



0101UZI0100REGISTER10111

Het beveiligen van UZI-servercertificaten

Elektronische communicatie speelt een steeds grotere rol in onze samenleving.

Ook in de zorg. Omdat zorginformatie over het algemeen privacy gevoelige gegevens bevat, staat zorgvuldige bescherming van die gegevens voorop. De patiënt moet daarop kunnen vertrouwen.

Het moet duidelijk zijn wie gegevens leest, verstuurt of ontvangt. Om hierover zekerheid te kunnen geven is het Unieke Zorgverlener Identificatie register, kortweg UZI-register, ontwikkeld.

Het UZI-register is onderdeel van het CIBG, agentschap van het ministerie van Volksgezondheid, Welzijn en Sport (VWS).

Het UZI-register maakt ook deel uit van het Informatiepunt BSN in de zorg en landelijk EPD.

Dit is een factsheet van het UZI-register, waarin een vaak gestelde vraag wordt beantwoord. Een overzicht van alle factsheets vindt u op de website www.uzi-register.nl.

Mei 2009

Het UZI-register geeft servercertificaten uit. Met behulp van deze servercertificaten kunnen zorgaanbieders en indicatieorganen veilig elektronisch communiceren. Het is daarbij van belang dat er rondom het gebruik een aantal waarborgen worden getroffen. De essentie hiervan is dat het praktisch onmogelijk moet zijn om de sleutels ongemerkt te stelen of te kopiëren. LET OP: het is heel moeilijk om een gewone werkplek aan deze beveiligingsmaatregelen te laten voldoen. Met deze factsheet zet het UZI-register de voorwaarden voor u op een rij. Door het technische karakter is specifieke deskundigheid nodig. Vraagt u daarom uw leverancier of ICT-deskundige u te helpen bij het beveiligen van uw servercertificaat. Naast de voorwaarden die het UZI-register stelt kunnen vanuit de toepassing aanvullende eisen worden gesteld (bijvoorbeeld de Goed Beheerd Zorgsysteem eisen)

Voor de beveiliging van het servercertificaat moeten in de praktijk bijvoorbeeld de volgende elementen minimaal op de server aanwezig zijn:

- Een virusscanner voorzien van de laatste updates (virus signatures).
- Een spyware scanner voorzien van de laatste updates (voor Macintosh computers is dat op dit moment niet noodzakelijk).
- Een firewall zo ingericht dat alle communicatiekanalen zijn afgesloten met uitzondering van die, die noodzakelijk zijn voor de bekende applicaties.
- Het besturingssysteem moet voorzien zijn van de laatste updates.
- Het servercertificaat mag alleen door het administrator account benaderd worden. Ook wel 'systeembeheerders account' genoemd.
- Bij een servercertificaat horen twee sleutels. Dit sleutelbaar bestaat uit twee wiskundig verbonden sleutels: een private en een publieke sleutel. De publieke sleutel wordt onderdeel van uw servercertificaat, de private sleutel houdt u ten allen tijden geheim. Met het sleutelbaar kan het systeem bewijzen dat het bij u hoort. De private sleutel moet versleuteld zijn. Dit om te voorkomen dat de private sleutel onbeveiligd op een backup komt te staan.

- Als u voor de versleuteling geen gebruik maakt van een Certificate Store, gebruik dan voor de versleuteling een gangbaar versleutelingsalgoritme voor private sleutels. Daarnaast moet u het bestand met daarin de private sleutel zo beveiligen dat alleen de applicatie toegang krijgt tot dit bestand. De consequentie is dat bij het herstarten van een systeem of applicatie, u altijd een activeringscode moet ingeven voordat u het servercertificaat kunt gebruiken.
- De activeringscode bestaat minimaal uit 6 karakters. Het is geen bestaand woord (of naam) en bestaat uit:
 - hoofdletters
 - kleine letters
 - en tenminste 1 cijfer
- Voor de activeringscode moet u een zogenaamde passphrase gebruiken. Dit is een voor de gebruiker makkelijk te onthouden zin (b.v. Ikvindmelknietlekker2006).
- Er moeten minimaal 2 lagen van fysieke toegangsbeveiliging zijn voordat er toegang is tot het systeem met de private sleutel. Denk hierbij aan bijvoorbeeld een afgesloten ruimte en een afgesloten serverkast waarin het systeem met de private sleutel zich bevindt.
- En tot slot, een schermbeveiliging die bij het verlaten van de ruimte geactiveerd wordt.

Als u gebruikt maakt van een HSM (Hardware Security Module) voor het genereren van het sleutelbaar en de beveiliging van de private sleutel die bij het servercertificaat hoort, is een aantal beveiligingseisen direct al ingevuld.

Naast de genoemde minimale set is het ook noodzakelijk om een goede risicoanalyse uit te voeren op basis van de NEN7510 norm (www.nen7510.org).