Whitepaper
Thema: veiligheid

Beveiliging van het verkeer op netwerkniveau

MedMij
Grip op je eigen gezondheidsgegevens

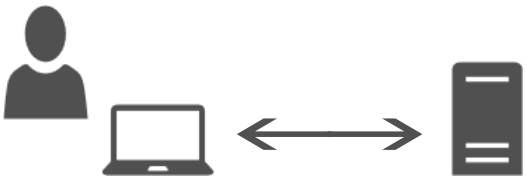
In deze whitepaper lees je meer over het volgende:

Voor de uitwisseling van gegevens is binnen het MedMij-netwerk een hoge mate van vertrouwen nodig. Dit vertrouwen wordt op verschillende niveaus gewaarborgd door de juiste inrichting en configuratie. Op het netwerkniveau betekent dit ook dat de beveiliging goed moet zijn ingericht. Vanuit het MedMij Afsprakenstelsel worden hier eisen aan gesteld.

MedMij ontvangt regelmatig vragen over de implementatie van deze beveiliging. Hoewel deze vragen natuurlijk individueel behandeld worden, is het ook belangrijk in een meer generieke vorm uitleg te geven. Waar het afsprakenstelsel de vereisten omschrijft, geeft dit document meer inzicht in het wat, hoe en waarom. Hierbij wordt ingegaan op de verschillende onderdelen die van toepassing zijn op de beveiliging van het netwerkverkeer.

Het verschil tussen frontchannel- en backchannelverkeer

Om te komen tot de beveiliging van het verkeer moet eerst duidelijk zijn welke vormen van verkeer onderscheiden worden. MedMij kent twee vormen van verkeer, namelijk frontchannelverkeer en backchannelverkeer. Voor sommigen zijn deze termen volkomen duidelijk, maar tegelijkertijd roepen ze bij anderen vragen op. Daarom hier de uitleg wat binnen MedMij bedoeld wordt als er gesproken wordt over frontchannel en backchannel.



Wat is frontchannelverkeer?

Voor de term frontchannel definieert het MedMij Afsprakenstelsel de volgende termen.

Frontchannelverkeer
Al het verkeer dat zichtbaar is voor een Persoon, vaak is hierbij een User Agent betrokken.

Hiermee is de term frontchannel nog niet altijd duidelijk. Wat is bijvoorbeeld een User Agent en is dit altijd een webbrowser, zoals in het MedMij Afsprakenstelsel beschreven wordt? En wat is voor de Persoon zichtbaar verkeer? Hieronder de antwoorden.

Wat is een User Agent?

Een zoektocht op internet brengt je al snel naar websites die ongeveer hetzelfde zeggen. Neem bijvoorbeeld de website van W3C (World Wide Web Consortium), één van de belangrijkste organisaties die verantwoordelijk is voor het ontwikkelen en vaststellen van standaarden die voor het web gelden. Zij definiëren User Agent als volgt:
A user agent is any software that retrieves, renders and facilitates end user interaction with Web content, or whose user interface is implemented using Web technologies.
Direct rijst tegenwoordig de vraag hoe het dan zit met native applications op de mobiele telefoon (mobiele applicaties). Moeten die ook tot User Agent worden gerekend, of is dat toch wat anders? In het kort is het antwoord 'ja', er is namelijk over het publieke internet verkeer met (interactie). Bijvoorbeeld moeten de getoonde gegevens worden opgehaald? Hiervoor worden webtechnologieën gebruikt.

Zichtbaarheid van frontchannelverkeer

Zoals hierboven ook beschreven is, kent het afsprakenstelsel een definitie voor frontchannelverkeer. Hierin wordt gesproken over zichtbaarheid voor de gebruiker. Nu is de vraag natuurlijk wat als zichtbaar voor de gebruiker wordt gezien. Binnen MedMij wordt al het verkeer tussen User Agent en DVP Server én het verkeer tussen User Agent en Authorization Server gezien als frontchannelverkeer.

Wat is backchannelverkeer?

Backchannelverkeer is eenvoudiger uit te leggen dan frontchannelverkeer. Het MedMij Afsprakenstelsel definieert dit als volgt:

Backchannelverkeer
Verkeer dat niet zichtbaar is voor een Persoon. Het gaat hierbij om verkeer tussen servers uit verschillende domeinen, die zonder tussenkomst van een Persoon met elkaar communiceren.

De definitie zegt dat het om verkeer gaat tussen servers en dat er geen tussenkomst is van een Persoon, oftewel een gebruiker. Hiermee wordt bedoeld dat de gebruiker geen direct inzicht heeft (en kan hebben) in de wat en hoe betreffende de communicatie. Dit type communicatie is tussen twee partijen, buiten de gebruiker om.

Het verkeer dat overblijft

Zoals bij frontchannelverkeer beschreven staat, is er ook voor de gebruiker onzichtbaar verkeer tussen User Agent en Server. Het afsprakenstelsel zegt niets over dit type communicatie. De gebruiker ziet hier niets van, maar zonder deze communicatie heeft een PGO geen waarde. De gegevens worden bijvoorbeeld opgehaald, zodat de grafische omgeving deze kan tonen.

Omdat zichtbaar frontchannelverkeer bij het gebruik van een User Agent beveiligd moet worden, kan het niet zichtbare verkeer op dezelfde manier beveiligd te worden. Maar dat hoeft niet. Het niet zichtbare verkeer wordt door MedMij als blackbox beschouwd, iets dat zich binnen de applicatie en haar directe omgeving te maken heeft. Een ontwikkelaar van een User Agent gebaseerde applicatie kan kiezen om het op dezelfde manier te beveiligen als het zichtbare gedeelte. Zodra er geen gebruik wordt gemaakt van een User Agent gebaseerde applicatie is dit anders. Bijvoorbeeld bij het gebruik van mobiele applicaties. Deze applicaties moeten voldoen aan de eisen van bijvoorbeeld Apple, voordat de applicaties in de store komen te staan. Identificatie en authenticatie van de leverende partij hoort hierbij. Daar zegt het afsprakenstelsel dan ook niets over. Maar ook mobiele applicaties moeten gegevens ophalen om deze te kunnen tonen. Ook dit wordt als een blackbox beschouwd.

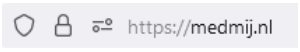
Beveiliging met certificaten

Voor de beveiliging van het verkeer wordt op het netwerk van MedMij gebruikgemaakt van in het algemeen gebruikte standaarden. Voor communicatie betekent dit dat gebruikgemaakt wordt van TLS (Transport Layer Security). Door gebruik te maken van TLS kunnen partijen elkaar authenticeren en wordt al het verkeer versleuteld. TLS komt binnen het MedMij netwerk in twee smaken, één voor al het frontchannelverkeer en één voor al het backchannelverkeer. Bij beide vormen wordt gebruikgemaakt van zogenoemde certificaten. Een certificaat kan worden vergeleken met een paspoort. Het bevat bijvoorbeeld gegevens over de identiteit van de server, de uitgever van het certificaat en tot wanneer het certificaat geldig is.

Verschillende typen certificaten

Organisatievalidatie-certificaten (OV) voor het frontchannelverkeer

Certificaten zijn te verdelen in drie typen, met een oplopend niveau van controle op de identiteit van de aanvrager: Domeinvalidatie (DV), Organisatievalidatie (OV) en Uitgebreide validatie (EV). Voor frontchannelverkeer binnen het MedMij netwerk wordt gebruikgemaakt van OV-certificaten, waarbij de leverancier van OV-certificaten (TSP) gevestigd is in een EU-/EER-land. De reden hiertoe is dat dit type certificaten zorgen voor een onmiddellijke bevestiging van de identiteit de bezochte website en het achterliggende bedrijf. Bij de aanschaf van dit type certificaat wordt namelijk de organisatie op een gestandaardiseerd niveau gecontroleerd. Alleen als zeker is dat het echt om de aanvragende organisatie gaat, wordt het certificaat uitgegeven.



Om de organisatie kunnen authenticeren, moeten gebruikers het certificaat kunnen inzien. Als er sprake is van een beveiligde verbinding, toont de gebruikte webbrowser een slotje bij de adresbalk.

Als de gebruiker op het slotje klikt en de details van het certificaat opent, staat daar de naam van de organisatie die eigenaar is van het certificaat.

DV-certificaten hebben deze eigenschap niet, omdat bij dit type certificaten alleen het bezit van (of controle hebben over) een domein gecontroleerd wordt bij de aanvraag, niet de identiteit van de aanvrager. Bij de uitgifte van een DV-certificaten is niet zeker welke organisatie de aanvraag heeft ingediend. Authenticatie van deze partij is daarom ook later niet mogelijk door gebruik te maken van een DV-certificaat.
Het gebruik van OV-certificaten is binnen MedMij alleen verplicht op de productieomgevingen. Op test- en ontwikkelomgevingen mag wel gebruik worden gemaakt van DV-certificaten.

PKIoverheid G1-certificaten voor het backchannel verkeer

G1-certificaten die vallen onder PKIoverheid worden gebruikt voor al het backchannelverkeer binnen het MedMij netwerk. Dit zijn certificaten die onder de verantwoordelijkheid van de Nederlandse overheid door een aantal partijen wordt uitgegeven. Deze certificaten zijn speciaal bedoeld om servers te beveiligen in server-to-server communicatie.
De verificaties zijn bij G1-certificaten strenger dan bij OV-certificaten. Net als bij OV-certificaten wordt de organisatie nagegaan, maar de controles zijn een stuk preciezer. Voor een G1-certificaat zijn meerdere extra stappen vereist, waaronder de verificatie van een openbaar bedrijfstelefoonnummer, de vestigingsdatum van het bedrijf en het inschrijvingsnummer. De aanvrager wordt ook gebeld om te controleren of de aanvrager ook werkelijk bij het bedrijf werkt. Binnen MedMij wordt vertrouwd op de betrouwbaarheid van het PKIoverheid stelsel, gecombineerd met de MedMij whitelist. De MedMij Whitelist wordt later beschreven.

Multi-domein certificaten

Certificaten zijn bruikbaar voor één of meerdere websites. Een certificaat bestaat uit verschillende velden. Het belangrijkste veld is de Common Name. Daarnaast kan ook gebruikgemaakt worden van Subject Alternative Names (SAN). Met beide type velden kan een certificaat aangeven door meerdere websites gebruikt te kunnen worden. Binnen MedMij wordt alleen het gebruik van Subject Alternative Names geaccepteerd. Dit moet wel uitgelegd worden.

De Common Name bevat de hostname, het eerste deel van het adres van de website (de URL), van de website die met het certificaat beveiligd wordt. Je zou kunnen zeggen dat daarmee de hostname gelijk is aan de URL die door de gebruiker in de adresbalk van de webbrowser is ingevoerd. Maar, in de Common Name kan gebruikgemaakt worden van zogenoemde wildcards. Een voorbeeld:

Een MedMij-website is te benaderen door https://medmij.nl in de adresbalk in te voeren. Hoewel MedMij hier geen gebruik van maakt, is het heel gebruikelijk de website ook met www te kunnen benaderen. Hiervoor zou de gebruiker dan https://www.medmij.nl moeten invoeren. Twee adressen en in de basis dus twee certificaten. Door in het certificaat gebruik te maken van een wildcard, is één certificaat genoeg. De Common Name van het certificaat verwijst in dit geval naar *.medmij.nl. '*' is in dit geval de wildcard en wordt door de browser vervangen door het eerste deel van het ingevoerde adres. https://medmij.nl pas binnen *.medmij.nl en https://www.medmij.nl ook.

Wildcard-certificaten worden gebruikt om meerdere servers te configureren om zo het beheer te vereenvoudigen en geld te besparen. Maar er kleven ook flinke risico's aan het gebruik hiervan. Als een hacker de unieke sleutel (private key) te pakken krijgt, kan hij een eigen omgeving met dit certificaat beveiligen. https://geefmijjouwgegevens.medmij.nl voldoet namelijk ook aan *.medmij.nl. De gebruiker denkt nog steeds op een omgeving van MedMij te werken, maar geeft zonder het te weten alle gegevens aan de hacker. Om deze reden worden wildcards verboden vanuit het MedMij afsprakenstelsel.

Om toch met één certificaat meerdere website te beveiligen, kan gebruik worden gemaakt van Subject Alternative Names. Hierbij bevat de Common Name één van de hostnames die met het certificaat beveiligd moeten zijn en worden de anderen toegevoegd als SAN. Hierboven is in het plaatje te zien dat de Common Name op het certifcaat van MedMij www.medmij.nl is. Deze staat op hetzelfde certificaat ook als SAN, net als medmij.nl.

NEN7510:2017 paragraaf 12.1.4 beschrijft dat productieomgevingen gescheiden moeten zijn van test- en ontwikkelomgevingen. Dit geldt niet alleen voor servers en databases, maar ook voor certificaten. Gebruik het certificaat van de productieomgeving daarom niet voor de test- en ontwikkelomgevingen, maar installeer daar een ander certificaat. Plaats de test- en ontwikkelomgevingen niet als SAN op het certificaat van de productieomgeving

TLS met OV certificaten voor frontchannel verkeer

TLS staat voor Transport Layer Security en is het protocol waarmee frontchannel verkeer wordt beveiligd. Wanneer een webbrowser toegang probeert te krijgen tot een beveiligde website, wordt een TLS-verbinding wordt gemaakt. Dit proces is niet zichtbaar voor de gebruiker, maar het resultaat wel, in de vorm van het slotje in de browser. Binnen MedMij wordt zoveel als mogelijk TLS versie 1.3 gebruikt. Indien dit niet mogelijk is, mag teruggevallen worden op versie 1.2.

De verbinding wordt beveiligd voordat er gegevens worden gecommuniceerd. Dus nog voordat de webbrowser de gegevens ophaalt waarmee de grafische omgeving wordt opgebouwd. Dit gaat als volgt:

1. De webbrowser stuurt een verzoek naar een webserver. Hierbij wordt binnen MedMij verplicht gebruikgemaakt van HTTPS. In dit verzoek vraagt de webbrowser de server om zich te identificeren.
2. De server stuurt een kopie van zijn certificaat (en de bijbehorende intermediate certificaten van certifcaatuitgever), inclusief de publieke sleutel (public key) waar de webbrowser gebruik van kan maken.
3. De webbrowser controleert het certificaat op betrouwbaarheid en of het niet verlopen of ingetrokken is. Als de identiteit van de server door de webbrowser vertrouwd wordt, maakt de browser een code, dit wordt ook wel de symmetric session key genoemd. Deze code geldt alleen voor de lopende sessie en wordt voor de beveiliging van de communicatie gebruikt. De code wordt door de webbrowser versleuteld. Hiervoor gebruikt de webbrowser de publieke sleutel die de server in stap 2 stuurde. De versleutelde code wordt naar de server gestuurd.
4. De server heeft een geheime unieke sleutel (private key), behorende bij de publieke sleutel, waarmee de server kan controleren of de code op de juiste manier versleuteld is. Als dit het geval is, stuurt de server een ontvangstbevestiging naar de webbrowser, waarbij dit bericht wordt versleuteld met de code die de server van de webbrowser ontving.
5. Vanaf dit moment is de verbinding tussen webbrowser en server beveiligd en worden alle berichten versleuteld met de code.

mTLS met G1 certificaten voor backchannel verkeer

Ook het backchannel verkeer moet goed beveiligd worden. Hiervoor wordt gebruikgemaakt van mTLS (mutual TLS, dus tweezijdig), een variant op het eerder genoemde TLS. In deze vorm moeten beide servers elkaar kunnen identificeren, voordat er gegevens worden uitgewisseld. Dit werkt als volgt:

1. De vragende server (de client) start door aan te geven een verbinding te willen maken met een ontvangende server (de server). Hierbij geeft de client direct informatie mee over zijn voorkeuren van beveiliging.
2. De server antwoord onder andere met de gekozen beveiligingsmethoden (TLS versie en cipher suite) en zijn G1 certificaat.
3. De client controleert de geldigheid van het ontvangen certificaat en leest de publieke sleutel. De client stuurt zijn G1 certificaat de server.
4. De server controleert het certificaat van de client. Als alles goed gegaan is hebben beide partijen nu dezelfde beveiligingsinformatie. Deze beveiligingsinformatie is uniek per sessie en wordt door beide partijen gebruikt om gegevens de versleutelen en ontsleutelen. De server geeft de client toegang tot zijn gegevens (resources)
5. Vanaf dit moment is de verbinding tussen de client en de server beveiligd en wordt alle berichten versleuteld

Verificatie van gebruikte certificaten

Gebruikte certificaten worden in het MedMij netwerk op verschillende manieren gecontroleerd. Zo moeten de uitgevers van de gebruikte certificaten vertrouwd worden. Door gebruik te maken van PKIoverheid-certificaten wordt de betrouwbaarheid van backchannel-certificaten gewaarborgd. Voor frontchannel-certificaten is dit wat lastiger, maar moet vertrouwd worden op de betrouwbaarheid van de leveranciers van gebruikte webbrowsers. Daarnaast zijn er nog twee methodes om de betrouwbaarheid te waarborgen.

Geregistreerde certificaten op de whitelist

Deelnemers van MedMij moeten de door hun gebruikte hostnames registreren bij MedMij Beheer. Dit zijn dezelfde hostnames die ook als Common Name of Subject Alternative Name zijn bekend zijn op het gebruikte certificaat. Geregistreerde certificaten worden op de zogenoemde whitelist (WHL) gezet, die ieder kwartier door de deelnemers opgehaald moet worden. Zo kunnen de deelnemers altijd controleren of een bepaalde hostname door MedMij geaccepteerd is en of het certificaat gebruikt mag worden.

Controle op basis van CRL en OCSP

De geldigheid van certificaten wordt niet alleen bepaald door de duur en de registratie bij MedMij Beheer. Certificaten kunnen ook door uitgevende partijen worden ingetrokken. Hier kan op twee manieren mee worden omgegaan, namelijk volgens de principes van CRL en OCSP. Vanuit het MedMij Afsprakenstelsel is CRL de primaire variant, maar mag ook gebruik worden gemaakt van OCSP.

Certificate Revocation List (CRL)

Bij CRL levert de uitgever ieder uur een lijst van ingetrokken certificaten. Partijen die een door deze uitgever uitgeven certificaat willen controleren, dienen de lijst ieder uur op te halen. Zodra een certificaat geverifieerd wordt, controleren zij of het ontvangen certificaat op de lijst staat. Zo ja, dan wordt de verbinding verbroken. Belangrijke nadelen van CRL zijn het feit dat de hele lijst ieder uur opgehaald moet worden en dat de lijst lang kan worden. In dat laatste geval kan het doorzoeken van de lijst de performance van de server verlagen. Toch is CRL de bovenliggende variant ten opzichte van OCSP. Niet alle uitgevers ondersteunen OCSP en als een CRL-lijst een keer niet beschikbaar is, mag de oude lijst maximaal 24 uur gebruikt worden. Het ophalen van een lijst mag daarom een aantal keer misgaan, voordat alle verzoeken worden geweigerd.

Online Certificate Status Protocol (OCSP)

Bij OCSP wordt uitgegaan van een online service waar de geldigheid van een certificaat kan worden nagevraagd. De verifiërende partij stuurt een verzoek naar de OCSP-server, die antwoord met het feit of het certificaat ingetrokken is. Dit is voor de verzoekende partij veel eenvoudiger, maar ook hier hangt een aantal nadelen aan. De OCSP-server kan bijvoorbeeld niet beschikbaar zijn. In tegenstelling tot CRL mag geen gebruikgemaakt worden van oudere gegevens, waardoor een certificaat niet gecontroleerd kan worden. Omdat de verzoekende partij de controle niet zelf uitvoert en geen gegevens heeft over ingetrokken certificaten, kan de verzoekende partij niets anders dan een certificaat weigeren.