Federatief SSOn Rijk

Beleid en kaders

Concept 0.10

Inhoudsopgave

Inhoudsopgave 1
1 Inleiding 2
2 Rijksbrede context 4
2.1 Gebruik 4
2.2 Beheer 4
2.3 Scope 4
2.4 Schematische voorstelling FSSOn Rijk 4
2.5 Definities 5
3 Aansluitvoorwaarden 7
3.1 Uitgangspunten en kaders 7
3.2 Kaders gebruik attributen 8
3.3 Kaders voor de Identity Provider rol 8
3.4 Kaders voor de Serviceprovider rol 9
3.5 Kaders beveiliging 10
4 Veranderingen in het proces ‘handmatigen’ 11
5 Aansluitvoorwaarden 12
5.1 Algemeen 12
5.2 Voorwaarden 12
6 Product- en dienstbeschrijving 13
6.1 Algemeen 13
6.2 Afnemers van FSSOn Rijk (rijksbrede dienst) 13
6.3 Functionele dienstverlening FSSOn Rijk 14
Bijlage 1: Ondersteunde protocollen en standaarden FSSOn Rijksoverheid 15
Bijlage 2: Attributen voor federatie in FSSOn Rijk 16

1 Inleiding

Sinds 2012 is Single Sign On Rijk (SSOn Rijk) de Rijksbrede ICT-voorziening waarmee Rijksmedewerkers eenvoudig en veilig worden geauthentiseerd en daarmee via een enkele aanmelding toegang krijgen tot toepassingen en voorzieningen[1]. De behoefte vanuit de Rijksdienst om Clouddiensten af te nemen c.q. aan te bieden en de behoefte vanuit rijksmedewerkers om via mobiele apparaten toegang te kunnen krijgen tot voorzieningen binnen het rijk resulteren in de vraag naar een toekomstvisie, doorontwikkelscenario's en roadmap voor SSOn Rijk. Gezamenlijk vraagt dit om een sterke, toekomstvaste positie van FSSOn Rijk, passend in de strategische I-agenda 2019-2021 van het Rijk en de kamerbrief 'Sturing IB en ICT Rijksdienst'. Het Gartner rapport Toekomstvisie SSOn Rijk biedt hierin onverkort de leidraad en kaders voor de inhoudelijke doorontwikkelstappen.

Dit document bevat een overzicht van aanvullend beleid en kaders voor de inrichting van de **vernieuwde Single- Sign-On** rijksbrede voorziening (SSOn Rijk). **SSOn Rijk is een bestaand werkende rijksbrede generieke voorziening** met een breed scala aan identificatie-, authenticatie- en aanpalende rijks-voorzieningen. Deze voorzieningen verzorgen op dit moment een pluriformiteit aan functies om gebruikers op een vriendelijke en veilige wijze gebruik te laten maken van rijksbrede applicaties of gedeelde applicaties.

Voortschrijdende ontwikkelingen in de informatietechnologie (IT), steeds meer applicaties worden gehost bij of door cloud-providers waarbij ook aanvullende functionaliteiten worden verlangd (bv Multi Factor Authenticatie). Daarnaast is een wildgroei ontstaan in aansluitvormen en in aangesloten organisaties. Dit vraagt om doorontwikkelingen van de bestaande voorziening. Dit op een zodanige wijze dat de goede werking, transparantie, veiligheid en toekomstvastheid gegarandeerd kunnen blijven.
In opdracht van CIO Rijk heeft Gartner vorig jaar een onderzoek uitgevoerd en is er, op basis van de uitkomsten een traject voor doorontwikkeling gestart, genaamd **Federatieve Single-Sign-On Rijk (FSSOn Rijk).**
Deze vernieuwing van de dienst heeft impact op de bestaande IT-voorzieningen van gebruikersorganisaties en rijksbrede en rijksgedeelde applicatie voorzieningen.

De vernieuwing naar FSSOn Rijk heeft consequenties voor de kaders en aansluitvoorwaarden van de huidige bestaande omgevingen. Aangepast beleid is daarom noodzakelijk en heeft vooral betrekking op de kaders welke nodig zijn bij de inrichting van de omgeving en de aansluitvoorwaarden.

Directie CIO Rijk, afdeling **ICT Voorzieningen en Infrastructuur Rijk** beschrijft dit beleid conform het rapport 'Toekomstvisie SSOn Rijk' (Gartner Consulting, 18 september 2019). De beschreven kaders zijn een uitwerking van dit rapport en een direct afgeleide van het bestaande 'Normenkader Rijksidentiteiten in relatie tot Rijksbrede voorzieningen' (goedgekeurd in ICBR 19 december 2017) en Normenkader Toegang (april 2016).
De informatie in dit document is zowel voor de betrokken Rijksorganisatie als voor de ICT-dienstverlener (op dit moment SSC-ICT) van belang. Er is alleen beleid opgenomen dat specifiek is voor de vernieuwing van FSSOn Rijk. Het beleid in dit document moet de aansluiting van de informatievoorziening bij de processen en organisatie waarborgen evenals de inpassing in de bestaande applicatieportfolio en ICT-infrastructuur.

De vernieuwing naar FSSOn zal voor de beheersbaarheid en noodzakelijkheid voor aanpassing in fases plaatsvinden. Voor een goede en veilige werking van het nieuwe FSSOn is er al een aantal voorbereidende

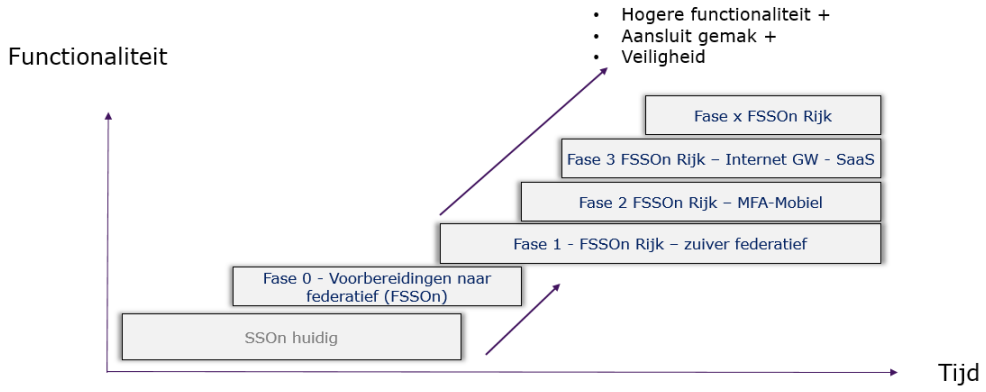
[1] ICCIO, 25 januari 2012

activiteiten uitgevoerd. Dit is **fase 0** genoemd en omvat een aantal maatregelen en inrichtingen bij de diverse organisaties om al tijdig te gaan werken en koppelen met een Identity Provider (IdP) en Service Provider (SP) aansluiting. Dit is in voorkomende gevallen en op projectbasis in de lijn van FSSOn reeds ingericht en uitgevoerd (anticiperende beweging richting federatief stelsel).

Fase 1 omvat het verder detailleren, voorbereiden en –**bindend**- inrichten van dit basisstelsel voor organisaties om aan te sluiten op de vernieuwde FSSOn Rijk. Dit is een noodzakelijk en fundamentele stap om de mogelijkheid te verkrijgen extra functionaliteiten, veiligheid en gebruiksgemak voor de toekomst te faciliteren. De toekomstvastheid en doorgroei, zoals beschreven in het Gartner rapport. **Fase 1** heeft vooral betrekking op verdere detaillering van de inrichting, stelsel, protocollen en koppelvlakken van de organisaties aan het FSSOn Rijk. *'Een set aan uniforme verkeersregels in het gehele rijks domein'*. De FSSOn fase 1 biedt een 'zuivere' federatieve koppeling tussen –alle- rijks gebruikers en applicaties.

In volgende fases zal de functionaliteit, conform de aanbevelingen in het Gartner rapport, worden uitgebreid. Hieronder valt onder andere ook extra de functionaliteiten zoals Multi-Factor-Authenticatie (**MFA**) voor mobiele gebruikers en het creëren van een zgn. **Cloud bridge** om cloud applicaties (SaaS) buiten het rijks domein te ontsluiten.

De MFA en Cloud bridge maken het mogelijk om op een veilige manier gebruik te maken van de identiteiten bij het inloggen op diensten die binnen of buiten de rijksdienst aangeboden worden. De Cloud bridge functioneert hierbij als een transparante IdP, die intern werkt als een veilige en gecontroleerde transparante koppeling. Het realiseren van de Cloud Bridge functionaliteit gaat daarbij noodzakelijkerwijs gepaard met de introductie van een hoger betrouwbaarheidsniveau voor de authenticatie van een identiteit. Er wordt daarvoor een tweede factor voor authenticatie geëist. De eisen, functionaliteiten en voorwaarden hiervoor worden op een later tijdstip met de departementen voor verdere detaillering afgestemd. In de daarop volgende fases kunnen technologische doorontwikkelingen plaatsvinden. Deze volgende fases en nieuwe functionaliteiten zijn op dit moment nog niet in detail gekaderd.



Figuur1: Schematisch overzicht van de fasering en functionaliteiten FSSOn Rijk

2 Rijksbrede context

2.1 Gebruik

Dit document is bedoeld voor zowel intern als extern gebruik. Het document biedt globaal inzicht in het vigerende beleid en de relevante omgeving. Bij intern gebruik heeft de inhoud een verplichtend karakter. Afwijking van het beleid of de kaders kan alleen na toestemming van de opdrachtgever Directie CIO Rijk, afdeling ICT Voorzieningen en Infrastructuur Rijk.
Bij extern gebruik, met name bij aanbestedingen, dient het document vooral om te kunnen beoordelen of systemen en applicaties geschikt zijn om te functioneren binnen de organisatie, het applicatieportfolio en de technische infrastructuur van met name SSC-ICT en in hoeverre zij passen bij de Rijksbrede ambities. Bij aanbestedingen zal door middel van selectiecriteria moeten worden beoordeeld in welke mate een aanbieding voldoet aan het Rijksbeleid en inpasbaar is in de huidige omgeving.

2.2 Beheer

Dit document wordt actueel gehouden door de Directie CIO Rijk, afdeling **ICT Voorzieningen en Infrastructuur Rijk**. Bij deze afdeling kan ook een actueel exemplaar van dit document worden aangevraagd. Bij intern gebruik kan nadere informatie over de inhoud worden verkregen bij de afdeling ICT Voorzieningen en Infrastructuur Rijk

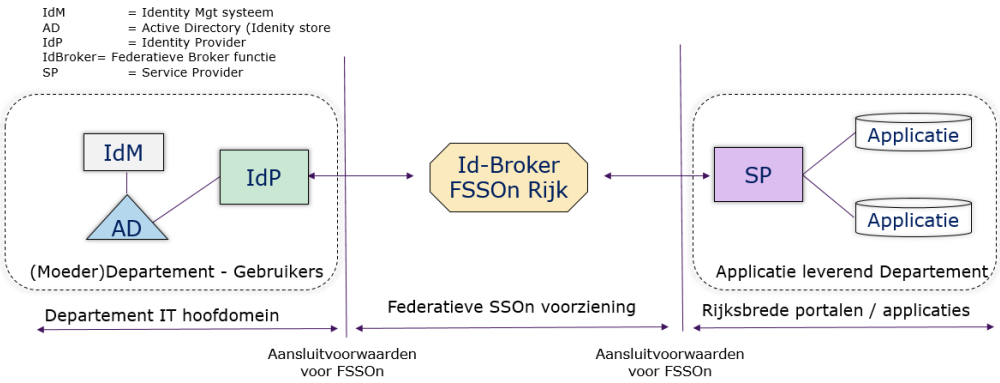
2.3 Scope

Single Sign On Rijk is een Rijksbrede voorziening voor departementen, Hoge Colleges van Staat en daaronder ressorterende overheidsorganisaties. De vernieuwing richt zich vooralsnog op de organisaties, binnen de huidige, bestaande reikwijdte van FSSOn Rijk.
Na de vernieuwing is de Single Sign On Rijk als koppelvlak ook voorbereid op toekomstige ontwikkelingen en is technisch gezien in staat om – indien dat door de eigenaar gewenst is – niet alleen Rijksbreed maar ook overheidsbreed organisaties en voorzieningen te bedienen.

Elk departement is zelf verantwoordelijk voor een FSSOn koppeling en de consolidatie van de benodigde FSSOn-informatie van hun eigen organisatie. Ook departementen die rijksgedeelde of rijksbrede-applicaties aanbieden zijn verantwoordelijk voor een FSSOn koppeling.
Uit inventarisatie blijkt dat een aantal organisaties binnen de huidige SSOn Rijk voorziening, gebruik maken van de optie om ***handmatig*** in te loggen. Deze voorzieningen zullen binnen FSSOn niet meer als onderdeel van de rijksbrede basisdienst ondersteund worden. Als er geen maatregelen worden getroffen vervalt het dienstenaanbod aan deze groep. Er zal door CIO Rijk in samenspraak met SSC-ICT alternatieve oplossingen, buiten FSSOn, overlegd worden.

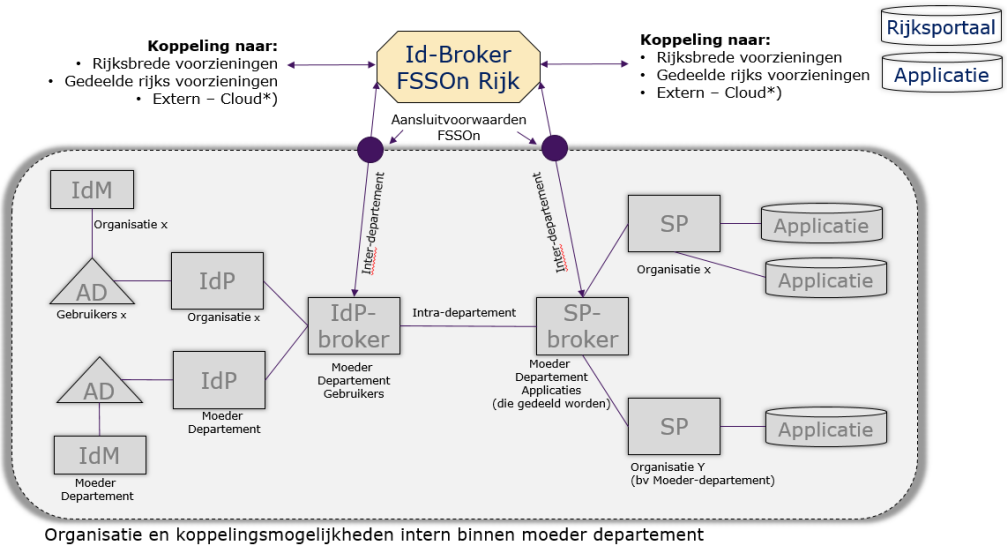
2.4 Schematische voorstelling FSSOn Rijk

De vernieuwing naar een volledig en veilig federatief stelsel voor identificatie, authenticatie en autorisatie vraagt om een goed afspraken stelsel en koppelvlakken. Uiteindelijk bepaalt elk departement en organisatie haar eigen IT- invulling en levert gebruikers identiteiten met een vastgesteld betrouwbaarheids niveau aan. Organisatie zijn hierin zelf verantwoordelijk voor het uitvoeren van authenticatieproces en bepalen zelf de middelen hiervoor. Organisaties die rijksbrede voorzieningen aanleveren of centrale Rijksvoorzieningen kunnen eenvoudiger en veiliger aansluiten op FSSOn Rijk op basis van de standaard koppelvlakken en protocollen.



Figuur2: Schematisch overzicht van aansluitvoorwaarden domein van FSSOn Rijk

FSSOn Rijk **fase 1** is de noodzakelijke basis van een nieuw federatieve stelsel. Organisaties en departementen hebben eigen mogelijkheden en IT-middelen voor intra koppelingen tussen gebruikers en applicaties. Voor het gebruik van voorzieningen **buiten** de eigen organisatie of departement faciliteert FSSOn Rijk. Koppelingen bijvoorbeeld naar het nieuwe Rijksportaal en andere centrale applicaties (inter koppelingen). Hieronder is als voorbeeld een diagram weergegeven van de rol en scope van FSSOn. De inrichting binnen de eigen organisatie dient ter illustratie van de principes.



Figuur3: Schematisch overzicht van het federatief stelsel en scope van FSSOn Rijk

2.5 Definities

- **Rijksidentiteit**
  Een minimale set van gegevens die een natuurlijke persoon representeren die een werkrelatie heeft met de Rijksoverheid.

- **Rijks Identificatie Nummer (RIN)**
  Elk persoon die voor het eerst een werkrelatie aangaat met organisatie binnen het Rijk krijgt een uniek nummer toegekend. Dit RIN fungeert als administratienummer en is onafhankelijk van een specifieke werkrelatie. Een persoon met meerdere werkrelaties heef één RIN.

- **IdM systeem departement**
  IdM systeem van een departement is een organisatorisch of locatie gebonden geheel van Identity Managementsystemen of andersoortige bronsystemen, processen en hulpmiddelen ten behoeve van het managen van de levenscyclus van een Rijksidentiteit. Een organisatie kan uit meerdere IdM domeinen bestaan, en meerdere organisaties kunnen samen gebruikmaken van één IdM domein.

- **IdM Domein**
  Een vertrouwd (eigen) IT-domein met eigen identiteiten (eigen 'trusted' Directory omgeving, AD. Dit kan een agentschap, uitvoeringsorganisatie binnen een moeder departement zijn).

- **Identity Provider (IdP)**
  Eenduidige rol voor het creëren en managen van identiteiten, inclusief authenticatie diensten binnen een federatieve omgeving (domein).
  Een IdP is de vertrouwde authenticatie provider en is verantwoordelijk voor Authenticatie assertions (echtheidsbewijzen), Attribute assertions (verstrek relevante extra informatie bij die identiteit) en Autorisatie assertions (verstrekt informatie over toegang, op basis van 'RBAC' en 'Policies'). Elk (moeder)departement verkrijgt toegang tot de federatieve omgeving door middel van de IdP rol en koppelvlak.

- **Federated identities management**
  Zorgt voor consistent en betrouwbare identiteiten tussen de domeinen. (In dit geval de volledige implementatie fase 1 FSSOn Rijk).

- **Identity Provider Broker (IdPB)**
  IdPB is een dienst die identiteit correlaties en data-aggregatie activiteiten uitvoert van de diverse IdP in een domein. IdPB is verantwoordelijk om vertrouwen (Trust) te creëren in relatie met de IdP en Service Provider (digital identities). Dit doormiddel van een Trust framework (certificaten). De IdPB aggregeert de IdP's van de organisaties binnen één moederdepartement en zorgt daardoor voor één oprit naar FSSOn Rijk.

- **Identity Assurance – vertrouwens niveau**
  Het niveau van vertrouwen (betrouwbaarheid dat de Identiteit. Dit kan meerdere niveaus hebben als gevolg van multi-factor authenticatie methodes (NIST 800-63 standaard)).

- **Service Provider (SP)**
  De SP is aangesloten op een IdP of IdB en bemiddelt voor authenticatie en autorisatie tussen een (web)applicatie en gebruiker. De (web)applicatie heeft een vertrouwensrelatie met de SP (en die SP opereert in een federatief identiteiten stelsel met IdP's en IdB's).

- **Service Provider Broker (SPB)**
  De SPB is aangesloten op een IdP, SP of IdB en bemiddelt voor authenticatie en autorisatie tussen een (web)applicatie en gebruiker. Een moederdepartement kan met een SPB de SP aggregeren en verzorgt dan 'één' oprit naar FSSOn Rijk. De (web)applicatie heeft een vertrouwensrelatie met de SP (en die SP opereert in een federatief identiteiten stelsel met IdP's en IdB's).

3 Aansluitvoorwaarden

FSSOn Rijk is een volledig federatief stelsel waarin (moeder)departementen nu als Identity Provider (IdP) optreden. Op het moment dat een departement de identiteit opvoert, kan deze identiteit gebruik maken van de benodigde diensten of applicaties die federatief zijn gekoppeld aan deze dienst. Indien een (uitvoerings) organisatie van een moederdepartement niet rechtstreeks (en dus niet via het moederdepartement) kan worden aangesloten, kan een technische oplossing worden gezocht binnen de daarvoor geldende kaders. Ook de applicaties en portalen die rijksbreed worden gebruikt binnen het federatieve stelsel worden gekoppeld via een Service Provider (SP) toegang. Per departement één SP koppelpunt.
De IdP en SP-functie worden door de departementen verzorgd. Desgewenst kan SSC-ICT hiervoor een aanvullende dienst aanbieden om deze functie te creëren.

3.1 Uitgangspunten en kaders

Het toekomstbeeld van FSSOn Rijk kent een aantal uitgangspunten en kaders op basis van de hiervoor beschreven uitgangspunten en zoals zijn vastgelegd in het Gartner rapport:

1. FSSOn als essentiële Rijks brede voorziening voor toegang tot centrale applicaties en portalen op basis van een veilige authenticatie;
2. De IdP en attributen volledig federatief en decentraal.

De uitgangspunten en vigerende kaders zien er als volgt uit:

Principe	Beschrijving en kader
Zo eenvoudig mogelijk	FSSOn Rijk wordt technisch gezien zo eenvoudig mogelijk uitgevoerd. Dit draagt bij aan de beheer(s)baarheid van de voorziening. Dit betekent dat technisch gezien, de FSSOn voorziening beperkt wordt tot twee bouwblokken (IdP Broker en in de toekomst de *Cloud Bridge*) op basis van standaard open authenticatie protocollen. FSSOn Rijk is technisch gezien in de nieuwe vorm onafhankelijk van alle andere diensten gerealiseerd – d.w.z. er is geen verwevenheid met DWR (werkplek) of andere diensten van SSC-ICT. Dit heeft als grote voordeel dat er eenvoudiger nieuwe organisaties (zoals ZBO's) aangesloten kunnen worden. Conform advies Gartner rapport en de architectuur principes voor Identity en Access management (IAM) van de Nederlandse Overheid Referentie Architectuur (NORA).
Hoog beschikbaar	FSSOn Rijk is technisch, zowel op applicatie als op de infrastructuurlaag, **hoog** beschikbaar en weerbaar uitgevoerd. Dit betekent dat de huidige centrale DWR-Active Directory services ook **niet** meer als back-up voorzieningen voor FSSOn Rijk worden ingezet.
Veiligheid	De FSSOn Rijk voorziening voldoet aan de kaders en veiligheidsrichtlijnen zoals vastgelegd in de BIO (BBN2 niveau). De toekomstige *Cloud bridge* biedt aanvullende bescherming voor kwetsbaarheden en cyberdreigingen. Minimaal een goede basisbescherming tegen Distributed-Denial-of-service (DDOS) aanvallen en actieve detectiemaatregelen (monitoring). Het zal op termijn mogelijk zijn om ook dashboards beschikbaar te stellen voor (departementale) SOC's. Toegang via de *Cloud bridge* is alleen mogelijk met verhoogde betrouwbaarheidsniveau 's voor identiteiten en authenticatie (en geaccrediteerde authenticatie-middelen), minimaal gebruik van een tweede authenticatie factor. Een Multi-Factor-Authenticatie mechanisme (MFA). Details over middelen , tweede-factor, eenmalige MFA of continue MFA worden in een volgende fase nader gedetailleerd uitgewerkt.
Gebruikers	Een Identity Provider (IdP) moet in staat zijn om 'real-time' nieuwe gebruikers te provisionen o.b.v. een geldige digitale identiteit. Conform de kaders zoals vastgelegd in Normenkader Rijksidentiteiten v1.1. Een IdP is verantwoordelijk voor de geldige identiteit en enkel factor goedgekeurde authenticatie. Een IdP **mag** een tweede factor authenticatie toevoegen om de betrouwbaarheid te vergroten. Voor de toekomstige Cloud bridge zullen gespecificeerde minimale eisen aan de beveiligingsniveaus en aansluitvoorwaarden voor MFA-gebruik van FSSOn Rijk worden vastgesteld.
Connectiviteit	Applicaties die buiten het eigen (trusted) domein van het rijk staan opgesteld (internetapplicaties) verkrijgen alléén connectiviteit met FSSOn Rijk door het gebruik van goedgekeurde certificaten. Deze applicaties ontvangen na aanvraag en goedkeuring een eigen uniek en veilig certificaat, waarmee de geldigheid door de IdP kan worden gecontroleerd. Hierbij wordt de open protocollen standaard gevolgd. Zie voor een overzicht van de ondersteunde protocollen en standaarden voor FSSOn Rijk in Bijlage 1.

Principe	Beschrijving en kader
Aansluiting	Een departement welke een applicatie rijksbreed beschikbaar stelt via de Service Provider (SP) mag eisen dat de betrouwbaarheid van de identiteit en authenticatie aan een minimaal acceptabel niveau voldoet. Deze eisen dienen in overleg tussen de IdP en de SP te worden vastgesteld. FSSOn Rijk biedt hiervoor een betrouwbare en veilige federatieve transportdienst. FSSOn Rijk zal de een set van minimale attributen voor identificatie, authenticatie garanderen. Afspraken met betrekking tot autorisatie (toegangsbeleid en condities/ 'authorisation policies' vinden altijd rechtstreeks plaats tussen IdP en SP. FSSOn Rijk faciliteert middels een veilig en betrouwbaar 'attributen' transport hierin.
Koppeling	Departementale applicaties die ontsloten worden naar andere Rijksonderdelen via FSSOn, maken altijd gebruik van een (enkele 'oprit') Service Provider (SP) van het departement. Bij afwijking hiervan zal eerst de impact hiervan bepaald worden door CIO Rijk. Indien nodig zal een opdracht richting SSC-ICT volgen om een speciale SP Proxyvoorziening hiervoor beschikbaar te maken.

3.2 Kaders gebruik attributen

In het kader van betrouwbaarheid, goede werking en uniforme aansluitvoorwaarden wordt er gebruik gemaakt van vaste formaten en een set aan attributen. Er kan door de IdP en SP gebruik gemaakt worden van de navolgende drie verschillende typen attributen.

Type	Beschrijving	Zichtbaarheid	Verantwoordelijkheid beheer
Verplichte set van minimale attributen (Vaststelling identiteit en rijksbrede identiteit kenmerken)	Deze beperkte set bevat generieke attributen, zoals e-mailadres, naam, achternaam en bijvoorbeeld het RIN-nummer. Deze attributen zijn voor alle applicaties zichtbaar.	Deze attributen worden altijd gedeeld bij elke aanvraag.	IdP - Identity Provider op basis van het IdM systeem en daarvoor geldende afspraken en kaders van het moeder departement (normenkader Rijksidentiteiten v.1.1)
Applicatie specifieke attributen	Deze set bevat applicatie specifieke attributen die gebruikt kunnen worden in autorisatieprofielen. Deze attributen kunnen door de SP aangevraagd worden om per identiteit rechten te verlenen. Deze attributen worden gebruikt indien per identiteit (gebruiker) extra informatie nodig is, zoals bijvoorbeeld het P-Direkt nummer.	Deze attributen worden alleen meegestuurd in het bericht van de applicatie waar ze voor bedoeld zijn.	SP - Service Provider (deze vraagt ze aan komt met IdP middels een afspraak/contract overéén)
Optionele en organisatie attributen	Bij applicaties waarbij toegangsverlening tot specifieke functionaliteit verder gaat dan de selectie op identiteit. (Applicaties specifieke detaillering van rollen en autorisaties) biedt FSSOn Rijk een attribuut met 'multi-value' veld, waarin de IdP en SP afspraken over de inhoud daarvan. Bijvoorbeeld voor autorisatieprofielen op afdelings- en rol niveau.	Deze attributen worden meegestuurd in het bericht van de applicatie waar ze voor bedoeld zijn.	Contract tussen IdP en SP. Zij spreken gezamenlijk de inhoud van het 'multi-value' veld af en bepalen betrouwbaarheid en granulariteit in de autorisatie policies.

In Bijlage 2 staan de verplichte en optionele attributen beschreven.

3.3 Kaders voor de Identity Provider rol

De federatieve opzet van FSSOn stelt de volgende eisen en kaders aan de rol van Identity Provider (IdP – departement). De volgende kaders zijn hierop van toepassing.

Kader	Inrichtingsgevolg en eisen voor IdP
Elk departement heeft de rol van Identity Provider (IdP) binnen FSSOn Rijk.	Naar FSSOn Rijk toe is het moederdepartement de Identity Provider (IdP), ongeacht of ook nog intern (d.w.z. met haar onderdelen en/of uitvoeringsorganisaties) identiteitsfederatie wordt gebruikt of niet. Het IdM

	systeem van het departement is leidend voor het opvoeren van identiteiten conform de normenkaders en heeft daarmee één unieke IdP 'oprit' tot FSSOn Rijk. Het moederdepartement kan daarvoor ook kiezen om een eigen departementale Identity Provider Broker in te zetten. IdPB
Een (uitvoerings)organisatie van een moederdepartement kan ook rechtstreeks (dus niet via het moederdepartement) worden aangesloten. Bij hoge uitzondering kan hiervoor worden gekozen. Alleen met een zwaarwegende reden (comply or explain).	Een departement kan intern namelijk ook met identiteitsfederatie werken (d.w.z. met haar onderdelen en/of uitvoeringsorganisaties). Er kan desgewenst ook een (interne) Identity Broker (IdPB) dienst van SSC-ICT afgenomen worden. Dus een valide technische noodzaak hiervoor geldt niet als zwaarwegende reden.
FSSOn Rijk verzorgt Identity Brokerage (IdB) rijksbreed voor de daarop aangesloten Identity Providers (IdP's).	In de eerste fase van FSSOn Rijk wordt ervan uit gegaan dat alle departementen binnen het Rijks domein de basis betrouwbaarheid voor identiteiten en authenticatie, conform BIO/BBN2 en normenkader Rijksidentiteiten v1.1. kan leveren. In de nabije toekomst (bij de introductie van Cloud bridge) zal een noodzakelijke tweede factor authenticatie door de IdP in staat moeten zijn om de identiteiten die zij beheert op verschillende betrouwbaarheidsniveaus (laag, midden en hoog) te kunnen verstrekken.
Elke aangesloten IdP moet de minimaal verplichte set van attributen implementeren (zie paragraaf 3.2).	De IdP is verantwoordelijk voor het beheren van de complete levenscyclus van de eigen identiteiten en de daarbij horende verplichte set attributen.
In samenspraak met de SP kunnen extra attributen gedefinieerd worden, zoals de naam van de afdeling, extra telefoonnummers, locatie/kamer. De IdP is hierbij verantwoordelijk voor de juistheid en draagt verantwoordelijkheid voor het beheer en betrouwbaarheidsniveau.	De IdP is verantwoordelijk voor het beheer en betrouwbaar aanleveren van extra attributen als dit voor een applicatie benodigd is (bijvoorbeeld, naam van de afdeling, locatie, rol). Dit is een afspraak direct tussen IdP en SP ('contract'). FSSOn Rijk faciliteert hiervoor alleen veilig en betrouwbaar transport.
Conform BIO/BBN2 niveau zijn er maatregelen genomen om de beschikbaarheid en vertrouwelijkheid te garanderen (conform SLA) en te bewaken.	De IdP heeft hiervoor de organisatie, processen en technologie ingericht.
IdP technologie en protocollen.	De aansluiting van IdP op FSSOn Rijk is technologie en leverancier onafhankelijk. Conform kaders van NORA, BIO/BBN2 en Gartner rapport worden open standaarden voor protocollen en identiteits-raamwerken toegepast. Zie voor de complete lijst Bijlage 1.

3.4 Kaders voor de Serviceprovider rol

Kader	Gevolgen voor SP rol
FSSOn Rijk wordt technisch gezien volledig federatief en volgens de beschreven principes uitgevoerd. Dit draagt bij aan de beheer(s)baarheid en de veiligheid van de FSSOn voorziening.	Een Service Provider die meerdere applicaties (diensten) aanbiedt, maakt gebruik van één enkele aansluiting (oprit) op FSSOn Rijk voor alle aangeboden applicaties. Dit draagt bij aan de beheer(s)baarheid van de voorziening. Desgewenst kan een departement daarvoor zelf een interne SP Broker inzetten. Deze dienst zou ook door SSC-ICT afgenomen kunnen worden.
FSSOn Rijk voorziet alleen in de authenticatie van de gebruiker. (De)Provisioning van de gebruikersidentiteit binnen de applicatie is verantwoordelijkheid van de applicatie eigenaar.	Dit is het beleid en dient als zodanig doorgevoerd te worden.
Elk departement die een of meerdere applicaties (diensten) aanbiedt via FSSOn Rijk heeft de rol van SP - Service Provider binnen FSSOn Rijk.	De SP is verantwoordelijk voor het bekend maken van extra (niet tot de minimum afgesproken set) behorende attributen die nodig zijn om van de dienst(en) gebruik te kunnen maken.
FSSOn Rijk verzorgt een éénduidige koppeling voor applicaties in het publieke internetdomein (SaaS / Cloud) via de Cloudbridge, zodat applicaties die niet gehost worden binnen een van de Rijks Datacenters toch gebruik kunnen maken van FSSOn. Deze functionaliteit voor in de volgende fase nader gedetailleerd.	De SP heeft de mogelijkheid om per applicatie de attributen vast te stellen binnen de daarvoor geldende kaders (zie bijlage 2 voor de vastgestelde attributen lijst) . De Cloudbridge is voorzien in de volgende fase en vereist een tweede factor authenticatie door de IdP. De Cloudbridge is dan ook minimaal voorzien van extra monitoring en protectie mechanisme voor de veiligheid.
De SP is leverancier-onafhankelijk opgezet en gebruikt standaard open protocollen.).	De SP is verantwoordelijk voor het eisen van het voor de dienst juiste niveau van identiteitsbeveiliging (laag/midden/hoog). De standaardprotocollen zijn: SAML2.0 (Security Assertions Markup Language, internationale standaard voor het uitwisselen van berichten met beveiligingsgegevens en informatie over eindgebruikers), OpenID Connect (authenticatiemechanisme om FSSOn op het internet mogelijk te maken) en OAuth2.0 (Open standaard voor autorisatie). Zie Bijlage 1 voor het overzicht van de ondersteunde protocollen.

3.5 Kaders beveiliging

Onderwerp	Beleid
Beveiligingsarchitectuur	De volgende uitgangspunten voor de beveiligingsarchitectuur zijn leidend: Gebruik van het IAA-principe (Identificatie, Authenticatie, Autorisatie) volgens NORA. Segmentering van interne netwerken en het gebruik van drie-lagenstructuur (DMZ) tussen interne en externe netwerk. En overkoepelend binnen de kaders van BIO/BBN2 niveau.
Beveiliging gegevens	Gegevens moeten beveiligd worden conform de wet BIO/BBN2, NORA IAA principes en de wet AVG (voor privacy).
	De betrouwbaarheid, integriteit en vertrouwelijkheid van informatie moet gewaarborgd zijn.
Escrow overeenkomst	Voor (een deel van de) aan te schaffen closed source software dient een escrow-overeenkomst aanwezig te zijn. De relevantie wordt bepaald middels de classificatie van de informatiesystemen.

4 Veranderingen in het proces ‘handmatigen’

Het project ‘Vernieuwing Rijksportaal’ (Rijksportaal 2.0) zal aan FSSOn Rijk gekoppeld worden. De ontsluiting vindt derhalve plaats via de vernieuwde FSSOn voorziening, waarbij er alleen toegang mogelijk zal zijn voor gebruikers van een IdP. Dit is voor een aantal organisatie een veranderingen ten opzichte van de huidige werkwijze en voorzieningen. De zogenaamde ‘handmatigen’.

Situatie	**Beleid**
Betrokken (uitvoerings) organisatie voldoet alsnog aan de genoemde uitgangspunten en aansluitvoorwaarden.	De (uitvoerings)organisatie wordt via het moederdepartement aangesloten.
Betrokken (uitvoerings) organisatie voldoet niet aan de genoemde uitgangspunten en kiest voor eigen ontwikkeling en beheer.	De (uitvoerings)organisatie ontwikkelt, beheert en onderhoudt een eigen IdP. Aansluiting mogelijk onder gestelde kaders en aansluitvoorwaarden.
Betrokken (uitvoerings) organisatie voldoet niet aan de genoemde uitgangspunten en kiest niet voor eigen ontwikkeling en beheer.	De (uitvoerings)organisatie maakt gebruik van een (nog te ontwikkelen) “IdP-als een Dienst” aangeboden vanuit SSC-ICT.
Betrokken (uitvoerings) organisatie voldoet niet aan de genoemde uitgangspunten en kiest voor een optie buiten de aangeboden Rijksbrede voorziening SSOn Rijk.	De (uitvoerings)organisatie wordt ontvlochten en zal géén toegang meer krijgen op de rijksbrede voorzieningen die op FSSOn zijn gekoppeld..

5 Aansluitvoorwaarden

5.1 Algemeen

Feitelijk ligt in de genoemde kaders eveneens de vernieuwde aansluitvoorwaarden besloten op beleidsniveau. De aansluitvoorwaarden bestaan uit een generiek deel met voorwaarden die op de gehele dienst van toepassing zijn en een dienst-specifiek deel. Ter verduidelijking een overzicht:

5.2 Voorwaarden

De volgende onderdelen worden voor FSSOn **toegevoegd aan de bestaande** aansluitvoorwaarden:

1. De toegestane en ondersteunde protocollen in FSSOn zijn: SAML2.0, OAuth2.0 en OpenID Connect. Zie *Bijlage 1: Ondersteunde protocollen en standaarden FSSOn Rijksoverheid* voor een volledig overzicht;
2. De mogelijkheid om gebruik te maken van de Cloud bridge en tweede factor authenticatie (in fase2 van FSSOn);
3. Attributen ondersteuning (SAML assertions Verplicht en Optioneel) volgens de tabel in *Bijlage 2 Attributen voor Federatie FSSOn Rijk*;
4. De beschikbaarheid en service window van de FSSOn Rijk wordt verhoogd naar 99,9% en een service window van 7*24;
5. Bij het doorvoeren van functionele wijzigingen dient de impact op verwerking van persoonsgegevens en informatiebeveiliging te worden bepaald. Indien gewenst kan CIO Rijk als voorwaarde stellen dat een pentest wordt uitgevoerd.

6 Product- en dienstbeschrijving

6.1 Algemeen

FSSOn Rijk valt onder de definitie van rijksbrede ICT-dienstverlening voor het Rijk. Dit is als het CIO-beraad besluit dat een ICT-dienst generiek is en als dusdanig rijksbreed wordt ingezet. De geraamde kosten van de rijksbrede ICT-diensten worden verdeeld over de rijksonderdelen. De verdeling van deze kosten wordt bepaald via de jaarlijkse “notitie kostenverdeling rijksbrede ICT”, aan de hand van een afgesproken verdeelsleutel (de individuele arbeidsrelatie (IAR)).

FSSOn Rijk valt binnen de **Producten- en Dienstencatalogus rijksbrede ICT-dienstverlening 2017** in de categorie A. Rijksbreed beschikbaar (Diensten waarvan door het CIO-beraad is besloten dat deze voor specifieke klantorganisaties (verzorgingsgebied) ter beschikking worden gesteld en gebruikt worden.
De rol van CIORIJK/IenI voor de categorie A-diensten is regievoerder voor de dienstverlening. IenI levert géén dienstverlening, maar is verantwoordelijk voor het maken van afspraken over de te leveren dienstverlening, het borgen van aan de dienstverlening gerelateerde processen (zoals incidentproces) en het bijsturen van de dienstverlening als deze niet volgens de afspraken verloopt.

6.2 Afnemers van FSSOn Rijk (rijksbrede dienst)

Organisatie	Sub-organisatie	Hoe gekoppeld
Ministerie van Algemene Zaken		Federatief (via IDP)
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	• **BZK** • **Logius**	**AD / kerberos**
Ministerie van Buitenlandse Zaken		Federatief (via IDP)
Ministerie van Defensie		Federatief (via IDP)
Ministerie van Economische Zaken en Klimaat		Federatief (via IDP)
Ministerie van Financiën		**AD / kerberos**
Ministerie van Infrastructuur en Waterstaat	• IenW • ILT • KNMI • PBL	Federatief (via IDP)
Ministerie van Justitie en Veiligheid	• Bestuursdepartement • CJIB • COA • IND • DJI • DT&V • Justid • NFI • Nationale Politie • OM • Reclassering NL • Raad voor de Kinderbescherming • Raad voor de Rechtspraak	Federatief (via IDP)
Ministerie van Landbouw, Natuur en Voedselkwaliteit		Federatief (via IDP)
Ministerie van Onderwijs, Cultuur en Wetenschap		Federatief (via IDP)
Ministerie van Sociale Zaken en Werkgelegenheid		Federatief (via IDP)
Ministerie van Volksgezondheid, Welzijn en Sport	• VWS • RIVM • SCP	Federatief (via IDP)
Belastingdienst		Federatief (via IDP)
Rijkswaterstaat		Federatief (via IDP)
ICTU		Federatief (via IDP)
Eerste Kamer		**Niet gekoppeld, handmatig inloggen**
Tweede Kamer		Federatief (via IDP)

Raad van State		Federatief (via IDP)
Algemene Rekenkamer		**Niet gekoppeld, handmatig inloggen**
Nationale Ombudsman		**Niet gekoppeld, handmatig inloggen**
Kanselarij der Nederlandse Orden		**AD / kerberos**
Het Kabinet van de Koning		**Niet gekoppeld, handmatig inloggen**

6.3 Functionele dienstverlening FSSOn Rijk

Functionele beschrijving	FSSOn zorgt voor een eenduidig, veilig en gedeelde transport voorziening van identiteit, authenticatie- en autorisatie-gegevens tussen gebruikers en applicaties binnen het rijks domein. Gebruikers binnen de departementen kunnen via FSSOn automatisch inloggen en hiermee ontsluiten van applicaties van rijksbrede en rijks-gedeelde portalen en applicaties. Dit op basis van de ingevoerde en geauthentiseerde aanmelding van deze gebruiker in een departement. (Eénmalig inloggen). FSSOn biedt de noodzakelijk basis voor doorontwikkeling naar meer functionaliteiten op basis van het federatief stelsel.	
Factsheet	Ja	
Portefeuillehouder	Directeur SSC-ICT	
Doelgroep	Rijksbrede ICT voorziening	
Aanbieder	• SSC-ICT voor de Technische voorziening • Applicaties / portalen aanbieders Rijksbreed	
Aansluiten		
Hoe aansluiten	Er zijn twee koppelvlakken • Gebruikers via IdP • Applicatieaanbieders via de SP. *Ad. Gebruikers:* Aangesloten (kern)departementen: AZ, BZ, BZK, DEF, EZ, FIN, IenM, JenV, OCW, SZW en VWS. Uitvoeringsorganisaties, agentschappen, achterliggende sectoren sluiten via het moederdepartement aan op FSSOn Rijk. De gebruikersfunctionaliteit van Federatief Single Sign On Rijk wordt vanuit CIO Rijk/ IenI gestuurd. *Ad. Applicatieaanbieders:* P-Direkt, SWF (intern en extern) en Rijksportaal zijn als rijksbrede applicaties ontsloten op FSSOn Rijk. Applicaties worden projectmatig ontsloten op basis een RFC Procedure met een intake- & offertetraject.	
Aansluitvoorwaarden van toepassing?	Ja: zie hoofdstuk 5. Aansluitvoorwaarden	
Aanvraagformulier	RFC procedure SSC-ICT	
Serviceniveaus		
Type	A	
Categorie dienst		
Standaardwijzigingen		
Aanvragen via	Helpdesk SSC-ICT	
Beschrijving wijziging	Beschrijving wijziging (functioneel)	Doorlooptijd (na indienen aanvraag tot aan levering)

Bijlage 1: Ondersteunde protocollen en standaarden FSSOn Rijksoverheid

Hieronder staan de ondersteunde protocollen en standaarden voor FSSOn vermeld:

Protocol / Standaard	Beschrijving	Toepassingsgebied FSSOn Rijk
SAML 2.0	Security Assertion Markup Language: Standaard Authenticatie raamwerk voor het uitwisselen van beveiligingsinformatie.	Single Sign On
PKIO	Public Key Infrastructure Nederlandse Overheid: Digitalel certificaten	Versleuteling van SAML gegevens en transport
TLS v1.2 en 1.3	Transport Layer Security: Encryptie transport protocollen voor veilige communicatie. Voor internetbeveiliging.	Beveiligd transport mechanisme
OIDC v1.0	OpenID Connect: authenticatie laag boven OAuth2.0.	Single Sign On Mobiel.
OAuth v2.0	Open Autentication standard: Is een open standard voor o.a. API autorisatie.	Autorisatie op content via API in samenwerking met Single Sign On
FIDO2	Fast Identity Online: Open industriestandaard (snelle) aanmeldmethode voor registratie en inloggen.	Aanvullende Multi Factor Authenticatie methode op Single Sign On.
SCIM	System for Cross-domain Identity Management: is een standaard voor geautomatiseerde uitwisseling van identiteitsinformatie tussen identiteits domeinen.	Datastructuur standaard voor uitwisseling van identiteits- en context gegevens tbv Single Sign On. *SCIM is meer een interne datastructuur standaard voor identiteits uitwisseling dan interface protocol voor FSSOn toegang.*

Meer details van de protocollen en standaarden zijn vastgelegd in : https://www.forumstandaardisatie.nl/open-standaarden.

Bijlage 2: Attributen voor federatie in FSSOn Rijk

In deze tabel zijn de attributen beschreven die worden ondersteund in het federatieve stelsel van FSSOn Rijk. Deze attributen zijn in lijn en grotendeels gebaseerd op internationale standaarden uit de academische wereld.

Attributen, formaat en gebruik volgens 'best practices' en standaarden zoals beschreven in:

- Organization for the Advancement of Structured Information Standards (OASIS) Authentication Concext fort he OASIS Security Asssertion Markup Language (SAML) V2.0 https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- Afsprakenstelsel Elektronische toegangsdiensten https://afsprakenstelsel.etoegang.nl/display/as/Attribuutcatalogus+natuurlijke+personen
- Attributen in SURFConext https://wiki.surfnet.nl/pages/viewpage.action?pageId=10125431,
- SCHema for ACademia (SCHAC) https://wiki.refeds.org/display/STAN/SCHAC
- Internet Enegineering Task Force (IETF) en OpenLDAP foundation: https://ietf.org/standards/rfcs/
- en https://www.openldap.org/

Gehanteerde uitgangspunten voor FSSOn (door ontwikkeling):

- Federatieve authenticatie op basis van SP initiatie met flows via front channel;
- Een aantal attributen worden mogelijk in de toekomst met o.a. OIDC via back channel gebruikt;
- Attributen vaststelling en aanpassing vindt minimaal één keer per jaar plaats.

Attributen ondersteuning Verplicht en Optioneel:

Omschrijving	Attribuut naam	Definitie	FSSOn Rijk Verplicht/Optioneel	Data type	Voorbeeld	Opmerking
Email address	urn:mace:dir:attribute-def:mail urn:oid:0.9.2342.19200300.100.1.3	RFC4524	Verplicht	RFC-5322 address (max 256 chars)	piet.jansen@minfin.nl	
Organization	urn:mace:terena.org:attribute-def:schacHomeOrganization urn:oid:1.3.6.1.4.1.25178.1.2.9	Schac	Verplicht	RFC-1035 domain string	minfin.nl (formele entry in RijksDNS)	
Organization Type	urn:mace:terena.org:attribute-def:schacHomeOrganizationType urn:oid:1.3.6.1.4.1.25178.1.2.10	Schac	Verplicht	RFC-2141 URN see Schac standard	Rijksoverheid	
Employee/student number	urn:schac:attribute-def:schacPersonalUniqueCode urn:oid:1.3.6.1.4.1.25178.1.2.14	Schac	Verplicht	RFC-2141 URN see BvR	RIN (Rijks identificerend nummer)	Relatie met «Identity Assurance Level » IAL niveau
PrincipalName	urn:mace:dir:attribute-def:govPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6	govPerson (1)	Verplicht	UTF8 String user@scope	piet.jansen@minfin.nl	
uid	urn:mace:dir:attribute-def:uid urn:oid:0.9.2342.19200300.100.1.1	RFC4519	Verplicht	UTF8 String (max 256 chars)	Lokaal DWR account	Relatie met lokale directory service omgeving
Surname	urn:mace:dir:attribute-def:sn urn:oid:2.5.4.4	X.520	Optioneel	UTF8 string (unbounded)	Jansen	
Given name or first name	urn:mace:dir:attribute-def:givenName urn:oid:2.5.4.42	X.520	Optioneel	UTF8 string (unbounded)	Piet	
FamilyNameInfix	urn:etoegang:1.9:attribute:FamilyNameInfix	X.520	Optioneel	UTF8 String (unbounded)	van (Piet – van- Alphen)	Typisch nederlandse tussenvoegsel in naam (van, de, der etc.)
Common name or Full Name	urn:mace:dir:attribute-def:cn urn:oid:2.5.4.3	X.520	Optioneel	UTF8 String (unbounded)	Piet Jansen	
Display name	urn:mace:dir:attribute-def:displayName urn:oid:2.16.840.1.113730.3.1.241	RFC2798	Optioneel	UTF8 String (unbounded)	Piet Jansen	
Affiliation	urn:mace:dir:attribute-def:govPersonAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.1	govPerson (1)	Optioneel	Enum type (UTF8 String)	Positie (intern / extern)	Relatie met IAL niveau
Scoped affiliation	urn:mace:dir:attribute-def:govPersonScopedAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9	govPerson (1)	Optioneel	UTF8 String user@domain	Rijksoverheid positie	
Entitlement	urn:mace:dir:attribute-def:govPersonEntitlement urn:oid:1.3.6.1.4.1.5923.1.1.1.7	govPerson (1)	Optioneel	RFC-2141 URN Multi-valued	(functie, taak) per service	Aansluitvoorwaarden Service Provider
isMemberOf	urn:mace:dir:attribute-def:isMemberOf urn:oid:1.3.6.1.4.1.5923.1.5.1.1	govMember	Optioneel	RFC-2141 URN Multi-valued	functierol via lidmaatschap	Relatie met OIDC / VOOT protocol

Nadere beschrijving van samengestelde namen (FamilyNameInfix) en namen met displaynaam /echtgenote kunnen als voorbeeld toegevoegd worden.