Grip op je eigen gezondheidsgegevens

PKIoverheid-certificaten binnen MedMij

MedMij ontvangt regelmatig vragen over PKIoverheid-certificaten rondom de inrichting, welke wanneer gebruikt mogen worden en hoe de certificaten te valideren. Met dit document geeft MedMij antwoord op deze vragen (en meer).

Auteur	Casper van der Harst
Versie	1
Datum	Mei 2021

Grip op je eigen gezondheidsgegevens

Inhoudsopgave

Grip op je eigen gezondheidsgegevens

1. Wat is PKIoverheid?

PKIoverheid is de public key infrastructure (PKI) van de Nederlandse overheid. Net als elke andere PKI is het een afsprakenstelsel om digitale certificaten uit te geven en te beheren. PKIoverheid wordt beheerd door Logius.

1.1. Welke certificaten zijn beschikbaar?

Er zijn twee soorten PKIoverheid-certificaten beschikbaar, namelijk:

- Persoonsgebonden certificaten
- Services servercertificaten

Binnen MedMij gebruik we alleen services-servercertificaten. Dit is een certificaat gebonden aan een organisatie en wordt uitgegeven aan apparaten, servers of groepen individuen. Het certificaat wordt gebruikt om de communicatie te beveiligen tussen elektronische (overheids)applicaties en diensten. Het gebruik omvat TLS-beveiligde websites (certificaten uit de EV-hiërarchie) en verbindingen tussen systemen (certificaten uit de G1-hiërarchie). Eén PKIoverheid services servercertificaat kan worden gebruikt voor meerdere voorzieningen.

1.2. Welke typen certificaten zijn beschikbaar?

Een PKIoverheid services servercertificaat kent twee soorten:

- een Public Root certificaat, certificaten uit de EV-hiërarchie.
- een Private Root certificaat, certificaten uit de G1-hiërarchie (Domein Private Services).

Servercertificaten zijn geschikt voor de beveiliging van verkeer tussen systemen en verkeer van/naar websites. Voor beide type certificaten geldt dat ze aan de eisen van PKIoverheid voldoen, veilig beheerd worden en een audit ondergaan door een derde, onafhankelijke partij. De certificaten verschillen op twee punten: de geldigheidsduur en de toepasbaarheid van het certificaat.

1.2.1. Public Root certificaten

Dit type certificaat wordt doorgaans gebruikt om websites te beveiligen. Een Public Root certificaat is ongeveer één jaar en één maand (397 dagen) geldig. Dit geldt voor nieuw uit te geven certificaten. Reeds uitgegeven certificaten behouden hun geldigheidsduur. Dit type certificaat is aangemeld bij softwareleveranciers, webbrowsers vertrouwen deze automatisch.

1.2.2. Private Root certificaten

Dit type certificaat wordt doorgaans gebruikt voor het beveiligen van communicatie tussen systemen. Een Private Root certificaat is drie jaar geldig. Dit type certificaat is niet aangemeld bij softwareleveranciers en webbrowser vertrouwen deze ook niet automatisch. Dit is echter geen belemmering als het certificaat gebruikt wordt voor berichtenverkeer tussen systemen. De systemen valideren zelf de certificaten, zoals verderop in dit document beschreven.

2. Beveiligen van verkeer

2.1 Welke vormen van verkeer kent MedMij?

Het MedMij Afsprakenstelsel kent twee vormen van verkeer, namelijk frontchannel- en backchannelverkeer. Beide varianten worden beveiligd door gebruik te maken van een (of meerdere) TLS-versie(s) die door NCSC als goed zijn beoordeeld (zie hoofdstuk 3).

2.1.1. Wat is frontchannelverkeer?

Bij frontchannelverkeer wordt via een User Agent gecommuniceerd met een natuurlijk persoon. In het geval van MedMij is een webbrowser de applicatie die dient als User Agent voor een natuurlijk persoon, oftewel de Zorggebruiker.

2.1.2. Beveiliging frontchannelverkeer

Om frontchannelverkeer te beveiligen moet gebruikgemaakt worden van een Public Root certificaat. Dit type certificaat is aangemeld bij softwareleveranciers en webbrowsers vertrouwen deze automatisch. Het certificaat moet geïnstalleerd worden op de nodes die een client levert, bijvoorbeeld de webservers waarop de webapplicaties staan die gebruikt worden door de zorggebruiker.

2.1.3. Wat is backchannelverkeer?

In tegenstelling tot frontchannelverkeer is er bij backchannelverkeer geen communicatie met een natuurlijk persoon. De communicatie verloopt tussen twee systemen/servers.

2.1.4. Beveiliging backchannelverkeer

In de communicatie tussen systemen moet gebruik gemaakt worden van een Private Root certificaat. De systemen moeten zelf valideren of een geldig certificaat wordt gebruikt.

3. Wat is TLS en hoe ondersteunt MedMij dit?

TLS (Transport Layer Security) zorgt ervoor dat data voor verzending naar gebruiker en/of website, of tussen verschillende systemen, versleuteld en onleesbaar wordt gemaakt. Dit voorkomt dat data onderschept kan worden.

Versie 1.4.0 van het MedMij Afsprakenstelsel verwijst naar versie 2.1 van ICT-Beveiligingsrichtlijnen voor Transport Layer Security van NCSC. Het afsprakenstelsel stelt dat uitsluitend de TLS-versies en algoritmesets die zijn beoordeeld met goed gebruikt mogen worden. MedMij hanteert een afwijking op deze regel, door TLS versie 1.2 tijdelijk toe te staan. Op het moment van publicatie van versie 1.4.0 van het afsprakenstelsel werd TLS-versie 1.3 nog niet door alle leveranciers ondersteund. MedMij-deelnemers zijn afhankelijk van deze leveranciers en kunnen daarom TLS-versie 1.3 niet aanbieden. Daarmee zijn alle deelnemers verplicht TLS-versie 1.2 tot nader order te blijven ondersteunen en waar mogelijk ook TLS-versie 1.3 aan te bieden. Tijdens de TLS-handshake moet de hoogst mogelijke versie gebruikt worden. Als beide partijen TLS-versie 1.3 ondersteunen, mag TLS-versie 1.2 dan ook niet worden gebruikt.

4. Validatie van certificaten

4.1. Wat moet gevalideerd worden?

Tijdens de validatie van de certificaten vindt controle plaats op de volgende punten:

1. Is het certificaat geldig en uitgegeven volgens de afgesproken protocollen?
2. Is het certificaat bij MedMij bekend onder de organisatie die het certificaat aanbiedt?
3. Is het aangeboden certificaat niet ingetrokken?

4.2. Geldigheid certificaat controleren

Bij backchannelverkeer moeten systemen de gebruikte certificaten controleren. Hierbij gaan we van de hiërarchie zoals door PKIoverheid wordt aangeboden:

- Stamcertificaat Staat der Nederlanden Private Root CA - G1
- Staat der Nederlanden Private Services CA - G1
- KPN PKIoverheid Private Services CA - G1
- QuoVadis PKIoverheid Private Services CA - G1
- Digidentity BV PKIoverheid Private Services CA - G1

Om verzoeken te kunnen controleren installeert de ontvangende partij het stamcertificaat (ofwel het rootcertificaat) op de eigen node. Tijdens de TLS-handshake worden de aangeboden certificaten gecontroleerd tegenover dit rootcertificaat. Als deze geldig is wordt de TLS-verbinding gelegd.
De verzoekende partij moet vooraf bij een door PKIoverheid erkende uitgever een certificaat aanschaffen. Bij een verzoek aan een server stuurt de verzoekende partij dit certificaat mee. Omdat de server alleen het rootcertificaat heeft, moet de verzoekende partij naast het eigen certificaat ook de tussenliggende certificaten meesturen. Dit betekent dat er drie certificaten meegestuurd worden, namelijk:

- Het eigen certificaat
- Het certificaat van de TSP (Trust Service Provider, KPN, Quovadis of Digidentity)
- Het Private Services CA – G1 certificaat van de Staat der Nederlanden

Het stamcertificaat mag niet worden meegestuurd, deze is al op de server aanwezig.

4.3. Hoe wordt gecontroleerd of een certificaat bij MedMij bekend is?

Ieder certificaat heeft een Common Name, in het geval van MedMij is dit hetzelfde als het domein waarvoor het certificaat gebruikt wordt. Dit is de domeinnaam zoals vastgelegd op de Stelselnode en toegevoegd aan de WHL (Whitelist). Deelnemers halen periodiek (ieder kwartier, 15 minuten) de WHL op en controleren of de domeinnaam bekend is bij de WHL. Als dit het geval is, valt het domein onder een MedMij-deelnemer en kan deze dus vertrouwd en geaccepteerd worden.

4.4. Hoe worden ingetrokken certificaten gecontroleerd?

Uitgegeven certificaten kunnen worden ingetrokken. Een ingetrokken certificaat is niet meer geldig en mag niet meer worden gebruikt. Omdat zowel eindcertificaten als de tussenliggende certificaten kunnen worden ingetrokken, moeten deze beiden worden gecontroleerd.

MedMij
Grip op je eigen gezondheidsgegevens

4.5. Tussenliggende certificaten

Bij de controle van de tussenliggende certificaten moet gebruik gemaakt worden van CRL (Certificate Revocation List). Een CRL is een lijst met certificaat-serienummers die herroepen zijn, niet meer geldig zijn en niet meer te vertrouwen zijn voor gebruikers.
Een CRL wordt periodiek beschikbaar gesteld. In het geval van PKIoverheid betekent dit dat CRL's ieder uur (60 minuten) worden gepubliceerd. Een gepubliceerde CRL blijft een dag (24 uur) geldig. Deelnemers moeten dus minimaal één keer per dag de CRL's updaten, maar wij raden aan dit elk uur (60 minuten) te doen.

4.6. Eindcertificaten

De eindcertificaten zijn op twee verschillende manieren te controleren. Ook voor deze certificaten worden CRL's gepubliceerd. Daarnaast is voor deze certificaten het gebruik van OCSP (Online Certificate Status Protocol) mogelijk. Omdat de tussenliggende certificaten met CRL gecontroleerd moeten worden en de nadelen van CRL binnen MedMij (nog) niet van toepassing zijn, raden we aan ook de eindcertificaten te controleren door gebruik te maken van CRL's.

4.7. Uitzonderingen

In navolging op Logius kunnen in het MedMij-netwerk de onder 'EV-Root' uitgegeven certificaten tijdelijk worden gebruikt voor machine2machine toepassingen. Een toekomstvaste oplossing voor machine2machine toepassingen is het gebruik van G1-certificaten.

Het voornemen is deze uitzondering te schrappen, zodra Logius het gebruik van de onder 'EV-Root' uitgegeven certificaten niet meer accepteert voor machine2machine toepassingen. Dit kan al dan niet met behulp van een snel door te voeren patch op het MedMij Afsprakenstelsel.

Zie **6c** in release 1.3.0 van het MedMij Afsprakenstelsel
Zie **6d** in release 1.4.0 van het MedMij Afsprakenstelsel

5. Vragen

Heb je nog vragen? Neem dan contact op met het MedMij-loket via info@medmij.nl.