INFORMATIEBEVEILIGING ZORGMAIL

Uitgave mei 2018

INHOUDSOPGAVE

1 ZORGMAIL OPLOSSING 3

2 GESTRUCTUREERDE BERICHTEN 3

3 ONGESTRUCTUREERDE BERICHTEN 4

3.1 Binnen de community 4
3.2 Tussen communities 4
3.3 Buiten de community 4

FIGUUR 1: SCHEMATISCHE WEERGAVE GESTRUCTUREERDE BERICHTENSTROMEN 5

FIGUUR 2: SCHEMATISCHE WEERGAVE ONGESTRUCTUREERDE BERICHTENSTROMEN 6

1 ZORGMAIL OPLOSSING

Enovation biedt met ZorgMail passende oplossingen voor grote en kleine (zorg)organisaties.

Om deelnemer te kunnen worden van ZorgMail vindt een screening van de aanmelding plaats door de Gebruikersadministratie van Enovation waarbij het verzoek onder meer wordt gecontroleerd op registratie in landelijke registers, zoals het AGB-code register, voordat tot acceptatie wordt overgegaan.

Gekoppelde organisaties en deelnemers zijn vindbaar in het ZorgMail adresboek. Als belangrijke schakel in de keten biedt Enovation als 'Trusted Third Party' veel toegevoegde waarde in het veilige berichtenverkeer tussen geauthentiseerde ZorgMail deelnemers evenals met deelnemers buiten de community.

Voor het veilig inloggen op ZorgMail applicaties wordt standaard gebruik gemaakt van Passage ID, een dienst van Enovation. Passage ID biedt de mogelijkheid aan gebruikers om het account te versterken met twee-staps-verificatie.

2 GESTRUCTUREERDE BERICHTEN

ZorgMail EDI is een besloten dienst: de afzender en geadresseerde zijn bekend. Koppelingen van ZorgMail EDI met informatiesystemen vinden plaats op basis van door Enovation opgestelde technische beveiligingsspecificaties.

Authenticatie is mogelijk middels:

a. een X.509 client certificaat (/RSA Sleutelpaar),
b. een applicatiewachtwoord, Access Key of API Key,
c. een gebruikersnaam en wachtwoord is tevens mogelijk voor de informatiesystemen die nog geen client certificaat authenticatie voor EDI berichtenverkeer ondersteunen.

De berichten worden van afzender naar geadresseerde verstuurd over een onafhankelijk systeem (ZorgMail) van een onafhankelijke partij (Enovation) waarbij de verbindingen van en naar de centrale server end-to-end worden beveiligd. Voor systemen die dat ondersteunen bestaat de mogelijkheid om, naast de end-to-end versleuteling van de verbindingen, ook de berichten te versleutelen (S/MIME, PGP). Bij het gebruik van Internet als toegangsnetwerk wordt de verbinding tussen de software van de gebruiker en de server van ZorgMail versleuteld met TLS. Op de server van ZorgMail staat een server certificaat waarmee een versleutelde verbinding opgezet kan worden.

De gebruikersnaam en het wachtwoord voor authenticatie worden binnen de TLS-tunnel versleuteld verstuurd. De gebruiker heeft zelf geen certificaat nodig als de verbinding door de gebruiker wordt opgezet en voor authenticatie een gebruikersnaam en wachtwoord worden gebruikt. ZorgMail ondersteunt de nieuwste protocollen voor versleutelde verbindingen (TLS 1.2), aangevuld met een aantal gangbare protocollen waarvan geen ernstige kwetsbaarheden zijn gevonden. De

protocolondersteuning wordt doorlopend beoordeeld en aangepast om het hoogste veiligheidsniveau te halen. Zie ook figuur 1: “Schematische weergave gestructureerde berichtenstromen”.

3 ONGESTRUCTUREERDE BERICHTEN

Voor het veilig versturen van ongestructureerde berichten zoals e-mail zijn diverse mogelijkheden voorhanden. Zo is er de Veilig Verzenden button die zorgt dat het juiste afzenderadres wordt gehanteerd. Daarnaast wordt met deze button de geadresseerde voorafgaand aan de verzending gecontroleerd en de e-mail als vertrouwelijk gemarkeerd. Koppelingen van ZorgMail Secure e-mail met informatiesystemen vinden plaats op basis van door Enovation opgestelde technische/beveiligingsspecificaties. Zie ook figuur 2: schematische weergave ongestructureerde berichtenstromen.

3.1 Binnen de community

ZorgMail Secure e-mail is de beveiligde oplossing van Enovation waarmee op veilige wijze tussen personen gecommuniceerd kan worden. Koppelingen met mailserveromgevingen worden op basis van door Enovation opgestelde technische/beveiligingsspecificaties gerealiseerd. De authenticatie van mailservers vindt plaats op basis van X.509 certificaten voor het benodigde vertrouwensniveau. In deze specificaties is ook beschreven hoe een deelnemer DKIM/SPF/DMARC maatregelen dient te nemen om mailvervalsing tegen te gaan. Voor de verbindingen wordt een sessie time-out bij inactiviteit gehanteerd van 20 minuten.

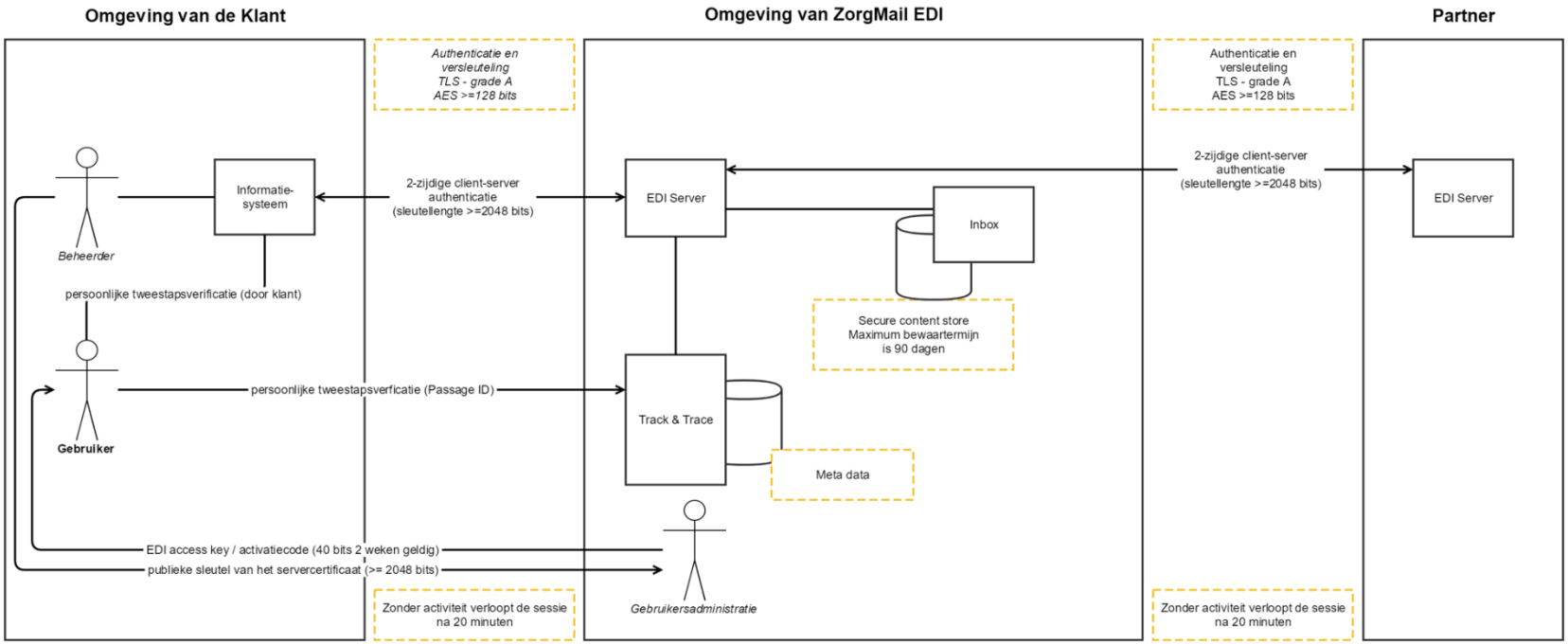
3.2 Tussen communities

Ook kent ZorgMail koppelingen met netwerken van andere leveranciers die dienen te voldoen aan de beveiligingseisen die Enovation stelt. Met de leveranciers van deze gekoppelde netwerken zijn afspraken gemaakt hoe de adresboeken van toegelaten organisaties over en weer in de adresboeken up-to-date worden gehouden. De verbindingen zijn voorzien van de benodigde TLS encryptie (data in transit).

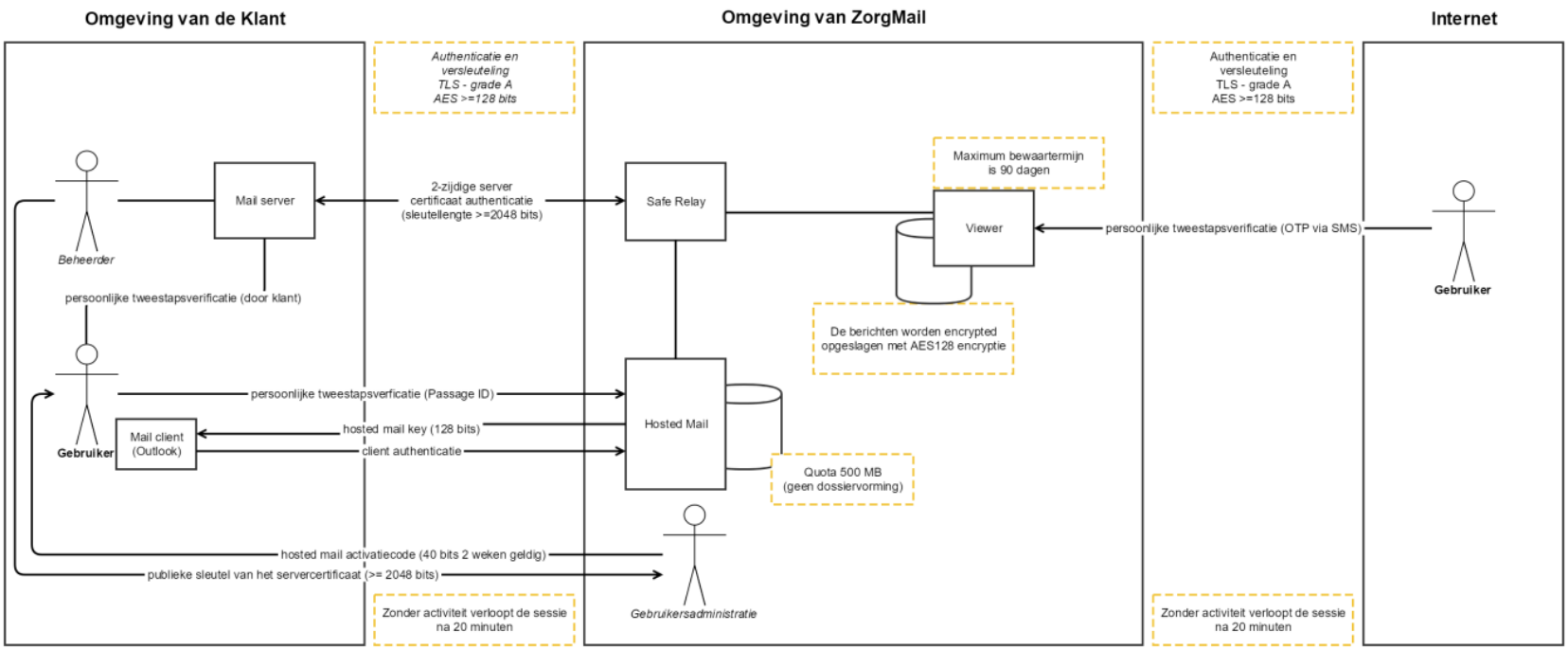
3.3 Buiten de community

Niet-ZorgMail deelnemers ontvangen een notificatiemail op hun internet e-mailadres. De niet-ZorgMail deelnemer krijgt via twee-staps-verificatie toegang tot het bericht gebruikmakend van de versleutelde ZorgMail omgeving. Koppelingen worden op basis van opgestelde technische/beveiligingsspecificaties gerealiseerd.

FIGUUR 1: SCHEMATISCHE WEERGAVE GESTRUCTUREERDE BERICHTENSTROMEN



FIGUUR 2: SCHEMATISCHE WEERGAVE ONGESTRUCTUREERDE BERICHTENSTROMEN




enovation®
care to connect