Cryptshare NTA-7516 Compliance

Inleiding

Vanaf 1 januari 2020 is de Wet op de Verplichte Geestelijke Gezondheidszorg (WvGGZ) van kracht. Daarin speelt veilige ad hoc e-mail communicatie conform de NTA-7516 norm een cruciale rol.

NTA7516 schrijft voor dat communicatie van medische persoonsgegevens uitgewisseld via e-mail, veilig verstuurd moeten worden conform de definities zoals deze in de NTA7516 zijn bepaald. Cryptshare klanten die medische persoonsgegevens communiceren, krijgen hier dus mee te maken. Voor klanten waar deze situatie zich niet voordoet, is dit schrijven niet relevant.

Interoperabiliteit en Cryptshare for NTA7516

Cryptshare heeft in december deelgenomen aan de projecathon die was georganiseerd door het Ministerie van VWS. Doel van deze projecathon was om onderlinge uitwisseling tussen verschillende toepassingen voor veilige e-mail te testen. Deze uitwisseling wordt interoperabiliteit genoemd en houdt in dat een veilige e-mail verzonden vanuit de ene veilige e-mail oplossing in de andere veilige e-mail oplossing kan worden gelezen. Voor de projecathon heeft Cryptshare een prototype ontwikkeld en deze succesvol getest op interoperabiliteit.

De volgende stap is dat dit prototype verder wordt uitgewerkt in een eerste versie van Cryptshare for NTA7516. Verwachting is dat deze versie in februari beschikbaar komt. Cryptshare for NTA7616 zal voor klanten met een Cryptshare Enterprise License beschikbaar zijn.

Over de achtergrond van de NTA7516, de WvGGZ en de berichten-box van Khonraad wordt hieronder ingegaan. Daarnaast wordt in woord en beeld uiteengezet hoe Cryptshare het NTA compliant zijn heeft ingericht voor de klant .

NTA7516

In mei 2019 is de NTA7516 gepubliceerd en is door een aantal veilige e-mail leveranciers een intentieverklaring ondertekend, waarmee de oplossingen van die leveranciers per mei 2020 zullen voldoen aan de NTA7516. Cryptshare is een van de partijen die deze intentieverklaring heeft ondertekend. In de NTA7516 staan 21 punten genoemd waaraan een veilige e-mail oplossing kan voldoen. Om als leverancier aan deze norm te voldoen dient aan tenminste twee van deze punten te worden voldaan. Het punt interoperabiliteit is daarbij voor alle leveranciers verplicht, het tweede punt is aan de leverancier. Voor organisaties geldt dat ze aan alle 21 punten moeten voldoen om NTA compliant te zijn.

WvGGZ

De WvGGZ is per 1 januari 2020 ingegaan. Deze wet bepaalt onder meer dat persoonlijke medische gegevens alleen via beveiligde e-mail mogen worden verstuurd en beroept zich daarbij op de definities zoals deze in de NTA7516 zijn uitgewerkt.

De intentie verklaring van de deelnemende leveranciers van veilige e-mail oplossingen moet per mei 2020 tot resultaat leiden. Cryptshare is een van de leveranciers die heeft aangegeven al eerder te kunnen voldoen aan de NTA7516. Er zullen ook leveranciers zijn die op deze datum niet kunnen voldoen aan de gestelde eisen.

Khonraad

De berichten-box van Khonraad voorziet in communicatie in geval zich een crisis in een gemeente voordoet. In dit soort situaties zijn er altijd gevoelige medische persoonsgegevens die beveiligd verstuurd moeten worden. Via de berichten-box gaan betrokken ketenpartners beveiligd over die situatie geïnformeerd worden. Dit zijn partijen zoals de GGZ, het Openbaar Ministerie, de burgemeester, de gemeente, etc. Buiten de ketenpartners zullen ook andere mensen zoals familieleden geïnformeerd worden over de crisis situatie. Omdat deze personen geen toegang tot de berichten-box hebben zal de communicatie in die gevallen niet via de berichten-box verlopen. Voor die gevallen maakt de berichten-box gebruik van de veilige e-mail oplossing van de gemeente.

Voor de gemeentes die met Cryptshare werken is voor deze situatie een koppeling met de berichten-box beschikbaar. Deze koppeling is voor klanten met een Cryptshare Enterprise License beschikbaar. De gemeentes die Cryptshare gebruiken zijn hier inmiddels over geïnformeerd. Indien een gemeente hier nog niet (voldoende) van op de hoogte is, bel 026-8200322 of stuur een mail naar info@cryptshare.com

Hoe werkt Cryptshare for NTA7516

NTA7516 streeft naar interoperabiliteit tussen verschillende veilige e-mail oplossingen. Dus een mail verstuurt van een veilige e-mail oplossing aan een ontvanger met een andere veilige e-mail oplossing moet door die ontvanger in zijn eigen veilige e-mail oplossing gelezen kunnen worden. In de technische handreiking van het Ministerie van VWS is aangegeven hoe de NTA7516 in de verschillende veilige e-mail toepassingen kan worden gerealiseerd en aan welke veiligheidseisen dit moet voldoen. Hierbij wordt gewerkt op basis van een verificatie van de status van een ontvanger, is deze al dan niet NTA-compliant. Zodra de ontvanger hieraan voldoet is voorgeschreven onder welke condities een veilige e-mail kan worden verstuurd. Dit leidt dan tot drie mogelijke scenario's die hieronder kort worden beschreven.

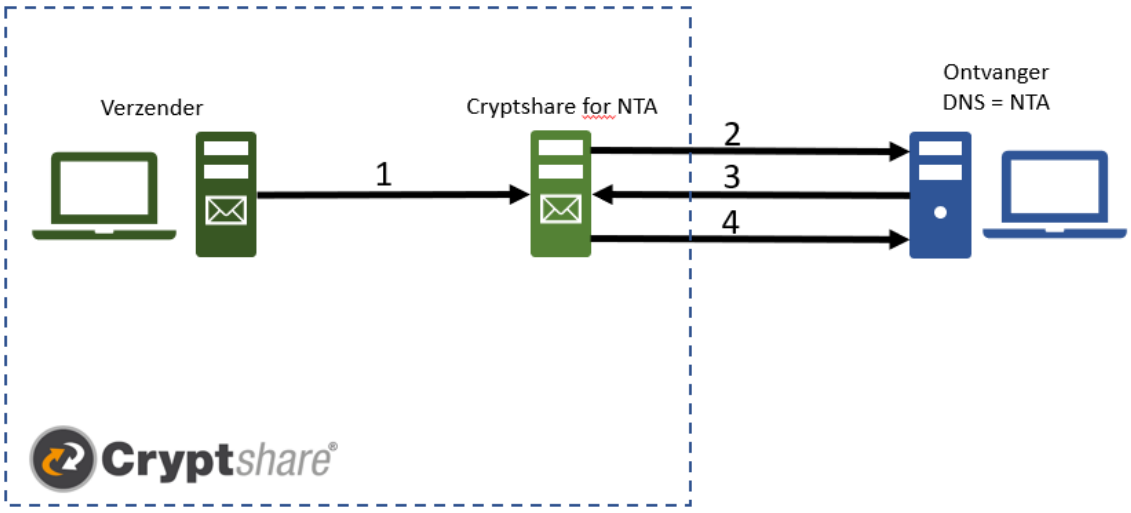
Scenario 1: verzenden aan een NTA compliant organisatie

Wanneer er medisch gevoelige gegevens verstuurd worden, controleert Cryptshare for NTA7516 voorafgaand aan het verzenden of de ontvanger NTA compliant is. Als de ontvanger NTA compliant is en als de e-mail geen grote bijlage heeft, kan er een mail worden verstuurd met een versleuteling zoals deze is voorgeschreven. Die versleuteling is dan op basis van open standaarden die door alle NTA compliant oplossingen worden gebruikt. Cryptshare for NTA7516 voorziet ook in deze versleuteling.

Opmerking: Wanneer de bijlage van de e-mail te groot zijn om via de NTA standaard verstuurd te worden zal de mail volgens scenario 2 verstuurd worden. In de regel zijn bijlagen groter dan 20MB te groot om via de NTA standaard verstuurd te worden.

De ontvanger kan met behulp van het DNS record van de mail server aangeven of zijn omgeving NTA compliant is. Om als organisatie NTA-compliant te zijn moet er worden voldaan aan de voorwaarden zoals deze zijn omschreven op https://www.nen.nl/Alles-over-NEN-7510/NTA-7516.htm

Proces omschrijving scenario 1



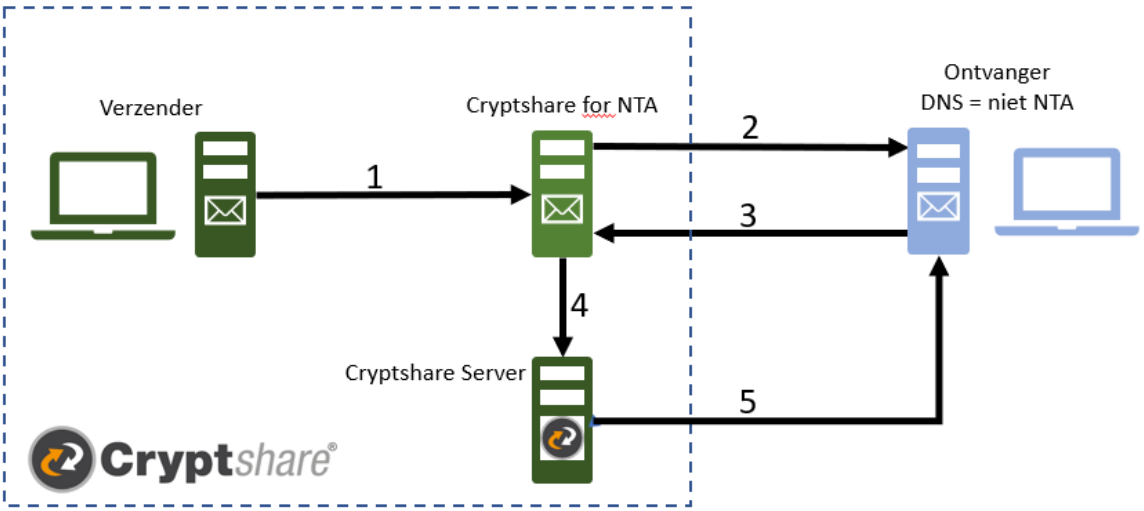
1. De mail van de verzender wordt aan Cryptshare for NTA7516 aangeboden.
2. De Cryptshare NTA7515 Connector doet een DNS (domain named system) lookup op de server van de ontvanger.
3. Het DNS record van de mailserver van de ontvanger geeft aan dat de organisatie van de ontvanger NTA compliant is.
4. De Cryptshare NTA7515 Connector verstuurt het bericht conform de eisen van versleuteling aan de ontvanger.

Scenario 2 : verzenden aan een niet NTA compliant organisatie of een persoon

In het geval dat Cryptshare for NTA7516 aangeeft dat de ontvanger niet NTA compliant is en er medisch gevoelige gegevens verstuurd worden, zal de mail via Cryptshare verstuurd moeten worden.

Opmerking: De implementatie van NTA compliancy bij organisaties is per 1-1-2020 vanwege de WvGGZ begonnen. De verwachting is dat er over tijd steeds meer organisaties compliant zullen zijn. Gevolg is dat bij aanvang veel organisaties nog niet NTA compliant zullen zijn terwijl communicatie volgens de AVG al wel beveiligd moet worden. In die gevallen zal standaard Cryptshare voor dit scenario voorzien in het beveiligen van die e-mail communicatie.

Proces omschrijving scenario 2

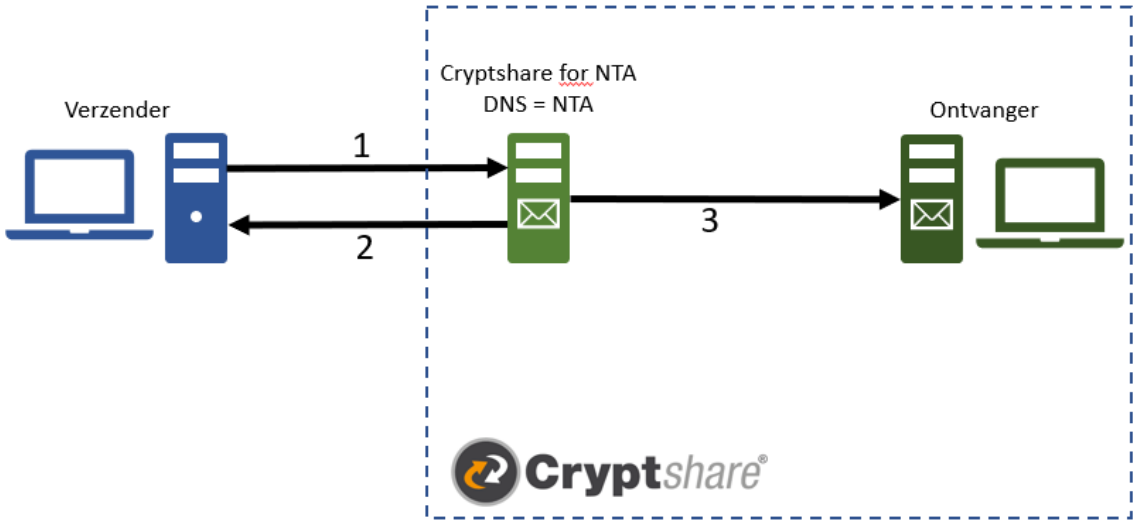


1. De mail van de verzender wordt aan de Cryptshare NTA7515 Connector aangeboden.
2. De Cryptshare NTA7515 Connector doet een DNS lookup op de server van de ontvanger.
3. Het DNS record van de mailserver van de ontvanger geeft aan dat de organisatie van de ontvanger niet NTA compliant is.
4. De Cryptshare NTA7515 Connector verstuurd het bericht naar de Cryptshare server.
5. Cryptshare verstuurt de e-mail op de gebruikelijke wijze, dus een notificatie mail met een download link voor de ontvanger, waarmee de versleutelde mail door de ontvanger wordt opgehaald.

Scenario 3: een mail ontvangen vanuit een NTA compliant organisatie

Wanneer je als Cryptshare klant Cryptshare for NTA7516 hebt geïnstalleerd en je als organisatie voldoet aan de eisen die aan een organisatie worden gesteld om NTA compliant te zijn, kun je dat via het DNS record duidelijk maken. Cryptshare for NTA7516 zal in dat geval e-mails die conform NTA7516 versleuteld zijn ontvangen en leesbaar aan de ontvanger binnen jouw organisatie aanbieden.

Proces omschrijving scenario 3



1. Een veilige e-mail oplossing voert een DNS lookup uit op Cryptshare for NTA7516. De Cryptshare NTA7515 Connector doet een DNS lookup op de server van de ontvanger.
2. Cryptshare for NTA7516 geeft via het DNS record aan dat de Cryptshare gebruiker NTA compliant is.
3. Cryptshare for NTA7516 ontsleutelt de aangeleverde mail en stuurt deze door aan de Cryptshare ontvanger.