RFC0065 (Patch), AF-1349 Gebruik publieke certificaten in afsprakenstelsel 1.5

1. Samenvatting

Waarom is deze RFC nodig?	PKIOverheid stopt per 4 december 2022 met het aanbieden van publieke certificaten. Bij al het frontchannel verkeer binnen MedMij, alsmede mogelijk bij een deel van het backchannel verkeer, wordt gebruiktgemaakt van deze publieke (EV) certificaten.
Oplossingsrichting	Deelnemers moeten voor 4 december 2022 overgestapt zijn naar andere publieke certificaten voor frontchannel verkeer. Deze certificaten moeten aan een nieuwe set van eisen voldoen, die zijn overgenomen uit de beleidslijnen van VWS. Daarnaast moeten publieke certificaten die gebruikt worden voor backchannel verkeer vervangen worden door PKIoverheid private (G1) certificaten. Nieuwe deelnemers moeten direct gebruikmaken van andere publieke certificaten voor frontchannelverkeer, voor backchannel verkeer gebruiken zij direct PKIoverheid private (G1) certificaten.

RACI	• Responsible: Casper van der Harst
	• Accountable: Egbert van Gelder
	• Consulted
	  • Ontwikkelteam (ontwikkeling@medmij.nl)
	  • Security Management (secmgt@medmij.nl)
	  • Acceptatie (acceptatie@medmij.nl)
	  • Stelselregie
	  • Deelnemers (Expertgroepsessie)
	• Informed
	  • Communicatie
	  • Loket (info@medmij.nl)
	  • Leveranciersmanagement

Aanpassing van	Afsprakenstel versie 1.5 en 1.6 4 december 2022 moeten de uitzonderingen verwijderd worden uit afsprakenstelsel versie 1.6 en 1.7, zoals in de uitzonderingen benoemd is.
Impact op rollen	MedMij Beheer, DVP, DVA
Impact op beheer	Bestaand proces moet gevolgd worden.
Impact op RnA	Bestaand proces moet gevolgd worden.
Impact op Acceptatie	Proces blijft hetzelfde, controle op de certificaten wordt net wat anders.
PIA noodzakelijk	
Gerelateerd aan (Andere RFCs, PIM issues)	• AF-1349, Gebruik publieke certificaten in afsprakenstelsel 1.5 • RFC0064 (Patch), AF-1329 Gebruik publieke certificaten in afsprakenstelsel 1.4
Motivatie verkorte RFC procedure (patch)	Binnen een jaar zijn de publieke certificaten van PKIoverheid niet meer te gebruiken. Het is van belang de deelnemers in het aankomende jaar goed te begeleiden en te informeren. Om de deelnemers goed voor te bereiden op deze wijziging, is daarom gekozen een wijziging door te voeren op de versies 1.4 en 1.5 van het afsprakenstelsel.

2. Uitwerking epic

Uitwerking Epic AF-1273, PKIoverheid stopt met uitgeven publiek vertrouwde webserver (SSL/TLS) certificaten

3. Wijzigingen afsprakenstelsel

3.1. Beveiliging

Huidige inhoud	Nieuwe inhoud

2.	De *OAuth Client* en *OAuth Authorization Server* gebruiken voor al hun onderlinge verkeer PKIoverheid-certificaten, en wel servercertificaten, ten behoeve van de authenticatie van de andere server in een uitwisseling. Dit is een maatregel tegen beveiligingsrisico's 4.4.1.1, 4.4.1.3, 4.4.1.4 en 4.4.1.5 in RFC 6819. De PKI-certificaten worden in deze release van het MedMij Afsprakenstelsel gebruik voor twee doelen op de Netwerklaag: authenticatie van servers en versleuteling, waarmee de vertrouwelijkheid en integriteit van de inhoud van het gegevensverkeer wordt geborgd.	core.beveiliging.201

2.	De *OAuth Client* en *OAuth Authorization Server* gebruiken voor al hun onderlinge verkeer PKI-certificaten, en wel servercertificaten, ten behoeve van de authenticatie van de andere server in een uitwisseling. Dit is een maatregel tegen beveiligingsrisico's 4.4.1.1, 4.4.1.3, 4.4.1.4 en 4.4.1.5 in RFC 6819. De PKI-certificaten worden in deze release van het MedMij Afsprakenstelsel gebruik voor twee doelen op de Technologielaag: authenticatie van servers en versleuteling, waarmee de vertrouwelijkheid en integriteit van de inhoud van het gegevensverkeer wordt geborgd.	core.beveiliging.201

3.2. TLS en certificaten

Huidige inhoud

	frontchannel-verkeer	**uitgaand backchannel-verkeer**	**inkomend backchannel-verkeer**
versleuteling volgens TLS, met PKIoverheid-certificaat	altijd		
identificatie op basis van ...	`redirect_uri` of *Zorgaanbiederslijst*		PKIoverheid-certificaat
authenticatie, op basis van PKIoverheid-certificaat, van ...	alleen de TLS-server	TLS-client én TLS-server	
autorisatie op basis van controle tegen de *Whitelist*	niet	voorafgaand aan de TLS-handshake	zie verantwoordelijkheid 14a

Nieuwe inhoud

	frontchannel-verkeer	**uitgaand backchannel-verkeer**	**inkomend backchannel-verkeer**
versleuteling volgens TLS	altijd		
identificatie op basis van ...	`redirect_uri` of *Zorgaanbiederslijst*		PKIoverheid-certificaat
authenticatie, op basis van PKI-certificaat, van ...	alleen de TLS-server	TLS-client én TLS-server	
autorisatie op basis van controle tegen de *Whitelist*	niet	voorafgaand aan de TLS-handshake	zie verantwoordelijkheid 14a

7.	Om zich te kunnen authenticeren en autoriseren op het *MedMij-netwerk*, kunnen alle *Backchannel Nodes* een PKIoverheid-certificaat overleggen, en wel een server-certificaat van een *PKIoverheid TSP*.	core.tls.306

~~7.~~	~~Om zich te kunnen authenticeren en autoriseren op het *MedMij netwerk*, kunnen alle *Backchannel Nodes* een PKIoverheid certificaat overleggen, en wel een G1 certificaat van een *PKIoverheid TSP*.~~	~~core.tls.306~~

7	Voor authenticatie en autorisatie bij backchannel-verkeer op het *MedMij-netwerk*, kunnen elke *PGO Node*, elke *ZA Node* en de *MedMij Stelselnode* een PKIoverheid-certificaat overleggen, en wel een G1-certificaat van een *PKIoverheid TSP*.
	
	• Private Root CA (per medio 2020 de standaard voor m2m)
	  • Stamcertificaat
	  • Staat der Nederlanden Private Root CA - G1
	  • Domein Private Services, maar alleen de volgende:
	  • 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
	
	Uitzondering
	
	Partijen die op <DATUM> al *Deelnemer* van MedMij waren en gebruikmaken van een publiek certificaat voor de beveiliging van hun backchannel-verkeer, kunnen dit certificaat tot uiterlijk 4 december 2022 gebruiken. Hierna is het gebruik van een privaat (G1) certificaat van *PKIoverheid* ook voor deze deelnemers verplicht voor de beveiliging van al het backchannel-verkeer en zal deze uitzondering verwijderd worden.
	
	• Stamcertificaat
	  • Staat der Nederlanden EV Root CA
	  • Intermediair Domein Server CA 2020
	  • QuoVadis PKIoverheid Server CA 2020
	  • Digidentity PKIoverheid Server CA 2020
	  • KPN PKIoverheid Server CA 2020
		core.tls.314

8	Voor authenticatie en autorisatie bij frontchannel-verkeer tussen productieomgevingen op het *MedMij-netwerk*, kunnen elke *PGO Node*, elke *ZA Node* en de *MedMij Stelselnode* een PKI-certificaat overleggen dat aan de volgende eisen voldoet: 1. De vereisten aan de certificaat leverancier voor PKI certificaten zijn: a. De meest up-to-date WebTrust audit is succesvol doorlopen en de certificering is geldig voor de 'Certificatie Authority' op iedere schakel in de keten van ondertekeningen tot en met de uitgifte processen. 2. De technische vereisten zijn: a. De 'private key' moet worden gegenereerd op het doelplatform waar het PKI certificaat wordt toegepast. b. Bij gebruik van publieke PKI certificaten is de toepassing van 'Certification Authority Authorization Resource Record' vereist. c. Het toepassen van DNSSEC op de gebruikte domeinen is vereist onder de voorwaarden van pas-toe-of-leg-uit. Strengere eisen kunnen worden gesteld vanuit aanvullende kaders, zoals aansluitvoorwaarden. d. Het gebruik van wildcard certificaten wordt niet toegestaan. e. Het gebruik van 'multi-domain'-certificaten is toegestaan, onder de voorwaarde dat de eigenaar van het certificaat gelijk is aan de eigenaar van alle domeinen die opgenomen zijn in de Subject Alt Name DNS waarden van het certificaat. 3. Uitgifte: a. Het zekerheidsuitgifte niveau moet minimaal op het OV-niveau (Organisation Validated) of met hogere zekerheid zijn uitgegeven voor publieke PKI webserver certificaten wanneer persoonsgegevens van bijzondere aard worden verwerkt. Dit is relevant voor de aanschaf van het certificaat en dit valt achteraf te controleren op het bestaan van Policy Object Identifiers (OIDs) die markeren welk type certificaat het betreft. b. De uitgever van de PKI certificaten is verantwoordingsplichtig aan de AVG en/of GDPR. 4. Beheer: a. Veilig beheer moet zijn toegepast zoals toegelicht in 'Factsheet Veilig beheer van digitale certificaten'. **Uitzondering** Partijen die op <DATUM> al *Deelnemer* van MedMij waren en gebruikmaken van een publiek certificaat voor de beveiliging van hun frontchannel-verkeer, kunnen dit certificaat tot uiterlijk 4 december 2022 gebruiken. Hierna is het gebruik van publiek certificaat dat voldoet aan de hierboven genoemde eisen verplicht en zal deze uitzondering verwijderd worden. • Stamcertificaat • Staat der Nederlanden EV Root CA • Intermediair Domein Server CA 2020 • QuoVadis PKIoverheid Server CA 2020 • Digidentity PKIoverheid Server CA 2020 • KPN PKIoverheid Server CA 2020	core.tls.315

8.	Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het PKIoverheid-stelsel. Een organisatie mag meerdere certificaten hebben. De keuze voor de PKI-standaard past bij principe 19 van het MedMij Afsprakenstelsel. Er bestaan andere manieren voor, en ideeën over, het borgen van vertrouwen in een netwerk van geautomatiseerde systemen, maar deze zijn nog lang niet zo bewezen als PKI, dat wereldwijd wordt ondersteund, en wereldwijd is beproefd, door overheden en marktspelers. Bij gebruik van de PKI-standaard doet zich de vraag voor van welk(e) PKI-stelsel(s) gebruik gemaakt kan of moet worden. Zo'n PKI-stelsel voorziet in een hiërarchie van organisaties die certificaten uitgeven, zodanig dat de betrouwbaarheid van de certificaten van zo'n organisatie leunt op de betrouwbaarheid van de eerst-hogere organisatie in die hiërarchie, doordat de certificaten van de lagere-in-hiërarchie een handtekening hebben van die van de hogere-in-hiërarchie. Aan de top van zo'n hiërarchie staat een zogenoemde root Certificate Authority (root CA) die zijn betrouwbaarheid niet aan een hogere kan ontlenen, zijn eigen (stam)certificaten tekent, en zo een steunpilaar is van het vertrouwen in het hele betreffende PKI-stelsel. Het MedMij Afsprakenstelsel had ervoor kunnen kiezen een PKI-stelsel specifiek voor MedMij in te richten, maar de kosten daarvan, voor zichzelf en voor haar deelnemers, wegen niet op tegen de voordelen, onder de voorwaarde dat er een ander geschikt PKI-stelsel voorhanden is. Deelnemers zullen met hun services immers ook in andere afsprakenstelsels betrokken kunnen zijn dan dat van MedMij. Zo'n keuze past bovendien niet bij principe P6. Omdat het MedMij-netwerk een nationale en maatschappelijk kritische infrastructuur is, met hoge eisen aan betrouwbaarheid, kiest het MedMij Afsprakenstelsel voor het momenteel enige PKI-stelsel waarin de betrouwbaarheid uiteindelijk steunt op een Nederlandse publiekrechtelijke rechtspersoon: PKIoverheid met de Staat der Nederlanden als root CA. Zo is de governance van de root CA transparant en toegankelijk belegd. Het MedMij Afsprakenstelsel bouwt voor het door hem aan zijn deelnemers geboden vertrouwen dus mede op het PKIoverheid-stelsel, op het door dat stelsel vastgestelde programma van eisen voor de in dat stelsel betrokken TSP's en op de certificatiehiërarchie van PKIoverheid. Deelnemers in het MedMij Afsprakenstelsel zullen dus service-certificaten moeten betrekken bij een bij PKIoverheid aangesloten TSP die bij haar past.	core.tls.307
10.	Alle *Backchannel Nodes* valideren tijdens de TLS-handshake aan het begin van een TLS-sessie of het een PKIoverheid-certificaat is en controleren bij de *Certification Authority* of het ontvangen certificaat geldig is, op basis van CRL of OCSP. In geval van het falen van één van deze controles wordt het certificaat niet geaccepteerd en de TLS-sessie niet gestart.	core.tls.309

8.	Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het PKI-stelsel waarvan zij een certificaat afnemen. Een organisatie mag meerdere certificaten hebben. De keuze voor de PKI-standaard past bij principe 19 van het MedMij Afsprakenstelsel. Er bestaan andere manieren voor, en ideeën over, het borgen van vertrouwen in een netwerk van geautomatiseerde systemen, maar deze zijn nog lang niet zo bewezen als PKI, dat wereldwijd wordt ondersteund, en wereldwijd is beproefd, door overheden en marktspelers. Bij gebruik van de PKI-standaard doet zich de vraag voor van welk(e) PKI-stelsel(s) gebruik gemaakt kan of moet worden. Zo'n PKI-stelsel voorziet in een hiërarchie van organisaties die certificaten uitgeven, zodanig dat de betrouwbaarheid van de certificaten van zo'n organisatie leunt op de betrouwbaarheid van de eerst-hogere organisatie in die hiërarchie, doordat de certificaten van de lagere-in-hiërarchie een handtekening hebben van die van de hogere-in-hiërarchie. Aan de top van zo'n hiërarchie staat een zogenoemde root Certificate Authority (root CA) die zijn betrouwbaarheid niet aan een hogere kan ontlenen, zijn eigen (stam)certificaten tekent, en zo een steunpilaar is van het vertrouwen in het hele betreffende PKI-stelsel. Het MedMij Afsprakenstelsel had ervoor kunnen kiezen een PKI-stelsel specifiek voor MedMij in te richten, maar de kosten daarvan, voor zichzelf en voor haar deelnemers, wegen niet op tegen de voordelen, onder de voorwaarde dat er een ander geschikt PKI-stelsel voorhanden is. Deelnemers zullen met hun services immers ook in andere afsprakenstelsels betrokken kunnen zijn dan dat van MedMij. Zo'n keuze past bovendien niet bij principe P6. Omdat het MedMij-netwerk een nationale en maatschappelijk kritische infrastructuur is, met hoge eisen aan betrouwbaarheid, kiest het MedMij Afsprakenstelsel voor de beveiliging van al het backchannel-verkeer voor het momenteel enige PKI-stelsel waarin de betrouwbaarheid uiteindelijk steunt op een Nederlandse publiekrechtelijke rechtspersoon: PKIoverheid met de Staat der Nederlanden als root CA. Zo is de governance van de root CA transparant en toegankelijk belegd. Het MedMij Afsprakenstelsel bouwt ondermeer voor het door hem aan zijn deelnemers geboden vertrouwen dus mede op het PKIoverheid-stelsel, op het door dat stelsel vastgestelde programma van eisen voor de in dat stelsel betrokken TSP's en op de certificatiehiërarchie voor private G1 certificaten van PKIoverheid. Deelnemers in het MedMij Afsprakenstelsel zullen dus service-certificaten moeten betrekken bij een bij PKIoverheid aangesloten TSP die bij haar past.	core.tls.307
10.	Alle *Backchannel Nodes* valideren tijdens de TLS-handshake bij backchannel-verkeer aan het begin van een TLS-sessie of het een PKIoverheid-certificaat is en controleren bij de *Certification Authority* of het ontvangen certificaat geldig is, op basis van CRL of OCSP. In geval van het falen van één van deze controles wordt het certificaat niet geaccepteerd en de TLS-sessie niet gestart.	core.tls.309

12.	Met inachtneming van verantwoordelijkheid core.tls.309, accepteren *Backchannel Nodes* PKIoverheid certficaten van elkaar door:
	• alle root-certificaten te vertrouwen zoals gepubliceerd op https://cert.pkioverheid.nl/;
	  • waarvan de geldigheidsdatum niet is verlopen en die NIET zijn ingetrokken;
	  • met uitzondering van de onderstaande root certificaten (deze zijn NIET toegestaan):
	  • de zogenaamde 'TEST' certificaten
	  • Alle roots gemarkeerd met 'Persoon'
	• deelnemers moeten alle valide domein en TSP certificaten onder PKIo hiërarchie opnemen in de truststore; zie hiervoor https://cert.pkioverheid.nl/;
	  • met uitzondering van (deze roots moeten NIET opgenomen worden):
	  • Organisatie Persoon
	  • Burger
	  • Autonome apparaten
	  • Private Personen
	  • ook de zogenaamde intermediate-certificaten moeten worden opgenomen in de truststore.
		core.tls.311

12.	Met inachtneming van verantwoordelijkheid core.tls.309, accepteren *Backchannel Nodes* PKIoverheid certficaten van elkaar door het stamcertificaat van de hiërarchie 'Staat der Nederlanden Private Root CA - G1', zoals gepubliceerd op https://cert.pkioverheid.nl/, te vertrouwen, zolang de geldigheidsdatum niet is verlopen en het stamcertificaat NIET is ingetrokken; **Uitzondering** Tot 4 december 2022 moeten alle *Deelnemers* ook de certificaten uit de hiërarchie 'Staat der Nederlanden EV', zoals gepubliceerd op https://cert.pkioverheid.nl/, accepteren. Dit doen zij door ook van deze hiërarchie het stamcertificaat te vertrouwen. Na 4 december 2022 mag dit stamcertificaat niet meer vertrouwd worden.	core.tls.311

13.	Voor alle frontchannel (internet-facing) verkeer moeten deelnemers een PKIoverheid-certificaat van het type 'publiek' toepassen, uitgegeven door de volgende keten en/of opvolgende generaties:
	• Stamcertificaat
	  • Staat der Nederlanden EV Root CA
	• Intermediair Domein Server CA 2020
	  • QuoVadis PKIoverheid Server CA 2020
	  • Digidentity PKIoverheid Server CA 2020
	  • KPN PKIoverheid Server CA 2020
	
	Voor alle backchannel verkeer (machine2machine) moeten deelnemers een PKIoverheid-certificaat van het type 'privaat' toepassen, uitgegeven door de volgende keten en/of opvolgende generaties:
	• Private Root CA (per medio 2020 de standaard voor m2m)
	  • Stamcertificaat
	  • Staat der Nederlanden Private Root CA - G1
	  • Domein Private Services, maar alleen de volgende:
	  • 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
	
	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.
		core.tls.312

14.	PKIoverheid certificaten moeten (in ieder geval op productie en acceptatie omgevingen) als complete keten inclusief alle intermediate certificaten worden verstuurd en gecontroleerd. Een certificaat keten bestaat uit het certificaat zelf, aangevuld met alle intermediate certificaten die worden meegeleverd door de CSP, de uitgevende instantie van het betreffende certificaat. Het root certificaat moet niet meegeleverd worden (dit is al aanwezig in de truststore van de tegenpartij).	core.tls.313
14.	PKI- certificaten moeten (in ieder geval op productie en acceptatie omgevingen) als complete keten inclusief alle intermediate certificaten worden verstuurd en gecontroleerd. Een certificaat keten bestaat uit het certificaat zelf, aangevuld met alle intermediate certificaten die worden meegeleverd door de CSP, de uitgevende instantie van het betreffende certificaat. Het root certificaat moet niet meegeleverd worden (dit is al aanwezig in de truststore van de tegenpartij).	core.tls.313

4. Principe's

Principe		Principe	
1 Het MedMij-netwerk is zoveel mogelijk gegevensneutraal	☐	11 Stelselfuncties worden vanaf de start ingevuld	☐
2 Dienstverleners zijn transparant over de gegevensdiensten	☐	12 Het afsprakenstelsel is een groeimodel	☑
3 Dienstverleners concurreren op de functionaliteiten	☐	13 Ontwikkeling geschiedt in een half-open proces met verschillende stakeholders	☐
4 Dienstverleners zijn aanspreekbaar door de gebruiker	☐	14 Uitwisseling is een keuze	☐
5 De persoon wisselt gegevens uit met de zorgaanbieder	☐	15 Het MedMij-netwerk is gebruiksrechten-neutraal	☐
6 MedMij spreekt alleen af wat nodig is	☑	16 De burger regisseert zijn gezondheidsinformatie als uitgever	☐
7 De persoon en de zorgaanbieder kiezen hun eigen dienstverlener	☐	17 Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld	☑
9 De dienstverleners zijn deelnemers van het afsprakenstelsel	☐	18 Afspraken worden aantoonbaar nageleefd en gehandhaafd	☐
10 Alleen de dienstverleners oefenen macht uit over persoonsgegevens bij de uitwisseling	☐	19 Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat	☑
Toelichting			

5. Risico's

Omschrijf de (privacy)risico's die kunnen ontstaan als deze RFC wordt aangenomen. In het onwaarschijnlijke geval dat deze RFC's geen risico's introduceert, geef dat dan wel aan.

Dreiging	Kans	Impact	DreigingsID (intern)	Maatregelen
Nieuwe deelnemers nemen toch een publiek vertrouwd PKIoverheid certificaat af, waardoor ze binnen een jaar extra kosten maken om over te schakelen naar een andere aanbieder	Klein	Klein		Nieuwe deelnemers goed informeren in het voortraject.
Het moeten gaan toestaan van meerdere certificaat leveranciers binnen het stelsel met de controle via CAB browser forum. Risico op foutieve uitgifte serverceritifcaten	Klein	Midden		Deelnemers informeren en vergelijkbare eisen stellen aan TSP voor de betreffende certificaat leveranciers.

6. Bijlagen

File	Modified

No files shared here yet.

7. Goedkeuring

Beoordelaar	Datum	Toelichting	Beoordelaar	Datum	Toelichting
Productmanager Stichting MedMij			Productmanager Beheerorganisatie		
Leadarchitect Stichting MedMij			Leadarchitect Beheerorganisatie		

Ontwerpteam					
Deelnemersraad			Eigenaarsraad		