Een aantal UZI-servercertificaten (nodig om via UZI in de zorg onderling te communiceren) voldoen op dit moment niet aan bepaalde eisen en moeten daarom (versneld) vervangen worden. Dit heeft te maken met internationale regels die door grote internetbedrijven worden gesteld. Die regels veranderen continu. Alle betreffende zorgverleners hebben hier een e-mail en een brief over gekregen.

Waar kan ik terecht met vragen?
Als u vragen heeft kunt u ons bereiken per e-mail op info@uziregister.nl of contact opnemen met het *Klant Contact Centrum* (KCC) van het CIBG via 0900 – 232 43 42

Wat is er aan de hand?
Halverwege maart 2019 constateerde toezichthouder Logius dat een deel van de PKIoverheid-certificaten niet voldoet aan de gestelde uitgifte-eisen. Eind augustus 2019 stuurde Logius een herziende memo rond met daarin een aangepaste datum en de constatering dat door nieuwe inzichten een deel van de door het CIBG uitgegeven certificaten vervroegd vervangen moet worden. De betreffende servercertificaten moeten voor 1 oktober vervangen zijn.

Om welke certificaten gaat het?
Het gaat om 2800 UZI/ZOVAR-servercertificaten.

En om welke niet?
Certificaten uitgegeven vanaf 1 januari 2018 hoeven niet vervangen te worden. Deze worden enkel gebruikt voor verkeer in besloten groepen gebruikers (in dit geval gecertificeerde zorgverleners en organisaties). Omdat deze certificaten niet gebruikt worden voor openbaar internetverkeer in browsers worden gebruikt en hoeven niet te voldoen aan internationale eisen

Certificaten

Hoe weten zorgverleners om welke certificaten het gaat?
Er zijn drie manieren om hier achter te komen:
1. De datum van uitgifte van het certificaat. Het gaat om G21certificaten, dit zijn servercertificaten die uiterlijk 22 maart 2020 verlopen en tot 31 december 2017 zijn uitgegeven. Certificaten uitgegeven vanaf 1 januari 2018, hoeven **niet** vervangen te worden.
2. Via de e-mail en brief die de zorgorganisaties van het CIBG en VZVZ ontvangen hebben.
3. Zorgverleners of netwerkbeheerders bij zorgorganisaties kunnen dit zelf opzoeken in hun computersystemen. Controle van de eigenschappen van het certificaat: hiërarchie. In de eigenschappen valt in te zien onder welke hiërarchie een certificaat is uitgegeven. Certificaten die vervangen moeten worden zijn uitgegeven door de UZI-register Server CA G21 en/of ZOVAR Server CA G21.

Hoe weten de zorgorganisaties wat ze moeten doen?
Alle zorgverleners die het certificaat moeten vervangen hebben een e-mail en een vernieuwingsbrief ontvangen. Deze vernieuwingsbrieven zijn rond 29 augustus 2019 verzonden. Hulp staat klaar bij VZVZ voor 2/3 van de groep zorgverleners die aangesloten zijn bij het *Landelijk Schakelpunt* (LSP). De overige zorgverleners kunnen terecht bij het *Klant Contact Centrum* (KCC) van het CIBG.

Zijn de G21-certificaten nog wel veilig?
Ja het is veilig. Er is *geen* sprake van een beveiligingsrisico.

Wat is dan het probleem?
De certificaten die uitgegeven worden onder de publieke tak van het PKIo-stelsel moeten voldoen aan internationale eisen. Er is bijvoorbeeld regelgeving over hoe een parameter opgenomen mag worden in dit certificaat. Omdat de internationale gemeenschap voortdurend nieuwe inzichten heeft kan het voorkomen dat de kaders anders ingevuld moeten worden. Het gevolg is dat de servercertificaten van het CIBG niet overeenkomen m*et* de internationale standaard. Dat wordt ook wel *compliance* genoemd.

Hoe kan het dat na de bekendmaking van de striktere invulling van eisen pas zo laat bekend is geworden dat alles vervangen moet worden?

De striktere invulling van eisen lijkt twee keer onverwacht te zijn gekomen: 1 keer in maart en 1 keer bij de aanlevering van de certificaten van het verouderde type. Feitelijk was de eerste een verrassing (wereldwijd) en de tweede was bekend en werd gedoogd door Logius en BSI.

Maar dan is er toch eigenlijk niets aan de hand?
Het systeem werkt inderdaad maar voldoet op dit moment niet aan alle eisen en daarom is actie wel nodig.

Wat is een certificaat?
Het PKIoverheid-certificaat is een computerbestand dat fungeert als een digitaal paspoort voor personen of organisaties. Het bevat gegevens in de vorm van parameters in invulvelden die nodig zijn voor authentieke en geverifieerde elektronische gegevensuitwisseling. Digitale certificaten zijn een onmisbare schakel in beveiligd internetverkeer. Bij alle Logius-diensten heeft u een digitaal certificaat van PKIoverheid nodig. Dit waarborgt de betrouwbaarheid van informatie-uitwisseling.

Waar gebruik je een certificaat voor?
In het geval van het CIBG worden UZI-passen en servercertificaten verstrekt aan individuele zorgverleners en (medewerkers van) zorgorganisaties. Zowel de fysieke UZI-passen als de digitale servercertificaten bevatten een PKIoverheid-certificaat, dat de identiteit van de zorgverlener, zorgorganisatie of zorgpersoneel garandeert. Zo kunnen zorgverleners bijvoorbeeld het BSN van een cliënt checken, zodat Wim Jansen uit Appelscha niet opeens verward wordt met Wim Jansen uit Goeree. Ook kunnen zorgpraktijken gemakkelijk en snel onderling berichten uitwisselen die nodig zijn voor de behandeling van patiënten.

In het kort:
- Toegang Landelijk Schakelpunt
- Authenticatie
- Versleutelen van informatie
- Elektronische handtekening
- Smartcard logon

En specifiek servercertificaten?
Deze kunnen gebruikt worden voor interne administratie en communicatie tussen zorgverleners. Bijvoorbeeld om het beveiligd delen van informatie tussen machines mogelijk te maken (intern netwerk). Met een servercertificaat kan de gebruiker:
- In het elektronisch verkeer aangeven dat het systeem bij de zorgaanbieder behoort;
- Veilige verbinding met andere systemen opzetten;
- Gegevens versleuteld verzenden en opslaan;
- Vanuit het zorginformatiesysteem geautomatiseerd gebruik maken van de BSN-diensten van de SBV-Z (voor het gebruik van de BSN-diensten via de SBV-Z website is een UZI-pas nodig).

Wie maken de regels voor die PKI's eigenlijk?
De PKI-stelsels zijn wereldwijd gebaseerd op regels die samengesteld worden door een internationale open gemeenschap van browserpartijen (zoals Google, Apple, Microsoft, Mozilla), Certificate Authorities (zoals Logius), netwerkontwikkelaars, verkopers, onderzoekers en geïnteresseerden die zich via werkgroepen en online fora bezig houdt met de evolutie van het internet. Toetsing en certificering van ons PKIo vinden plaats op basis van he programma van Eisen van Logius, dit programma is gebaseerd op Europese ETSI/eIDAS regelgeving.

Wie beheert die PKIo dan?
Binnen de Rijksoverheid is BZK verantwoordelijk voor beleid op het gebied van gegevensuitwisseling. Agentschap Logius heeft binnen BZK de taak om internationale regels te vertalen in kaders en hier toezicht op te houden.

Vervangen certificaten

Waarom duurt het installeren van al die certificaten zo lang?
Met het behandelen van een aanvraag is een certificaat nog niet geïnstalleerd. Sommige zorgverleners hebben een vast onderhoudscontract met een softwareleverancier. Een van de grotere leveranciers gaf aan ongeveer drie certificaten per uur te kunnen vervangen. Een van de betrokken leveranciers moet ruim 600 servercertificaten vervangen, wat met de afgegeven tijdsindicatie minimaal 200 vervangingsuren zou betekenen.

Hoe worden de servercertificaten vervangen?
Van betreffende servercertificaten ontvangt de persoon die het UZI-servercertificaat heeft aangevraagd van ons een vernieuwingsbrief met het aanvraagformulier. Deze brieven zijn rond **29 augustus 2019** verzonden. Dit formulier moet vóór dinsdag 17 september aanstaande ingevuld aan ons, het CIBG, terug worden gestuurd.

Voldoen alle nieuwe certificaten aan de eisen?
Ja, als er een nieuw servercertificaat wordt aangevraagd dan voldoet dit aan de gestelde eisen.

Doen de UZI-passen het dan ook niet meer als het servercertificaat wordt ingetrokken?
De UZI-passen zijn niet gekoppeld aan het servercertificaat. De UZI-pas is persoonsgebonden en het servercertificaat betreft de systeem identiteit. Ook zonder servercertificaat kan een zorgverlener UZI-passen aanvragen en gebruiken.

Hoe worden de zorgverleners geholpen bij het installeren?
Zowel het CIBG als ketenpartner VZVZ (van het LSP, waar 2/3 van de zorgverleners bij aangesloten is) hebben ondersteuning ingericht en het aanvraagproces vergemakkelijkt.

De tijd om een servercertificaat aan te vragen is krap, wat nu?
Vanwege de tijdsdruk gaan we een aantal stappen in het controle- en uitgifteproces van deze servercertificaten iets aanpassen.

- Daar waar mogelijk kijken we of de domeintoets van het te vernieuwen certificaat weer/nog steeds is te gebruiken
- De identiteitsvaststelling gaat niet via Dynalogic. Als het nieuwe certificaat door dezelfde persoon wordt aangevraagd als het te vervangen certificaat, dan gebruiken we eenmalig de identiteitsvaststelling van de vorige keer. Als het nieuwe servercertificaat door een andere aanvrager wordt ingediend, dan doen we de identificatie telefonisch.

Krijgen de zorgverleners de resterende maanden vergoed?
Helaas is dat niet realistisch. De meeste van de 2800 servercertificaten zijn nog maar één of enkele maanden geldig, tot uiterlijk maart 2020. Restitutie van de resterende maanden à € 12,50 per maand zou onevenredig veel meer kosten aan uitzoekwerk en facturatie. Dat is ook niet wenselijk.