPF of beide) en wat uw beleid is als de authenticatie mislukt:

p=quarantine
'Quarantine' laat de e-mailontvangers weten dat u wilt dat zij e-mails die de DMARC-verificatiecontrole niet doorstaan met extra voorzichtigheid moeten behandelen. De e-mails worden nog steeds geaccepteerd door de ontvanger, maar de ontvanger beslist welk quarantainebeleid hij wil implementeren.

p=reject
Met 'Reject' zorgt u ervoor dat alle schadelijke e-mail wordt gestopt. De ontvanger van de kwaadaardig bedoelde e-mail zal niet op de hoogte worden gebracht van de e-mail, omdat deze nooit naar een spam- of quarantainemap wordt gestuurd. Doordat zij volledig worden geblokkeerd, worden e-mails nooit afgeleverd en kunnen eindgebruikers niet worden misleid om op een kwaadaardige link te klikken of een gevaarlijke bijlage te openen.

Opties in NTA 7516 kanaal

Met versie 1.4 van Bastion 365 hebben wij een aantal opties geintroduceerd voor het NTA 7516 kanaal die u in het configuratie portaal kunt inrichten.

Soepelere omgang met het NTA 7516 record

U kunt nu instellen dat er een wat soepelere omgang met het NTA 7516 record gewenst is. Bastion 365 controleert bij ontvangers het NTA 7516 record -net als alle andere veiligheidsmaatregelen- op juistheid conform de standaard. Helaas blijkt dat deze records vaak niet (helemaal) kloppen zoals bijvoorbeeld een onjuiste einddatum of een niet geheel correcte syntax.

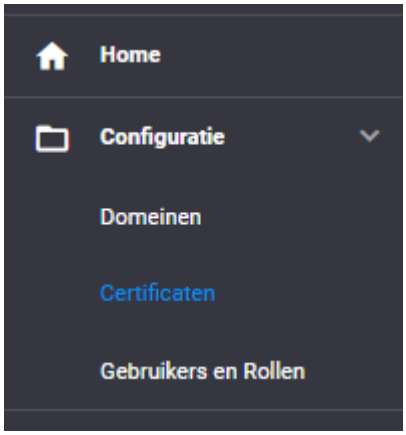
Dit zorgt voor problemen met de interoperabiliteit en daarom bieden wij in het NTA 7516 kanaal de optie om hier wat soepeler mee om te gaan. Dit is geheel op eigen verantwoordelijkheid en het wordt gelogd dat deze validatie wordt overgeslagen.

Indien er van deze optie gebruik wordt gemaakt, dan kan er wel voor wat veiligheid betreft via NTA 7516 worden verstuurd, mits er verder alles technisch in orde is.

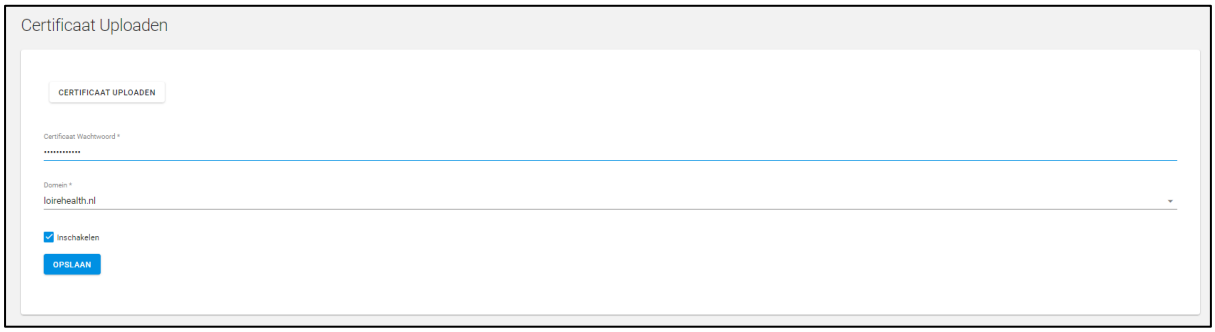
CAdES handtekening voor berichten

Vanaf nu is het ook mogelijk om berichten te voorzien van een CAdES handtekening. Daarmee tekent men voor het bericht, zodat de ontvanger zeker weet dat het bericht echt authentiek is.

Het certificaat voor de handtekening kunt u inrichten in het configuratie portaal onder hoofmenu item Configuratie:



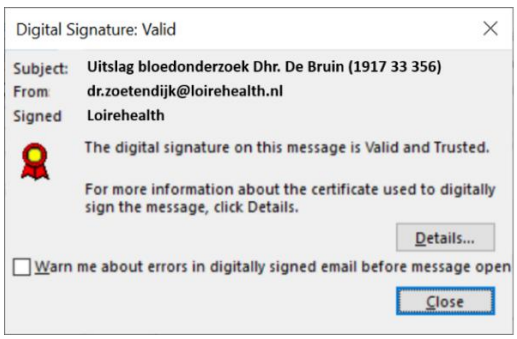
U kunt daar per domein een certificaat met het bijhorende wachtwoord uploaden



Berichten met een geldige CAdES handtekening zijn in de inbox van de ontvanger zichtbaar door een symbool aan de rechterkant.

Als men het bericht opent is zichtbaar dat het bericht is ondertekend en door wie.

Het geverifieerde certificaat kan ook worden opgevraagd



In het configuratieportaal kunt u per kanaal aangeven wat er respectievelijk bij ontvangen en verzenden moet gebeuren met betrekking tot de CAdES handtekening.

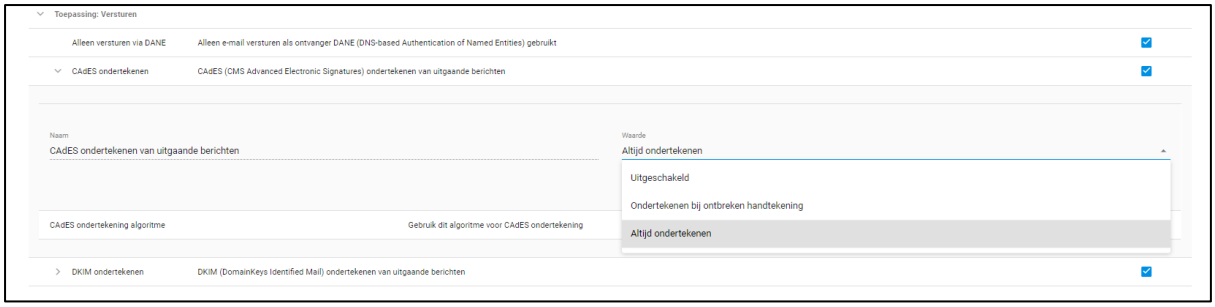
Ontvangen:

U kunt aangeven dat alle ontvangen berichten moeten voorzien zijn van een CAdES handtekening of alleen bepaalde algoritmes toestaan.

Verzenden:

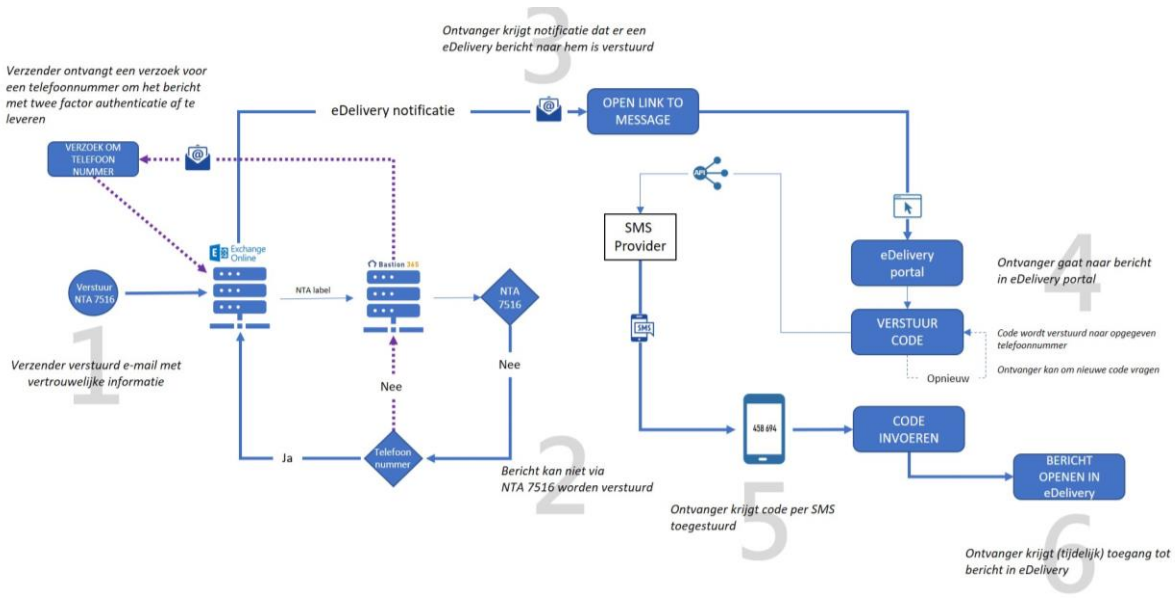
Net als bij de DKIM-handtekening kan ervoor worden gekozen om de CAdES- handtekening toe te voegen enkel indien hij ontbreekt of altijd toe te voegen.

U kunt hier ook het algoritme kiezen dat u wilt gebruiken bij het ondertekenen.

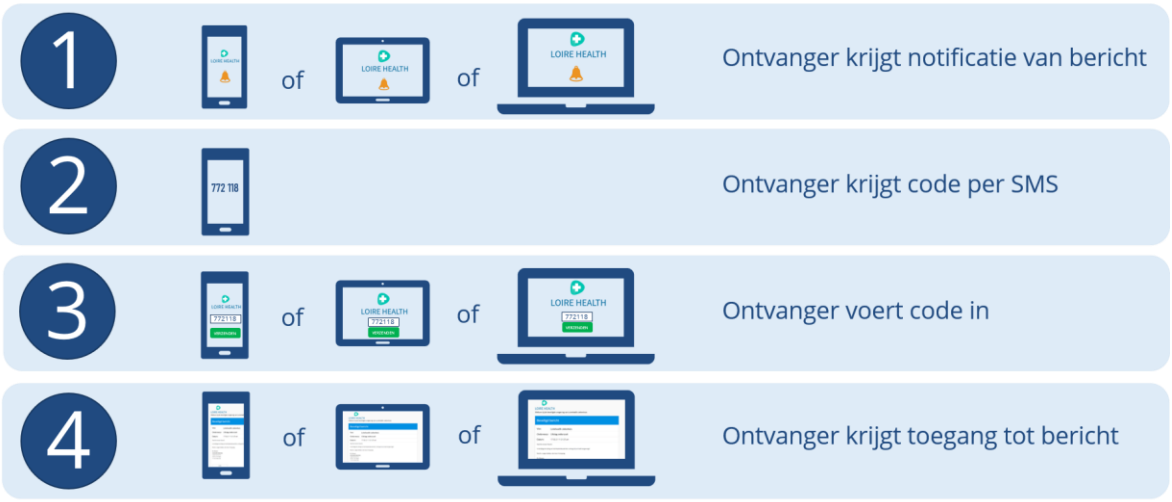


Inrichten twee-factor portaal (eDelivery)

Bastion 365 heeft een veilig mailportaal, waarmee berichten kunnen worden afgeleverd als de validatie van de NTA 7516 inrichting bij de ontvanger mislukt. De verzender zal in dat geval een verzoek krijgen om een telefoonnummer op te geven voor de ontvanger. De ontvanger krijgt dan een notifcatie e-mail dat er een veilig bericht klaar staat in het portaal met een link daarnaartoe. Via deze link kan hij een toegangscode aanvragen die dan per SMS wordt toegestuurd en na ingave toegang geeft tot het mailbericht zelf.



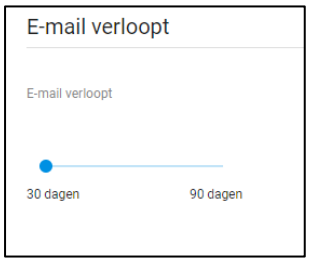
De ontvanger heeft verder geen speciale inrichting nodig en de oplossing is niet afhankelijk van de mail-client of mailprovider die de verzender gebruikt.



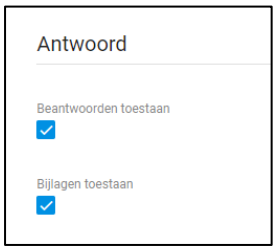
Het eDelivery portaal in Bastion 365 is ook in hoge mate inrichtbaar zodat u deze kunt afstemmen op uw behoeftes.

Algemene instellingen

U kunt instellen hoe lang u de berichten wilt bewaren (minimaal 30 dagen en maximaal 90 dagen)

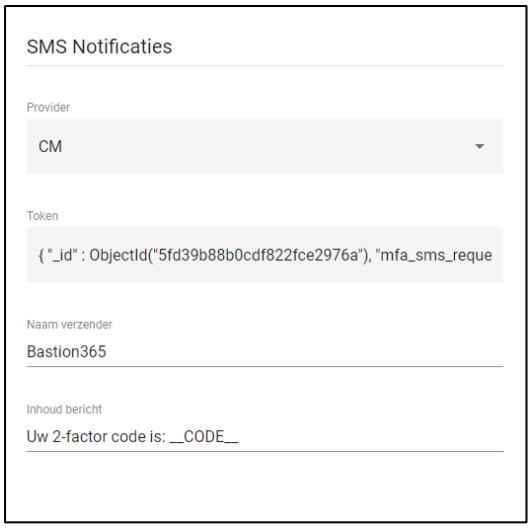


U kunt bepalen of de ontvanger van een eDelivery bericht ook een antwoord mag sturen naar u en deze mag voorzien van een bijlage.



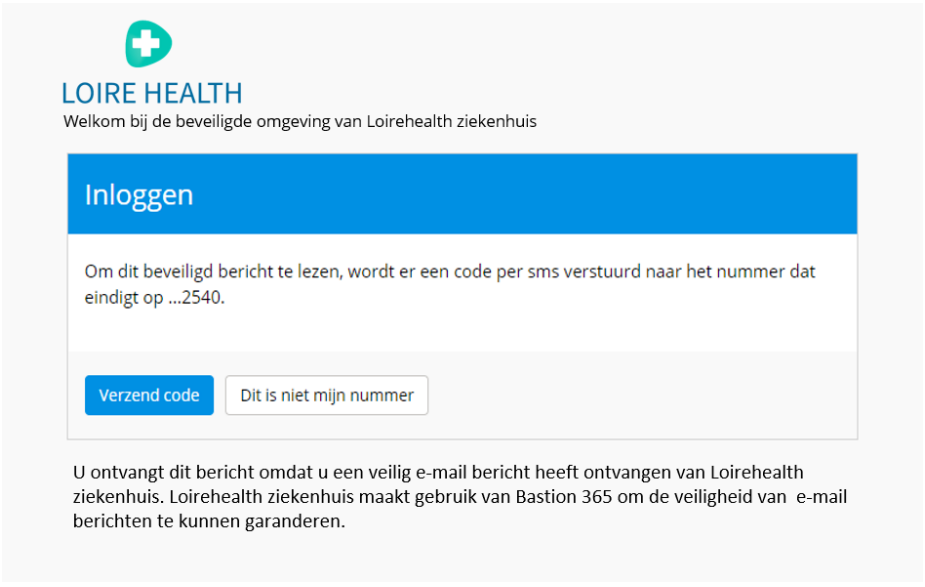
Voor het versturen van de tijdelijke toegangscodes via SMS kunt u gebruikmaken van de Bastion 365 standaard provider, maar u kunt ook gebruikmaken uw eigen SMS-provider. Op dit moment bieden wij versturen van codes via SMS door CM of Spryng. U kunt dan uw eigen token gebruiken om de codes per SMS te sturen naar de ontvanger. Indien u gebruik maakt van de standaard

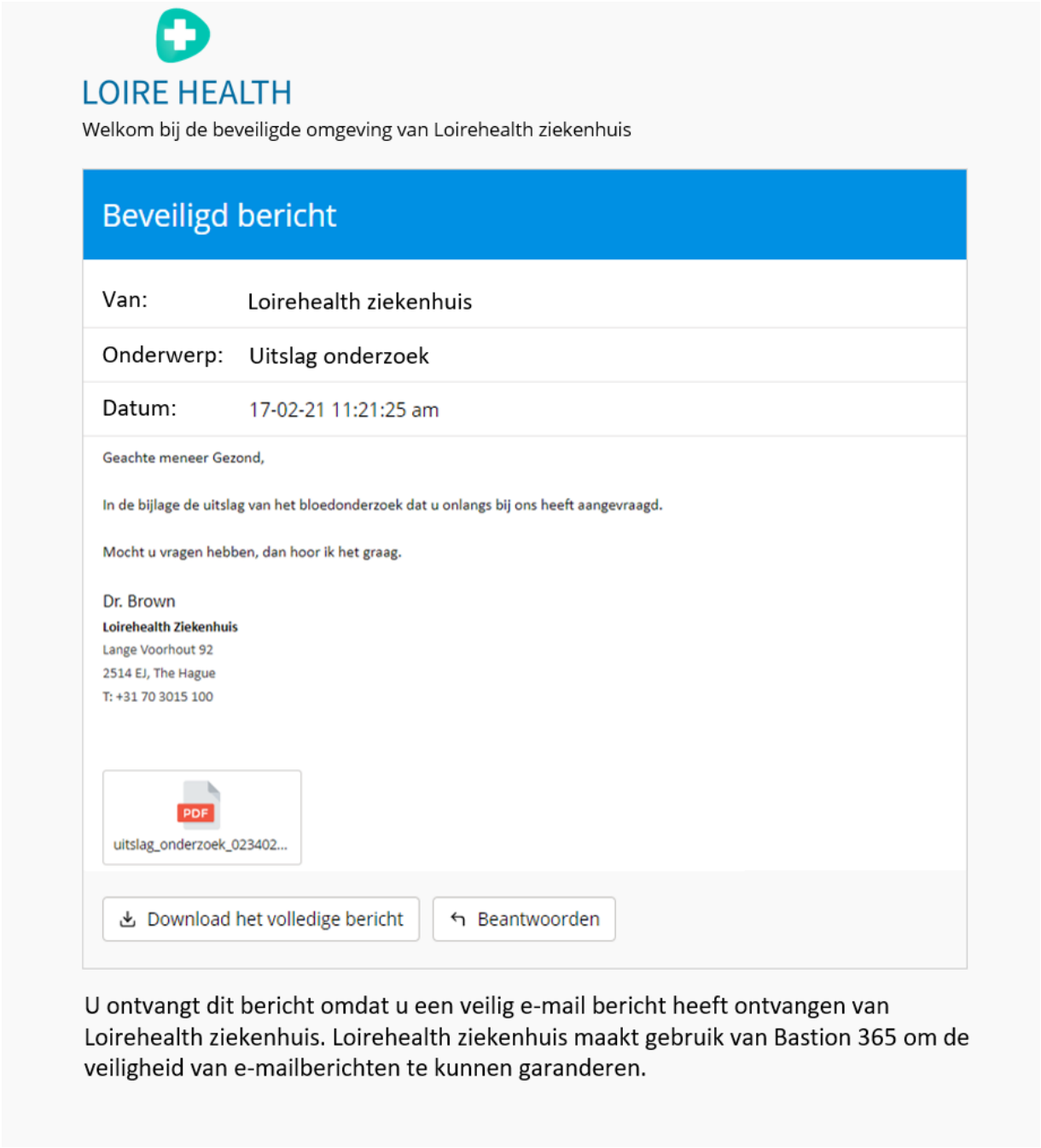
provider van Bastion 365, zullen de kosten voor het versturen van de SMS-berichten apart aan u worden gefactureerd.



Portaal

Het two factor berichten portaal kunt u inrichten met uw eigen logo en teksten, zodat deze vertrouwd overkomt voor de bezoekers.





U ontvangt dit bericht omdat u een veilig e-mail bericht heeft ontvangen van Loirehealth ziekenhuis. Loirehealth ziekenhuis maakt gebruik van Bastion 365 om de veiligheid van e-mailberichten te kunnen garanderen.

Notificaties

Notificatie ontvanger

De notificatie dat er een bericht voor de ontvanger is afgeleverd in het eDelivery portaal is voor een groot deel inrichtbaar gemaakt. U kunt de volgende zaken wijzigen:

E-mailadres afzender

Standaard worden de notificaties van Bastion 365 gestuurd via het e-mailadres noreply@UWDOMEIN. U kunt dit aanpassen naar een ander **valide** e-mailadres.

Naam verzender

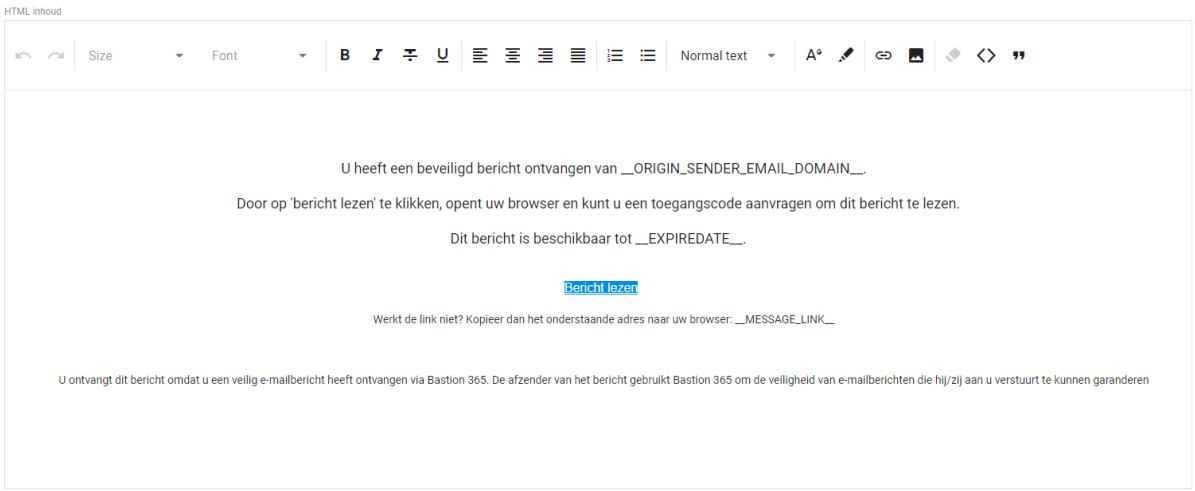
Dit is de naam van de verzender zoals die in de e-mailclient die de ontvanger gebruikt zichtbaar is. Normaal gesproken is dit de naam van de verzender, maar u kunt dit bijvoorbeeld veranderen in een generieke naam zoals de naam van uw organisatie.

Onderwerp

U kunt het onderwerp van de notificatie aanpassen. Let hierbij op dat het een generieke tekst moet zijn omdat u niet al in het onderwerp gevoelige informatie wilt doorgeven voordat de identiteit van de ontvanger is gecontroleerd met multi-factor authenticatie.

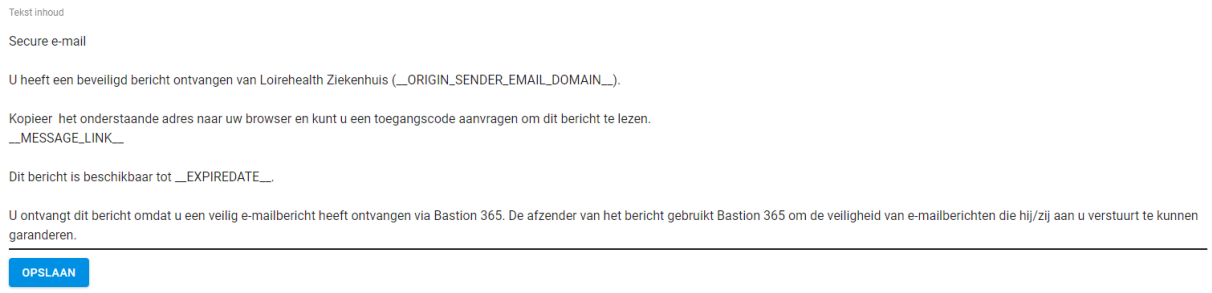
HTML-inhoud

Het notificatie bericht naar de ontvanger kan worden aangepast of aangevuld. Met behulp van een eenvoudige HTML-editor kunt u de notificatie bijvoorbeeld voorzien van uw logo of aanvullen met extra instructies of informatie.



Tekst inhoud

Voor het geval de ontvanger geen HTML kan lezen via zijn e-mailclient is het nodig om ook een tekstversie van de notificatie aan te kunnen bieden.



Notificaties voor verzender

De verzender van een e-mailbericht dat via eDelivery wordt afgeleverd krijgt een aantal notificaties die eveneens door u kunnen worden aangepast of aangevuld.

Leesbevestiging

De verzender van een e-mailbericht dat via onze eDelivery portaal wordt bezorgd, krijgt een notificatie dat het bericht is gelezen.

Hier kunt u ook de afzender naam en e-mailadres, onderwerp en inhoud (HTML en tekst) aanpassen of verrijken met informatie of instructies.

Mislukte bezorging

De verzender van een e-mailbericht dat via onze eDelivery portaal wordt bezorgd, krijgt een notificatie dat het bericht niet is gelezen door de ontvanger en is verwijderd.

Hier kunt u ook de afzender naam en e-mailadres, onderwerp en inhoud (HTML en tekst) aanpassen of verrijken met informatie of instructies.

Ongeldig telefoonnummer

De verzender van een e-mailbericht dat via onze eDelivery portaal wordt bezorgd, krijgt een notificatie dat het telefoonnummer niet klopt.

Hier kunt u ook de afzender naam en e-mailadres, onderwerp en inhoud (HTML en tekst) aanpassen of verrijken met informatie of instructies.

Overzicht tags voor Notificaties

Hieronder een overzicht en uitleg van de diverse tags die in de notificaties kunnen worden gebruikt.

__ORIGIN_SENDER_NAME__	De naam van de originele verzender die in de mailclients wordt getoond (bijvoorbeeld Dr. De Bruin).
__ORIGIN_SENDER_EMAIL__	Het e-mail adres van de originele verzender.
__ORIGIN_SENDER_EMAIL_DOMAIN__	Het domein van de originele verzender.
__ORIGIN_RECIPIENT_EMAIL__	Het e-mail adres van de ontvanger.
__MESSAGE_LINK__	De link naar het bericht in eDelivery portaal.
__SUBJECT__	Het originele onderwerp.
__SEND_DATE_TIME__	Datum/tijd van versturen originele bericht.
__DATE_TIME__	Datum/tijd van deze actie.
__EXPIREDATE__	Datum waarop eDelivery bericht wordt verwijderd.
__PHONE_SHORT___	Het ingekorte telefoonnummer (laatste vier cijfers).