Beveiliging documentuitwisseling zorginstellingen

Auteur: Marc de Graauw
Versie: 1, 10 september 2013

Inhoudsopgave

1. Inleiding

Dit document beschrijft de beveiligingsaspecten van documentuitwisseling tussen zorginstellingen.

Dit document dient in samenhang gelezen te worden met:

- Infrastructuur documentuitwisseling zorginstellingen

Per implementatie dienen er extra documenten te zijn:

- Configuratie infrastructuur [naam uitwisseling]
- Parameters document [naam verslag en uitwisseling]

Versie	Datum	Wijzigingen
1	10 september 2013	Eerste versie, groter voorgaand document gesplitst in drieën.

2. Beveiliging

Voor beveiliging van het berichtenverkeer wordt een tweezijdige TLS 1.0 verbinding opgezet. De zender initieert de verbinding. De verbinding wordt opgezet met UZI of PKIO servercertificaten. (Er wordt niet - zoals in Aorta - gebruik gemaakt van de private key op de persoonsgebonden UZI-passen voor het de authenticatie.)

Verificatie dat de juiste persoon, met de juiste autorisaties, het bericht inzendt wordt overgelaten aan de bestaande procedures binnen de instelling. De betrokken artsen dienen wel een UZI-pas aan te vragen, om over een UZI-nummer te kunnen beschikken.

3. Certificaten

Gebruikte UZI-certificaten zijn van de UZI-register Server CA G21 tak, dus servercertificaten van de SHA-2 generatie.

Certificaten worden niet meegezonden, kunnen met LDAP opgehaald (en eventueel gecached) worden, de ontvanger moet dan een certificaat per instelling opslaan en de CRL regelmatig ophalen.

UZI testservercertificaaat kunnen aangevraagd worden op:
http://www.uziregister.nl/ondersteuning/testomgeving/testpasenservercertificaat/

Een UZI-servercertificaat kan aangevraagd aanvragen worden op:
http://www.uziregister.nl/servercertificaat/servercertificaataanvragen/. Daarbij staat ook de technische how-to van de aanvraag (met PKCS#10 bestand e.d.) per omgeving.

3.1 Zorginstellingen

Coloscopiecentra gebruiken een UZI-servercertificaat. Dit kan een nieuw aangevraagd certificaat zijn. Wanneer een ziekenhuis echter al over een UZI-servercertificaat beschikt, bijvoorbeeld voor opvragen BSN of WID-verificatie, mag dat ook gebruikt worden.

Het UZI register heeft de volgende positie ingenomen t.o.v. certificaten t.b.v. dit soort zorgcommunicatie (n.a.v. communicatie met Colonis):

"U gaf aan dat er binnenkort een pilot start waar het Maasstad ziekenhuis bij betrokken is. Het Maasstad heeft al een UZI servercertificaat, wat gebruikt wordt voor verificatie van het BSN. De vraag is of zij ditzelfde certificaat kunnen gebruiken voor de uitwisseling met Colonis (RIVM).

Indien het servercertificaat door dezelfde abonnee gebruikt wordt, welke het certificaat heeft aangevraagd, is dat geen bezwaar, met inachtneming van de beveiligingsvoorwaarden van het Uzi-register.

Er kan dan een export (PFX) van het servercertificaat gemaakt worden en op een andere server geïnstalleerd worden. Hoe u dit kunt uitvoeren staat beschreven in onze handleidingen op
http://www.uziregister.nl/ondersteuning/handleidingeneninstallatie/installerenuziservercertificaat.asp"

(Emailcommunicatie met UZI register d.d. 8-2-2013)

3.1.1 Niet-zorginstellingen

Bij niet-zorginstellingen wordt geen UZI certificaat gebruikt, maar een certificaat uit de PKI-Overheid tak.

4. Controles op de certificaten en verbinding

Gebruik van certificaten alleen is niet voldoende garantie voor geautoriseerd gebruik. Wanneer de eis gesteld wordt dat een UZI-servercertificaat gebruikt wordt voor communicatie met een ontvanger, kan immers nog steeds iedere eigenaar van een UZI-servercertificaat communiceren met de ontvanger, terwijl meestal slechts een beperkt aantal bekende zorginstellingen daartoe gerechtigd zijn. Bij PKIO-certificaten voor niet-zorginstellingen, breidt dit zich uit tot alle PKIO certificaten. De volgende validaties zijn dus vereist.

4.1 Validaties bij ontvanger

De ontvanger moet verifiëren dat voor het opzetten van de SSL verbinding door een zorginstelling een UZI-servercertificaat gebruikt wordt, dus getekend met:
http://www.uzi-register.nl/cacerts/uzi-register_server_ca_g21.cer
Met als subject:
CN = UZI-register Server CA G21
O = agentschap Centraal Informatiepunt Beroepen Gezondheidszorg
C = NL
Belangrijk is bij accepteren van de verbinding deze certificaten toe te staan, en niet alle certificaten die via een certificate chain getekend zijn met het "Staat der Nederlanden" certificaat.

Bij het opzetten van een SSL verbinding door een niet-zorginstelling wordt een PKIO certificaat gebruikt. Dit moet een bekend PKIO-certificaat zijn. Het is dus nooit correct alle PKIO-certificaten te accepteren, dit moet er een zijn uit een gelimiteerde lijst die bij de ontvanger bekend is.

Wanneer het certificaat door de ontvangende web server is gevalideerd, moet de waarde in "subject.commonName" (hierin staat de Fully Qualified Domain Name (FQDN) van de service) gecontroleerd worden tegen geautoriseerde inzenders. Bij de ontvanger moet dus een tabel zijn met geautoriseerde inzenders met daarin:

- de FQDN van de inzender, b.v. "communicatie.mijnzorginstelling.nl"
- de URA van deze inzender, b.v. "12345678"
- overige gegevens van de inzender, b.v. de naam van de organisatie.

Bij binnenkomst van een bericht moet De ontvanger dan verifiëren dat de FQDN uit subject.commonName van het gebruikte certificaat voorkomt in deze tabel, en dat de beheerder (custodian) uit het ingezonden bericht hoort bij dezelde rij in de tabel. Op deze wijze wordt gegarandeerd dat alleen geautoriseerde inzenders berichten inzenden. De rij in de tabel wordt gevuld bij het afsluiten van de overeenkomst. Voor Stichting Palga wordt een soortgelijke rij opgenomen.

Door verificatie van de FQDN wordt voorkomen dat wanneer een UZI servceritficaat verloopt, en een nieuwe wordt aangevraagd, De ontvanger aangepast moet worden. Uiteraard moet de aanvragen van het nieuwe certificaat borgen dat dezelfde FQDN gebruikt wordt als bij het certificaat dat bijna verlopen is.

4.2 Validaties bij inzenders

De validaties bij inzenders zijn soortgelijk, maar iets eenvoudiger. De inzender moet verifiëren dat de ontvanger een UZI-servercertificaat gebruikt, getekend met: http://www.uzi-register.nl/cacerts/zorg_csp_ca.cer. Daarnaast moet de gebruiker controleren dat in de subject.commonName de FQDN van De ontvanger staat.