Coding standards

- Directory structure:
  /src/api/medmij/…
  /test/…
  /readme.md

- Coding standards – afhankelijk van de programmering taal. (Sonarqube check)

Technical Design: Aannamen

- De MedMij-beheerorganisatie wordt **Registration Authority (RA)** in PKIoverheid, jegens alle betrokken Certificate Authorities (CA's). PKIoverheid kent echter die mogelijkheid niet.
- De MedMij-beheerorganisatie geeft een **domeinverklaring** af, zodat deelnemers zelf een subdomein onder .medmij.nl kunnen aanvragen bij een CA. Daarmee heeft de beheerorganisatie wel invloed op de uitgifte van een certificaat, maar laten intrekken is niet mogelijk, tenzij er sprake is van misbruik. Er is immers geen juridische relatie tussen de eigenaar van het domein (de beheerorganisatie) en de CA.

1. *Configuratie:*
   Elke configuratie parameter zal apart gedefinieerd worden en duidelijk gedocumenteerd

2. *Installatie:*
   Elke bouwblock kan apart gecompileerd een installeert kunnen worden. Documentatie over de Installatie proces, configuratie en gebruikt is nodig.

3. *Test:*
   Elke bouwblock kan apart getest kunnen worden. Een unit test (specifiek per programmering taal) file dat sluit aan bij de functies van de library is nodig.

4. *XML/XSD Code generatie:*
   Er is nodig om voor de implementatie doelen een proces te bieden voor aanpassingen binnen XSD. Generatie van de code vanuit een XSD file zal helpen om in de toekomst elke XSD verandering te kunnen regenereren.

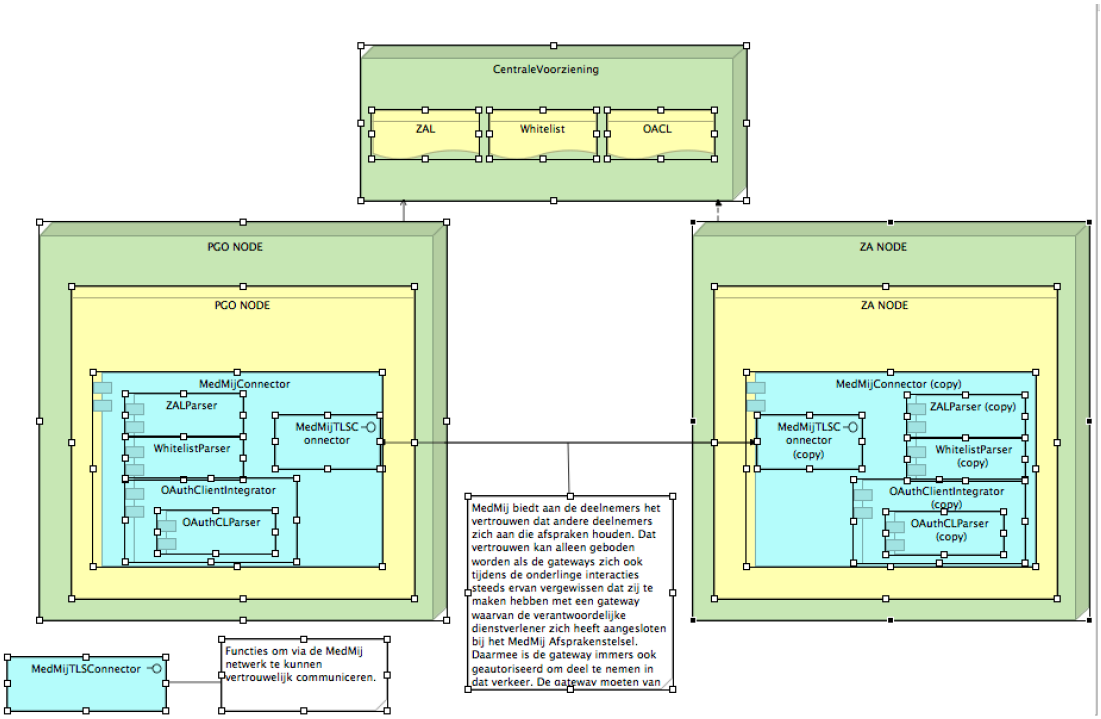
5. *Framewerk:*
   Een duidelijke afsplitsing per component is nodig om bouwblokken te kunnen integreren en expanderen met andere functies.
   1. Implementatie framewerk specifiek per programmering taal.
   2. Bijv: Het aansluiten van een communicatie component (SSL,..).

   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.: het design maken van en abstractie laag als een standard TLSComponent dat sluit aan direct op MedMij Netwerk. Deze component wordt gebruikt als een aparte ***Channel*** voor de aansluiting (niet in de huidige project implementatie scope)

6. *Taal- en technische keuzes*

- Voor de aanduiding van namespaces wordt gebruikgemaakt van een URL. Dit is de gemakkelijkste optie, omdat dit - anders dan bij een URN - geen namespaceregistratie bij IANA vereist.
- De namespace-URL kent de volgende opbouw: xmlns://afsprakenstelsel.medmij.nl/[naamLijst]/release[releasenummer].

- Een namespace-URL gebruikt xmlns:// als schema-aanduiding. Daarmee wordt duidelijk gemaakt dat het slechts een identificatie betreft, en dat de URL niet is bedoeld voor dereferencing (bijvoorbeeld om het XML-schema te downloaden).
- Het domein afsprakenstelsel.medmij.nl is een unieke hostname op het internet. Gebruik daarvan biedt zowel voldoende herkenbaarheid als uniciteit.
- De variabele naamLijst betreft één van de volgende waarden: Whitelist, OAuthclientlist of Zorgaanbiederslijst.
- De aanduiding release is toegevoegd voor de menselijke leesbaarheid en daarmee duidelijkheid.
- Waar het metamodel geen namen heeft gedefinieerd, kiezen we om redenen van consistentie en elegantie voor lowercase in de opbouw van de URL.
- Er wordt gebruikgemaakt van elementFormDefault = "qualified". Dit vergroot de leesbaarheid van de XSD's omdat er geen prefixes nodig zijn bij het definiëren van elementen, zonder aan enige functionaliteit af te doen.
- De prefixes voor de namespaces worden zo kort mogelijk gehouden en zijn geheel in lowercase, omwille van de leesbaarheid van de XSD's, en hebben de waarde wl, ocl of zal.
- De XML-schema's gaan uit van XML 1.0 en XML Schema 1.0. Deze versies bieden voldoende functionaliteit en kennen een zeer brede implementatie en ondersteuning.
- De XML-schema's zijn pretty-printed; door het gebruik van regeleinden en inspringing wordt de leesbaarheid vergroot.
- De bestandsnaam van een XML-schema kent de opbouw MedMij_[naamLijst].xsd. De variabele naamLijst betreft één van de volgende waarden: Whitelist, OAuthclientlist of Zorgaanbiederslijst.
- De XML-schema's bevatten de XML Declaration <?xml version="1.0" encoding="UTF-8"?>. De aanwezigheid van een declaratie wordt aanbevolen door de XML-specificaties. De encoding is optioneel bij het gebruik van UTF-8. De encoding is echter toch expliciet omdat dit mogelijke onzekerheid over de bedoeling of het correct volgen van de specificaties voorkomt. Er wordt geen gebruik gemaakt van het pseudo-attribuut "standalone", omdat er gebruikgemaakt wordt van XML Schema in plaats van DTD.
- Omwille van de leesbaarheid kent de XSD een standaardvolgorde in haar opbouw:
- Het root element, voorafgegaan door de commentaartekst <!--Root element-->.
- De simpleTypes, voorafgegaan door de commentaartekst <!--SimpleTypes-->.
- De complexTypes, voorafgegaan door de commentaartekst <!--ComplexTypes-->.
- De XSD's bevatten geen Byte Order Mark. Het gebruik van een Byte Order Mark is volgens de XML-specificaties optioneel bij UTF-8. Omdat ervaringen in andere sectoren leren dat de aanwezigheid van een BOM in sommige situaties problematisch kan zijn, gebruiken we het nooit.



Functies van de MedMijTLSConnector Component:

1. Versleuteling

Al het verkeer over het MedMij-netwerk is beveiligd met Transport Layer Security (TLS). In het bijzonder:
- worden SSL 1.0, 2.0 en 3.0 NIET gebruikt;
- maken back-channel-verbindingen (rechtstreeks tussen Gateways) gebruik van TLS-versies en -algoritmen die door NCSC zijn geclassificeerd als "goed";
maken front-channel-verbindingen (tussen Gateways enerzijds en User Agents anderzijds) gebruik van TLS-versies en -algoritmen die door NCSC zijn geclassificeerd als "goed" of "voldoende";
    - wordt voor encryptie altijd de sterkste vorm als eerste geprobeerd.
    -

Toelichting

Ten behoeve van vertrouwelijkheid en integriteit van alle uitgewisselde gegevens, wordt al het verkeer versleuteld. De eisen voor front-channel-verbindingen zijn minder streng om gebruikers met oudere hard- en software niet uit te sluiten. De vierde sub-eis zorgt ervoor dat de risico's beperkt worden.

2. Certificaten

Bij het afsluiten van de Deelnemersovereenkomst met Stichting MedMij schaft *Dienstverlener Persoon* of *Dienstverlener Zorgaanbieder* een PKIoverheid-certificaat aan, en wel een servercertificaat, van een PKIoverheid TSP, ten behoeve van elke de door laatstgenoemde gevoerde *PGO GW*, respectievelijk *ZA GW*. Ook MedMij Registratie beschikt over een PKIoverheid-certificaat. Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het PKIoverheid-stelsel.

Toelichting

De certificaten worden ook gebruikt voor authenticatie van gateways; dat is opgenomen op de applicatielaag. 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.

Autorisatie van gateways, dat wil zeggen, de vaststelling dat een gateway een MedMij-gateway is en uit dien hoofde geautoriseerd is deel te nemen in MedMij-verkeer, wordt niet gebaseerd op certificaten, maar op een door de MedMij-beheerorganisatie beheerde en ontsloten whitelist.

ZA GW Node, PGO GW Node en MedMij Stelselnode valideren steeds bij de TLS-handshake aan het begin van een TLS-sessie, bij de Certification Authority, op basis van OCSP, de geldigheid van het betreffende certificaat. In geval van een falende validatie of het uitblijven van een validatieresultaat, wordt het certificaten niet geaccepteerd en de TLS-sessie niet gestart. Dit is de UCI Authent. Gateway, die deel uitmaakt van alle use case-implementaties op de Applicatielaag.

Een organisatie mag meerdere certificaten hebben. Bijvoorbeeld omdat certificaten kunnen verlopen en op voorhand al een nieuwe klaar moet staan.

3. Whitelist

ZA GW Node, PGO GW Node en MedMij Stelselnode *valideren steeds bij de TLS-handshake aan het begin van een TLS-sessie, of de hostname van de server die verbinding met hen zoekt op de meest actuele* Whitelist *voorkomt. In geval dat niet het geval blijkt of niet vastgesteld kan worden, wordt het verkeer niet geaccepteerd en de TLS-sessie niet gestart. Dit is de* UCI Autor. Gateways*, die deel uitmaakt van alle use case-implementaties op de Applicatielaag.*