RFC’s M2M identificatie, authenticatie en autorisatie

Datum: 27 september 2024
Auteur: Architectenraad Edu-V

Via het Change- en releasemanagementproces van Edu-V zijn een aantal RFC’s ingediend aangaande de M2M identificatie, authenticatie en autorisatie. Het betreffen voornamelijk voorstellen ter verduidelijking van de toepassing van het NL GOV Assurance Profile voor OAuth2.0. De RFC’s zijn bijgevoegd als bijlage bij dit document.

Binnen de Architectenraad Edu-V zijn deze RFC’s besproken. In dit document is een korte toelichting beschreven voor zowel de indiener als voor de werkgroep Edukoppeling die namens het volledige onderwijs afspraken maakt over de M2M gegevensuitwisselingen en ook schakelt met het Kennisplatform ten aanzien van het NL GOV profiel. Voor de Werkgroep Edukoppeling zijn adviezen en verzoeken geformuleerd ten aanzien van de alignment tussen het NL GOV profiel, de Best Practice van Edukoppeling en de implementatiekeuzes in het Afsprakenstelsel van Edu-V.

RFC	Naam	Behandeling en reactie naar Indiener	Werkgroep Edukoppeling
RFC008	Client id	• Binnen het Afsprakenstelsel Edu-V staat reeds beschreven dat het clientId toebehoort aan een referentiecomponent en niet aan een organisatie. De voorstellen voor verduidelijking overnemen uitgezonderd de formulering omtrent het OIN. • Het Client Id SHOULD NOT het OIN van de organisatie zijn. Het gaat te ver om bijvoorbeeld een foutmelding te gaan geven als een organisatie besluit om Client Ids uit te geven waarbij wel het OIN wordt gehanteerd. Duidelijk moet zijn dat het een identifier van de Client is. En niet een identifier van de Organisatie.	Advies en verzoek om de Best Practice uit te breiden met de wijze waarop clientIds worden uitgegeven en hoe deze toegepast kunnen worden.

RFC009
RFC010
RFC011
	jwks_uri, private_key_jwt en PKIoverheid	• De RFC's vragen om een duidelijkere toelichting op de wijze waarop de private_key_jwt methodiek geïmplementeerd dient te worden.
		• Daarnaast worden argumenten gegeven waarom bepaalde implementatievarianten ongewenst zijn.
		• Dit heeft geleid tot een aanscherping van de documentatie op Confluence op twee pagina's:
		  ○ M2M gegevensuitwisselingen: hier is het proces van Registratie nader uitgewerkt.
		  ○ M2M identificatie, authenticatie en autorisatie is in meer detail uitgewerkt. Ook is een nieuwe interactie-analyse toegevoegd.
			Advies en verzoek om de Best Practice uit te breiden op basis van de gedetailleerde documentatie in het Edu-V afsprakenstelsel.
			
			Daarnaast verzoek aan de Werkgroep Edukoppeling om de invulling zoals binnen Edu-V gekozen te verifiëren bij NL GOV en na te gaan of deze consistent is.

RFC012	API design rules	• Deze RFC is afgewezen. • De API Design rules zijn een onderdeel van het NL GOV Assurance profiel. Om hiermee Consistent of Compliant te zijn is het van belang dat we deze hanteren. • Daarnaast is de koppelvlakspecificatie binnen Edu-V gebaseerd op REST/JSON. Daarmee zijn de API Design Rules wel degelijk relevant.	Geen verdere actie vereist.
RFC013	MUST NOT Discovery	• In de nieuwe uitwerking van de M2M identificatie, authenticatie en autorisatie is duidelijker weergegeven dat Discovery een COULD is.	Advies en verzoek aan Werkgroep Edukoppeling om de Best Practice op dit punt aan te passen. MUST NOT Discovery is niet de intentie geweest van Edu-V.

RFC014	MUST NOT mTLS	• Binnen Edu-V hanteren we TLS voor zowel de Autorisatieserver en Resourceserver. • Wat ons betreft is mTLS niet verboden en zou de keten ook moeten kunnen werken als partijen hier bilateraal en samen voor kiezen. • Met andere woorden een verbod op mTLS lijkt niet ons niet wenselijk. • In aanvulling hierop is mTLS een variant die ook onderdeel is van het NL GOV Assurance profiel. Door dit af te wijzen zijn we niet meer Consistent met dit profiel.	Geen verdere actie vereist.

RFC formulier – RFC008

Dit formulier kan worden gebruikt voor het indienen van een Request For Change. Het volledige RFC proces kan worden ingezien op Confluence.

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/203292674/Change-+en+releasemanagement+proces

indiener	Joost van Velzen
organisatie(s)	Iddink Digital / Magister
Datum	18-9-2024
Prioriteit	**Blocker** ~~/ Critical / Major / Minor / Trivial~~
Afspraak waar de RFC betrekking op heeft	Specificaties omtrent M2M authenticatie zijn onvoldoende duidelijk voor implementatie. Er bestaat onduidelijkheid over de bepaling van het client id.
Link naar Confluence pagina	https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie en daarvanuit link naar: Edustandaard OAuth best practices

Beschrijving van de concrete gewenste wijziging	Opgesteld zoals besproken op 16-9-2024 met: Koen Voermans, Erwin Reinhoud, Edwin Kense, Brian Dommisse, Esther Veldstra, Joost Molenaar, Jorn Nolles, Erick Bouwman, Dino Nijemcevic en Joost van Velzen.
	
	De huidige spec laat onduidelijkheid toe over het bepalen van client id's van referentiecomponenten. Daarnaast zijn er extra gegevens nodig voor het aanmaken van een client.
	
	Daarom is het goed om te stellen dat:
	• Een client id wordt bepaald en uitgegeven door leverancier van de Authorization Server
	• Bij het aanvragen/registreren van een client bij de leverancier van de Authorization Server moeten de volgende gegevens aangeleverd worden. Hierop zal de leverancier een uniek client id uitgeven aan de client die de verstrekte registratiegegevens weergeeft:
	  ○ Naam van het product/component
	  ○ Omschrijving van het product/component
	  ○ Hoge kwaliteit icon van het product/component (optioneel)
	  ○ Gewenste scopes
	  ○ Naam van de leverancier
	  ○ OIN (KvK nummer) (zie ook RFC "Verduidelijking toepassing PKIo met OIN")
	  ○ JWKS-waarde OF een JWKS_URI (zie ook RFC "Verduidelijking toepassing private_key_jwt authenticatie" en "Verplichten

	toepassing jwks_uri bij clients“) • 1 client id identificeert 1 softwarecomponent of product van 1 leverancier. Een leverancier kan 1 of meer componenten/producten aanbieden. • Het client id van een software component is **niet** gelijk aan het OIN • Het client id van een software component kan verschillen wanneer er wordt geauthenticeerd tegen verschillende Authorization Servers • Dit is geen afwijking van het NL GOV OAuth profiel, maar een verduidelijking.
Praktijkvoorbeeld	De organisatie “Iddink Digital BV” (met OIN 12345678) heeft twee sub-organisaties: “TIG“ en “Magister“. “TIG“ heeft een fictief product “MyDashboard“ welke toegang nodig heeft tot de “Students API“. “Magister“ heeft een fictief product “ELO“ welke toegang nodig heeft tot de “Progress API“. Binnen Edu-V zijn meer (potentiële) deelnemers die meer dan één product hebben. Bijvoorbeeld een roosterpakket en een formatiepakket. In de praktijk komt het dan zelfs voor dat scholen het roosterpakket afnemen, maar een formatiepakket van een andere aanbieder gebruiken. In deze gevallen acteren beide producten los van elkaar in de keten, hebben (compleet) verschillende sets aan scopes nodig, hebben een losse product life cycle, worden door andere medewerkers beheerd, identificeren van elkaar losstaande software componenten. Bovenstaande gaat uit van een organisatie met meerdere producten, maar een product kan ook verschillende additionele modules bevatten, waardoor deze modules los van elkaar geïdentificeerd zouden moeten worden in de keten.
Onderbouwing van nut en noodzaak/ rationale	Deze bevestigt en verduidelijkt wat ook in NL GOV OAuth en OAuth RFCs staat: • All clients MUST register with the authorization server. (NL GOV OAuth 2.2) • Client registration MAY be completed by either static configuration (out-of-band, through an administrator, etc…) or dynamically. (NL GOV OAuth 2.2) ○ Waarbij dynamically uitgesloten wordt, dus betreft het static (handmatige) configuration in geval van EDU-V • The authorization server issues the registered client a client identifier -- a unique string representing the registration information provided by the client. (RFC 6749: The OAuth 2.0 Authorization Framework) Daarnaast: • Clients wordt in geval van Magister weergegeven aan eindgebruikers (klanten) in de Privacy Manager (consent management module). Een klant geeft een client expliciet toegang tot de Magister-omgeving. • Client id’s kunnen gelogd gaan worden bij de verschillende

	ketenonderdelen, dit verbetert de traceerbaarheid • Het OIN moet vastgelegd gaan worden per client bij de AS, om PKIo met OIN validatie in het verdere proces uit te kunnen voeren • Door te stellen dat client id niet gelijk is aan het OIN wordt voorkomen dat er logica wordt gekoppeld aan het client id, wat interoperabiliteit in de weg staat
Gewenste moment van invoering	Zo snel mogelijk, maar in ieder geval voor de eerste release.

RFC formulier – RFC009

Dit formulier kan worden gebruikt voor het indienen van een Request For Change. Het volledige RFC proces kan worden ingezien op Confluence.

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/203292674/Change-+en+releasemanagement+proces

indiener	Joost van Velzen
organisatie(s)	Iddink Digital / Magister
Datum	19-9-2024
Prioriteit	~~Blocker /~~ **Critical** ~~/ Major / Minor / Trivial~~
Afspraak waar de RFC betrekking op heeft	Specificaties omtrent M2M authenticatie zijn onvoldoende strict voor toepassing in de keten. Het wordt aanbevolen een jwks_uri bij een client te registreren, maar dat zou verplicht moeten ten behoeve van betere beheersbaarheid.
Link naar Confluence pagina	https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie en daarvanuit link naar: Edustandaard OAuth best practices
Beschrijving van de concrete gewenste wijziging	Opgesteld zoals besproken op 16-9-2024 met: Koen Voermans, Erwin Reinhoud, Edwin Kense, Brian Dommisse, Esther Veldstra, Joost Molenaar, Jorn Nolles, Erick Bouwman, Dino Nijemcevic en Joost van Velzen. In de NL GOV OAuth specificatie wordt in hoofdstuk 2.3.4 (Client Keys) gesteld dat “It is **RECOMMENDED** that clients use a **jwks_uri if possible** as this allows for key rotation more easily. This applies to both dynamic and static (out-of-band) client registration.“ • **RECOMMENDED** zou moeten worden omgezet naar een **MUST**
Praktijkvoorbeeld	Verwacht wordt dat er tientallen tot misschien wel honderd (EDU-V) clients per Authorization Server gemanaged gaan worden. Wanneer partijen de client keys willen roteren, waarvan de reden bij veiligheid kan liggen of bij verlopen van PKIo certificaten, ontstaat een grote administratieve last bij het beheren van deze Authorization Server. Daarnaast is het verlopen van certificaten of out-of-sync zijn van public keys een grote bron van verstoringen.
Onderbouwi	Redenen om jwks_uri verplicht te stellen:

ng van nut en noodzaak/ rationale	• Betere beheerbaarheid • Betere robuustheid • Betere veiligheid Beheerbaarheid omdat er geen handmatige acties nodig zijn bij de AS om verlopen of ongeldige keys te rotaten Robuustheid omdat een client zelfstandig, op eigen gelegenheid, zijn keys kan rotaten Veiligheid omdat een rotated key per direct niet meer te gebruiken is, in tegenstelling tot vele handmatige acties welke anders nodig zijn om een key uit de keten te halen. Dit betekent dat er sneller ingegrepen kan worden als een partij slachtoffer van een hack is. Het volgen van een recommendation met betrekking tot veiligheid en robuustheid is eenvoudig uit te voeren wanneer partijen nog moeten beginnen met implementeren
Gewenste moment van invoering	Zo snel mogelijk, maar in ieder geval voor de eerste release.

RFC formulier – RFC010

Dit formulier kan worden gebruikt voor het indienen van een Request For Change. Het volledige RFC proces kan worden ingezien op Confluence.

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/203292674/Change-+en+releasemanagement+proces

indiener	Joost van Velzen
organisatie(s)	Iddink Digital / Magister
Datum	19-9-2024
Prioriteit	**Blocker** ~~/ Critical / Major / Minor / Trivial~~
Afspraak waar de RFC betrekking op heeft	Specificaties omtrent M2M authenticatie zijn onvoldoende duidelijk voor implementatie. Er bestaat onduidelijkheid over de bepaling van het client id.
Link naar Confluence pagina	https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie en daarvanuit link naar: Edustandaard OAuth best practices 3.1.5. MUST: Client Authenticatie conform OIDC private_key_jwt methode
Beschrijving van de concrete gewenste wijziging	Opgesteld zoals besproken op 16-9-2024 met: Koen Voermans, Erwin Reinhoud, Edwin Kense, Brian Dommisse, Esther Veldstra, Joost Molenaar, Jorn Nolles, Erick Bouwman, Dino Nijemcevic en Joost van Velzen. De huidige spec laat onduidelijkheid toe over de manier waarop de public key bij de AS geregistreerd wordt. In de NL GOV OAuth specificatie wordt in hoofdstuk 2.3.4 (Client Keys) gesteld dat “These clients MUST register their public keys in their client registration metadata by either sending the public key directly in the jwks field or by registering a jwks_uri that MUST be reachable by the authorization server.“. Hier kan gelezen worden dat bij het opvragen van het access token direct in dezelfde call ook de public key meegestuurd kan worden, dit is echter niet het geval. Dit vereist de volgende verduidelijking: • Bij registratie van een client bij de Authorization Server moet een public key als JWKS-waarde OF als JWKS_URI vooraf geregistreerd worden. • De tekst “sending the public key directly in the jwks field“ uit NL GOV OAuth 2.3.4 slaat op de “Dynamic Registration” functionaliteit welke in hoofdstuk “3.1.3 Dynamic Registration” verder wordt omschreven. Wanneer er geen gebruik wordt gemaakt van Dynamic Registration, zoals hier het geval is, dient de public key dus op een andere manier bij

	de AS geregistreerd te worden.
	
	• Zoals omschreven in NL GOV OAuth is het JWKS_URI RECOMMENDED:
	
	  ○ It is RECOMMENDED that clients use a jwks_uri if possible as this allows for key rotation more easily. This applies to both dynamic and static (out-of-band) client registration.
	
	  ○ Zie RFC “Verplichten jwks_uri bij clients“ welke hier op verder gaat.

Praktijkvoorbeeld	Nvt omdat dit standaard OAuth client_credentials private_key_jwt betreft.

Onderbouwing van nut en noodzaak/ rationale	• De Authorization Server heeft altijd een gegeven nodig om de client mee te authenticeren. In geval van private_key_jwt is dit een public key, welke vooraf geregisteerd wordt bij de Authorization Server.
	• Dit is conform NL GOV OAuth en ook conform RFC7523 “JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants“
	  ○ Zie 2.2 Using JWTs for Client Authentication RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
	  ○ https://www.rfc-editor.org/rfc/rfc7523.html#section-2.2

Gewenste moment van invoering	Zo snel mogelijk, maar in ieder geval voor de eerste release.

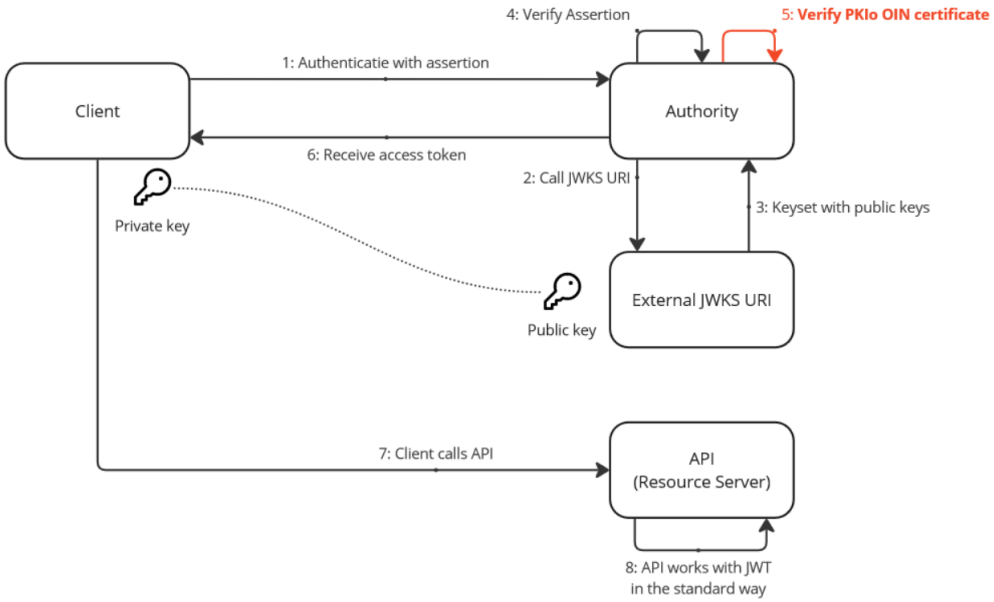
RFC formulier – RFC011

Dit formulier kan worden gebruikt voor het indienen van een Request For Change. Het volledige RFC proces kan worden ingezien op Confluence.

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/203292674/Change-+en+releasemanagement+proces

indiener	Joost van Velzen
organisatie(s)	Iddink Digital / Magister
Datum	19-9-2024
Prioriteit	~~Blocker /~~ **Critical** ~~/ Major / Minor / Trivial~~
Afspraak waar de RFC betrekking op heeft	Specificaties omtrent M2M authenticatie zijn onvoldoende duidelijk voor implementatie. Er bestaat onduidelijkheid over de precieze toepassing van PKIo met OIN bij het aanvragen van een token.
Link naar Confluence pagina	https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie en daarvanuit link naar: Edustandaard OAuth best practices 3.1.6. MUST: Client Key en toepassing van PKIo certificaat

Beschrijving van de concrete gewenste wijziging	Opgesteld zoals besproken op 16-9-2024 met: Koen Voermans, Erwin Reinhoud, Edwin Kense, Brian Dommisse, Esther Veldstra, Joost Molenaar, Jorn Nolles, Erick Bouwman, Dino Nijemcevic en Joost van Velzen.
	
	Er wordt gesteld dat een PKIo met OIN certificaat gebruikt moet worden, maar niet op welk punt en waarom dit gedaan moet worden. Ook NL GOV OAuth heeft hier geen uitgebreide omschrijving van.
	
	• Omschreven moet worden dat een PKIo met OIN certificaat bedoeld is om de organisatie (leverancier) van client te valideren, niet om een client zelf te authenticeren (dit wordt gedaan met het private_key_jwt mechanisme)
	• De PKIo validatie dient uitgevoerd te worden nadat de client gevalideerd is middels private_key_jwt, via een performant cryptografische controle van het signature van de Client JWT tegen de geregisteerde public key
	• De public key van de client is een PKIo met OIN certificaat
	• Om PKIo met OIN validatie uit te voeren is het nodig om het OIN bij de registratie van de client bij de AS bekend te maken (zie RFC “Verduidelijking gebruik client id“)
	• Bij de controle van het PKIo met OIN certificaat moeten in ieder geval de volgende attributen gecontroleerd worden:
	  ○ Geldigheid datum vanaf / tot
	  ○ Certificate chain / issuer
	  ○ OIN moet overeen komen met geregistreerde OIN van de client

	○ CRL • PKIo certificaten dienen alleen gebruikt te worden door clients, niet door de Resource Server of Authorization Server. RS en AS hebben een onderlinge trust door middel van inrichting van een authority uri.
Praktijkvoorbeeld	**Praktijk implementatie voorbeeld:** Onderstaande diagram geeft de plaats aan wanneer het PKIo met OIN certificaat gecontroleerd wordt (stap 5). Dit is een extra stap boven op het uitvoeren van de standaard OAuth private_key_jwt flow. 
Onderbouwing van nut en noodzaak/ rationale	Technische implementatiedetails missen in de specificaties, waardoor interoperabiliteit in gevaar komt. • De cryptografische 'assertion' van de 'client keys' is een snelle, betrouwbare, robuuste, eerste check welke altijd gedaan moet worden volgens OAuth, om een client te authenticeren • Het valideren of er gebruik gemaakt is van een PKIo met OIN certificaat is hier een laag bovenop, om te valideren of de client daadwerkelijk afkomstig is van de geregistreerde leverancier ○ Door de controle op PKIo met OIN wordt het autorisatiemechanisme restrictiever, waardoor de attack surface kleiner wordt
Gewenste moment van invoering	Zo snel mogelijk, maar in ieder geval voor de eerste release.

RFC formulier – RFC012

Dit formulier kan worden gebruikt voor het indienen van een Request For Change. Het volledige RFC proces kan worden ingezien op Confluence.

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/203292674/Change-+en+releasemanagement+proces

indiener	Joost van Velzen
organisatie(s)	Iddink Digital / Magister
Datum	19-9-2024
Prioriteit	~~Blocker / Critical / Major /~~ **Minor** ~~/ Trivial~~
Afspraak waar de RFC betrekking op heeft	Specificaties omtrent M2M authenticatie.
Link naar Confluence pagina	https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie Edukoppeling - M2M gegevensuitwisseling binnen het onderwijs - Edukoppeling OAuth Best Practices
Beschrijving van de concrete gewenste wijziging	Opgesteld zoals besproken op 16-9-2024 met: Koen Voermans, Erwin Reinhoud, Edwin Kense, Brian Dommisse, Esther Veldstra, Joost Molenaar, Jorn Nolles, Erick Bouwman, Dino Nijemcevic en Joost van Velzen. Het hoofdstuk “3.2.2. MUST: API design conform Kennisplatform API Design Rules” zou verwijderd moeten worden uit best practices.
Praktijkvoorbeeld	Niet van toepassing
Onderbouwing van nut en noodzaak/ rationale	• De standaarden volgen OAuth RFCs, er wordt geen REST API ontwikkeld • De aangehaalde ‘Design Rules’ zouden kunnen conflicteren met OAuth, dit zorgt voor onduidelijkheid
Gewenste moment van invoering	Zo snel mogelijk, maar in ieder geval voor de eerste release.

RFC formulier – RFC013

Dit formulier kan worden gebruikt voor het indienen van een Request For Change. Het volledige RFC proces kan worden ingezien op Confluence.

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/203292674/Change-+en+releasemanagement+proces

indiener	Joost van Velzen
organisatie(s)	Iddink Digital / Magister
Datum	19-9-2024
Prioriteit	~~Blocker / Critical / Major /~~ **Minor** ~~/ Trivial~~
Afspraak waar de RFC betrekking op heeft	Specificaties omtrent M2M authenticatie.
Link naar Confluence pagina	https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie Edukoppeling - M2M gegevensuitwisseling binnen het onderwijs - Edukoppeling OAuth Best Practices
Beschrijving van de concrete gewenste wijziging	Opgesteld zoals besproken op 16-9-2024 met: Koen Voermans, Erwin Reinhoud, Edwin Kense, Brian Dommisse, Esther Veldstra, Joost Molenaar, Jorn Nolles, Erick Bouwman, Dino Nijemcevic en Joost van Velzen. Het hoofdstuk “3.1.4. MUST NOT: Discovery” zou verwijderd moeten worden uit best practices. • Hoewel een well-known discovery endpoint niet noodzakelijk is voor het functioneren van OAuth, is het wel aanbevolen om dit toe te passen.
Praktijkvoorbeeld	Een Authorization Server geeft access tokens uit, dit zijn JWT's. Deze JWT's zijn bestemd voor Resource Servers, deze Resource Servers moeten vervolgens de JWT valideren. Om dit te doen zal een Resource Server een vertrouwde ‘Authority’ geconfigureerd hebben. Deze Authority is de url van de Authorization Server. Om de JWT te valideren heeft de Resource Server vervolgens het jwks endpoint nodig. In plaats van dit hard-coded in te stellen kan de Resource Server gebruik maken van het Discovery endpoint. Dit is altijd <authority url>/.well-known/openid-configuration Oftewel: een Authorization Server zal dit endpoint al hebben en het geeft de Autorization Server de vrijheid om URLs te wijzigen zonder impact
Onderbouwing van nut en noodzaak/	• Het heeft geen toegevoegde waarde om het Discovery endpoint uit te sluiten omdat dit onderdeel is van de OAuth spec, welke een Authorization Server sowieso al implementeert; • Het kan ook door clients gebruikt worden om het token endpoint op te

rationale	halen; • De software wordt robuuster en minder foutgevoelig doordat er minder hard-coded configuratie nodig is; • Door het hoofdstuk “3.1.4. MUST NOT: Discovery” te verwijderen uit de best practices volgt deze NL GOV OAuth.
Gewenste moment van invoering	Zo snel mogelijk, maar in ieder geval voor de eerste release.

RFC formulier – RFC014

Dit formulier kan worden gebruikt voor het indienen van een Request For Change. Het volledige RFC proces kan worden ingezien op Confluence.

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/203292674/Change-+en+releasemanagement+proces

indiener	Joost van Velzen
organisatie(s)	Iddink Digital / Magister
Datum	19-9-2024
Prioriteit	**Blocker** ~~/ Critical / Major / Minor / Trivial~~
Afspraak waar de RFC betrekking op heeft	Specificaties omtrent M2M authenticatie zijn onvoldoende duidelijk voor implementatie. Er bestaat onduidelijkheid of mTLS toegepast moet worden voor referentiecomponenten.
Link naar Confluence pagina	https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie
Beschrijving van de concrete gewenste wijziging	Opgesteld zoals besproken op 16-9-2024 met: Koen Voermans, Erwin Reinhoud, Edwin Kense, Brian Dommisse, Esther Veldstra, Joost Molenaar, Jorn Nolles, Erick Bouwman, Dino Nijemcevic en Joost van Velzen. De huidige spec laat onduidelijkheid toe over gebruik van mTLS. Toevoegen: • mTLS **MUST NOT** be used
Praktijkvoorbeeld	In het geval van Magister wordt de Authorization Server ook gebruikt voor H2M verkeer. mTLS is hierdoor niet mogelijk, PKIo-certificaten worden niet door browsers vertrouwd.
Onderbouwing van nut en noodzaak/ rationale	• mTLS is niet toe te passen voor componenten welke ook H2M-verkeer afhandelen • het gebruik van mTLS zorgt voor moeilijker inzetten van standaard Authenticatie oplossingen • mTLS heeft geen toegevoegde waarde boven het reeds toegepaste gebruik van OAuth • mTLS heeft geen toegevoegde waarde boven het reeds toepassen van HTTPS/TLS middels een vertrouwde CA • mTLS heeft geen toegevoegde waarde voor identifcatie van organisaties boven het reeds toepassen van PKIo met OIN certificaat binnen private_key_jwt • mTLS zorgt voor een hogere beheerlast

	• mTLS wordt niet verplicht vanuit het NL Gov OAuth profiel
Gewenste moment van invoering	Zo snel mogelijk, maar in ieder geval voor de eerste release.