SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Federatieve authenticatie
Afstudeerscriptie

Vertrouwelijk

Bijlagen

Auteur:	Tim van Dijen - studentnummer 00008055
Opdrachtgever:	Dhr. R. P. van Kruistum
Bedrijfsmentor:	Dhr. M. R. Heeren
Begeleidend Examinator:	Dhr. J. P. M. de Vreught
Tweede Examinator:	Dhr. P. Burghouwt

Datum:	donderdag 7 januari 2016
Versie:	1.0
Status:	Definitief

Inhoudsopgave

Afstudeerplan

Informatie afstudeerder en gastbedrijf (*structuur niet wijzigen*)

Afstudeerblok: 2015-2.1 (start uiterlijk 31 augustus 2015)
Startdatum uitvoering afstudeeropdracht: z.s.m.
Inleverdatum afstudeerdossier volgens jaarrooster: 8 januari 2016

Studentnummer: 00008055
Achternaam: dhr. van Dijen
Voorletters: T.
Roepnaam: Tim
Adres: Charlotte de Bourbonstraat 69
Postcode: 2641 EX
Woonplaats: Pijnacker
Telefoonnummer: 015-2010651
Mobiel nummer: 06-26754450
Privé emailadres: tvdijen@gmail.com

Opleiding: Technische Informatica
Locatie: Delft
Variant: voltijd

Naam studieloopbaanbegeleider: dhr. A.G.P. Pronk
Naam begeleidend examinator: dhr. J.P.M. de Vreught
Naam tweede examinator: dhr. P. Burghouwt

Naam bedrijf: SSC-ICT Haaglanden
Afdeling bedrijf: Identity & Access Management
Bezoekadres bedrijf: Europaweg 81
Postcode bezoekadres: 2711 EP
Postbusnummer: 7385
Postcode postbusnummer: 2701 AJ
Plaats: Zoetermeer
Telefoon bedrijf: 079-3302300
Telefax bedrijf: 079-3302222
Internetsite bedrijf: http://www.sscicthaaglanden.nl

Achternaam opdrachtgever: dhr. Van Kruistum
Voorletters opdrachtgever: R.P.
Titulatuur opdrachtgever:
Functie opdrachtgever: Manager Identity & Access Management
Doorkiesnummer opdrachtgever: 079-3302387
Email opdrachtgever: r.p.kruistum@gdi.minvenj.nl

Achternaam bedrijfsmentor: dhr. Heeren
Voorletters bedrijfsmentor: M.R.
Titulatuur bedrijfsmentor:
Functie bedrijfsmentor: Coördinator Identity Management
Doorkiesnummer bedrijfsmentor: 079-8883411
Email bedrijfsmentor: m.r.heeren@gdi.minvenj.nl
NB: bedrijfsmentor mag dezelfde zijn als de opdrachtgever

Doorkiesnummer afstudeerder: 079-3302246
Functie afstudeerder (deeltijd/duaal):

Titel afstudeeropdracht:

Herontwerp van de Federatieve authenticatie (Single Sign-On) binnen het Ministerie van Veiligheid en Justitie.

Opdrachtomschrijving

1. Bedrijf

SSC-ICT Haaglanden is als onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties verantwoordelijk voor de levering van generieke, gemeenschappelijke en specifieke ICT-diensten. De afgelopen jaren heeft de organisatie zich ontwikkeld van werkplekleverancier tot een integrale serviceprovider voor ruim 30.000 werkplekken.

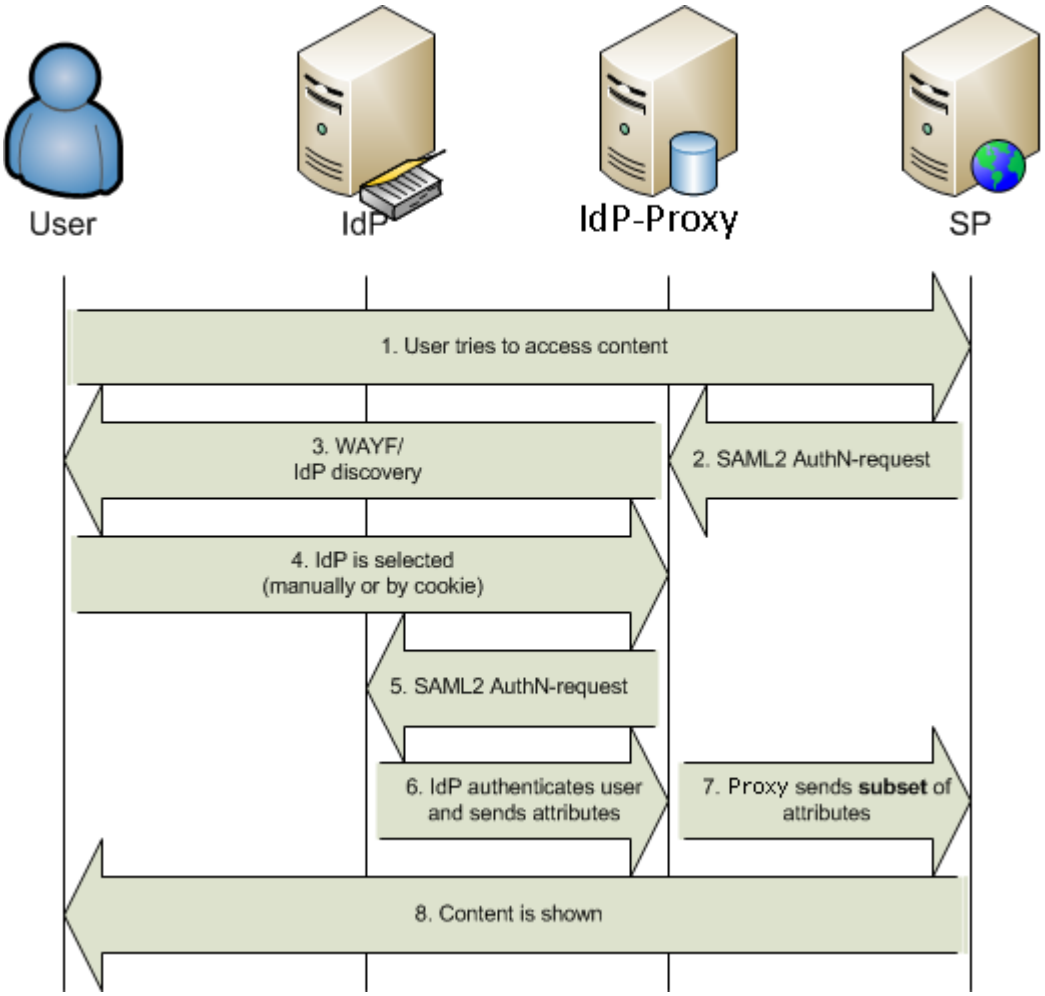
Het verzorgingsgebied is verspreid over bijna alle departementen binnen de Rijksoverheid. Naast reguliere beheertaken voor een 7x24-uurs dienstverlening is SSC-ICT Haaglanden verantwoordelijk voor projecten en programma's die een bijdrage leveren aan een compacte en duurzame overheid.

De afdeling Identity & Access Management (IAM) richt zich specifiek op het beheren van identiteiten en autorisaties. Als onderdeel hiervan wordt Single Sign-On als dienst aangeboden via de Federatieve Service.

2. Situatieschets

Enige jaren geleden is begonnen met de Federatieve Service voor het Ministerie van Veiligheid en Justitie en haar taakorganisaties. Federatieve Service maakt authenticatie mogelijk op basis van een onderlinge vertrouwensrelatie. Dit kan zowel tussen organisaties en gebruikers van deze dienst als tussen organisaties onderling plaatsvinden. Het doel van dit zogeheten Federatieve Identity Management is vrijwel altijd het vertrouwen en/of authentiseren van personen van buiten de eigen organisatie, middels publieke (niet vertrouwde) infrastructuur zoals het internet.

Een federatie in zijn meest simpele vorm bestaat uit een Identity Provider (IdP) en een Service Provider (SP). Door middel van een Identity Provider Proxy (IdP-Proxy) kunnen ook complexe federatieve ketens gemaakt worden. De SP is een webapplicatie, welke zelf geen eigen identity store heeft. Een gebruiker die naar de webapplicatie gaat, en nog geen geldige security token heeft, zal worden doorverwezen naar de IdP. Hier moet worden ingelogd, waarna de gebruiker met een security token weer wordt teruggestuurd naar de webapplicatie. Door de onderlinge vertrouwensrelatie tussen de SP en de IdP, zal de gebruiker worden toegelaten tot de applicatie. Deze vertrouwensrelatie is gebaseerd op PKI (Public Key Infrastructure). Het onderlinge berichtenverkeer verloopt middels het SAML protocol.



Een voorbeeld van een dergelijke omgeving binnen de publieke sector is DigID. Diverse overheidssites (SP's) vereisen dat een bezoeker zich authentiseert bij DigID (IdP). De SP's vertrouwen hierbij op de authenticatie van deze IdP. Op deze manier hoeft niet elke website een eigen identity store te hebben.

De Federatieve Service van het Ministerie van Veiligheid en Justitie bestaat uit vijf IDP's, drie SP's en twee IdP-Proxies, waarvan één IdP Proxy en drie IdP's in beheer zijn van SSC-ICT Haaglanden. Dit deel van de omgeving is in het verleden neergezet als Proof of Concept, waarbij niet of nauwelijks is gekeken naar zaken als beveiliging, schaalbaarheid, beschikbaarheid en beheerbaarheid. Onder druk van de opdrachtgever is deze omgeving vervolgens ingezet als productieomgeving, waarbij te weinig aandacht is geweest voor het beheer (omgevingen zijn niet homogeen, testomgeving is niet aanwezig), beveiliging en de documentatie van het geheel. Hierdoor is een directe behoefte ontstaan om een nieuw ontwerp te bedenken voor de federatie waarin wél rekening gehouden wordt met bovenstaande problemen.

3. Probleem

Als gevolg van gedane concessies op het gebied van beveiliging, schaalbaarheid, beschikbaarheid en beheerbaarheid verloopt het beheer van de omgevingen moeizaam, wat de uitbreiding van deze omgevingen in de weg staat.

4. Doelstelling

Het doel van de opdracht is om nog dit jaar nieuwe IdP's en SP's op een veilige manier aan te kunnen sluiten op de federatie, zonder dat dit de beheerlast onnodig vergroot.

5. Resultaat

Het resultaat van de opdracht is een nieuw ontwerp en een nieuw te realiseren testomgeving.

6. Uit te voeren werkzaamheden, inclusief een globale fasering, mijlpalen en bijbehorende activiteiten

Oriëntatiefase:

Doorlooptijd: 1 week
Mijlpaal: Plan van Aanpak
Activiteiten:

- Verhelderen van de opdracht
- Risico's analyseren
- Planning opstellen

Definitiefase:

Doorlooptijd: 5 weken
Mijlpaal: Definitiestudie
Activiteiten:

- Inlezen in de materie
- Analyseren van de huidige situatie
  - Analyseren beveiliging
  - Analyseren schaalbaarheid
  - Analyseren beschikbaarheid
  - Analyseren beheerbaarheid
- Achterhalen van de behoeften van de klant en die van de beheerders.
- Bepalen systeemeisen

Ontwerpfase:

Doorlooptijd: 5 weken
Mijlpaal: Ontwerprapport
Activiteiten:

- Ontwerp architectuur
- Uitwerken van één of meerdere alternatieven
- Laten bepalen van de oplossingsrichting door de opdrachtgever
- Ontwerpen van het nieuwe prototype

Realisatiefase:

Doorlooptijd: 6 weken
Mijlpaal: Testrapportage
Activiteiten:

- Aanvragen van servers, certificaten, infrastructuur
- Installatie en configuratie van verschillende componenten
- Testen
- Overdracht aan beheerorganisatie

Op te leveren (tussen)producten

- Plan van aanpak
- Definitiestudie
- Ontwerprapport
- Testrapportage

7. Te demonstreren competenties en wijze waarop

G1 (Praktische aspecten hanteren in (internationale) projecten)

Deze beroepstaak wordt aangetoond aan de hand van de risicoanalyse in het Plan van Aanpak.

A1 (Analyseren van het probleemdomein)

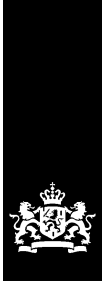
Deze beroepstaak wordt aangetoond aan de hand van de huidige situatie in de definitiestudie.

C9 (Ontwerpen van een infrastructuur)

Deze beroepstaak wordt aangetoond aan de hand van het ontwerp van de architectuur en alternatieven in het Ontwerprapport.

D18 (Testen van een infrastructuur)

De juiste werking van het prototype zal worden aangetoond aan de hand van de testrapportage.



SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Doorontwikkeling Federatieve Service

Plan van aanpak

Auteur: Tim van Dijen

Opdrachtgever: Dhr. R.P. van Kruistum

Datum: maandag 21 september 2015
Versie: 1.2
Status: Definitief

Documenthistorie

Versie	Status	Datum	Wijzigingen
0.1	Concept	07-09-2015	Eerste versie
0.2	Concept	09-09-2015	Verwerking commentaar M. Heeren
0.3	Concept	15-09-2015	Toevoeging contactgegevens, risicoanalyse en issuelogboek
1.0	Definitief	18-09-2015	Vastgesteld i.o.m. opdrachtgever
1.1	Definitief	18-09-2015	Spelling
1.2	Definitief	21-09-2015	Paragraaf Kwaliteit toegevoegd

Inhoudsopgave

1. Inleiding

Het doel van dit Plan van Aanpak is het beschrijven van de opdracht en de op te leveren producten.

Hoofdstuk 2 bevat een korte inleiding op de organisatie en op het concept van een federatieve dienst, als onderdeel van Identity- en Access Management. Tevens wordt er toegelicht wat een federatieve dienst precies is en hoe deze nu in gebruik is bij het Ministerie van Veiligheid en Justitie.

Hoofdstuk 3 bevat de opdrachtomschrijving, de probleem- en doelstelling en het op te leveren resultaat.

Hoofdstuk 4 bevat de mijlpalen en een planning van het project.

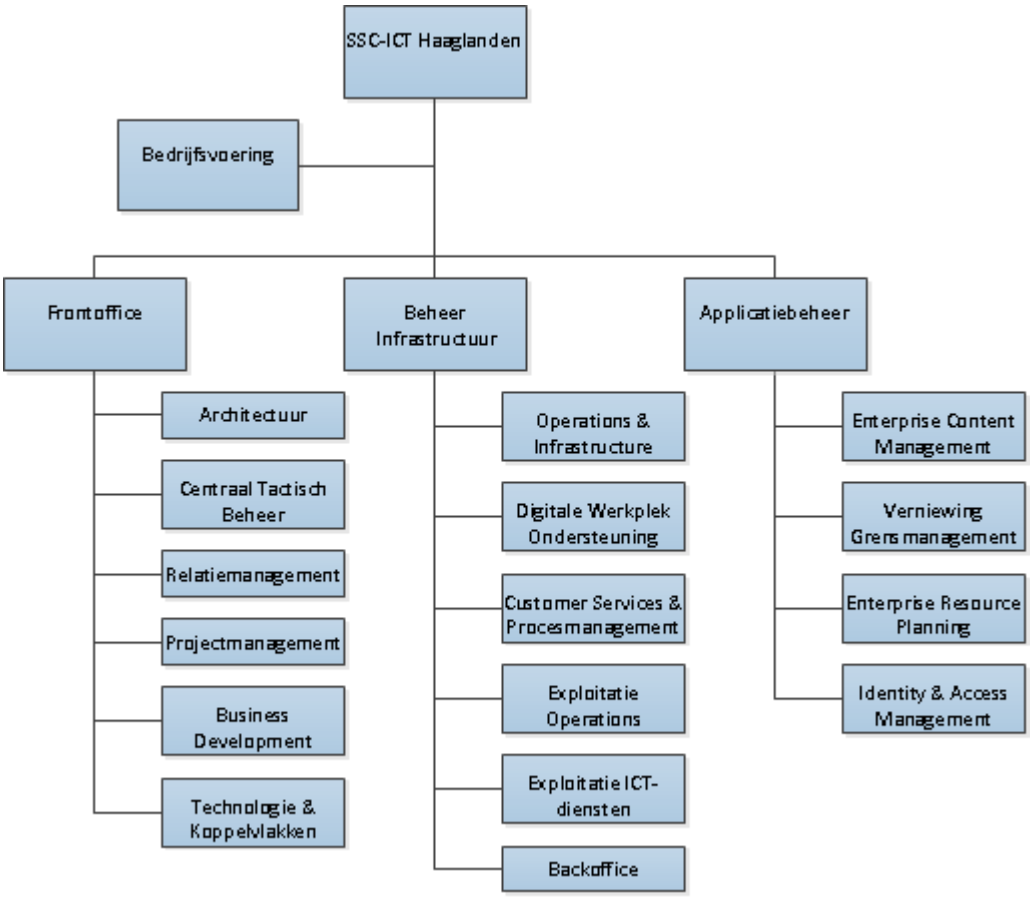
Tot slot in hoofdstuk 5 het issuelogboek, waarin de problemen die zich tijdens het afstudeerproject voordoen worden bijgehouden.

2. Achtergrond

2.1 SSC-ICT Haaglanden

SSC-ICT Haaglanden is als onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties verantwoordelijk voor de levering van generieke, gemeenschappelijke en specifieke ICT-diensten. De afgelopen jaren heeft de organisatie zich ontwikkeld van werkplekleverancier tot een integrale serviceprovider voor ruim 30.000 werkplekken.

Het verzorgingsgebied is verspreid over bijna alle departementen binnen de Rijksoverheid. Naast reguliere beheertaken voor een 7x24-uurs dienstverlening is SSC-ICT Haaglanden verantwoordelijk voor projecten en programma's die een bijdrage leveren aan een compacte en duurzame overheid.



Figuur 1:Organogram SSC-ICT Haaglanden

2.2 Identity & Access Management

De afdeling Identity & Access Management richt zich specifiek op het beheren van identiteiten en autorisaties. Door het op één plaats bijhouden en beheren van identiteiten, wordt het beheer vereenvoudigd en wordt de veiligheid gewaarborgd. Dit zorgt ervoor dat toegangsrechten worden verleend op grond van een interpretatie van het beleid en dat alle gebruikersidentiteiten en diensten goed zijn geverifieerd, geautoriseerd en gecontroleerd. Als onderdeel hiervan wordt Single Sign-On als dienst aangeboden via de dienst Federatieve Services.

2.3 Federatieve Services

Een federatieve service maakt authenticatie mogelijk op basis van een onderlinge vertrouwensrelatie. Dit kan zowel tussen organisaties en gebruikers van deze dienst als tussen organisaties onderling plaatsvinden. Het doel van dit zogenaamde Federatieve Identity Management is vrijwel altijd het vertrouwen en/of authentiseren van personen van buiten de eigen organisatie, middels publieke (niet vertrouwde) infrastructuur zoals het internet.

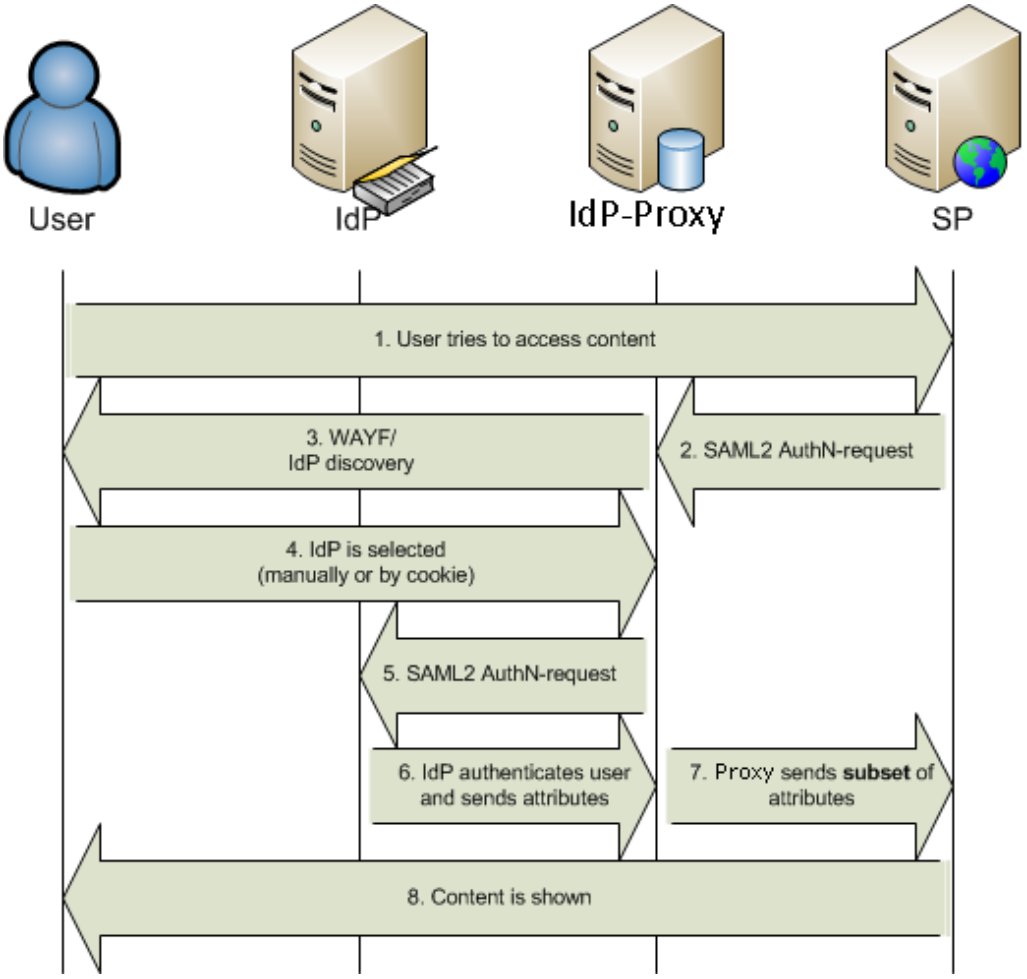
De afstudeeropdracht richt zich specifiek op de federatie van het Ministerie van Veiligheid en Justitie met al haar aanverwante taakorganisaties en de koppeling naar de rijksbrede federatie.

2.4 Situatieschets

Enige jaren geleden is begonnen met de Federatieve Service voor het Ministerie van Veiligheid en Justitie en haar taakorganisaties. Federatieve Service maakt authenticatie mogelijk op basis van een onderlinge vertrouwensrelatie. Dit kan zowel tussen organisaties en gebruikers van deze dienst als tussen organisaties onderling plaatsvinden. Het doel van dit zogeheten Federatieve Identity Management is vrijwel altijd het vertrouwen en/of authentiseren van personen van buiten de eigen organisatie, middels publieke (niet vertrouwde) infrastructuur zoals het internet.

Een federatie in zijn meest simpele vorm bestaat uit een Identity Provider (IdP) en een Service Provider (SP). Door middel van een Identity Provider Proxy (IdP-Proxy) kunnen ook complexe federatieve ketens gemaakt worden. De SP is een webapplicatie, welke zelf geen eigen identity store heeft. Een gebruiker die naar de webapplicatie gaat, en nog geen geldige security token heeft, zal worden doorverwezen naar de IdP. Hier moet worden ingelogd, waarna de gebruiker met een security token weer wordt teruggestuurd naar de webapplicatie. Door de onderlinge vertrouwensrelatie tussen de SP en de IdP, zal de gebruiker worden toegelaten tot de applicatie. Deze vertrouwensrelatie is gebaseerd op PKI (Public Key Infrastructure). Het onderlinge berichtenverkeer verloopt middels het SAML protocol. Zie Figuur 2 op de volgende pagina voor een voorbeeld van federatieve authenticatie.

Een voorbeeld van een dergelijke omgeving binnen de publieke sector is DigID. Diverse overheidssites (SP's) vereisen dat een bezoeker zich authentiseert bij DigID (IdP). De SP's vertrouwen hierbij op de authenticatie van deze IdP. Op deze manier hoeft niet elke website een eigen identity store te hebben.



Figuur 2: Voorbeeld federatieve authenticatie

De Federatieve Service van het Ministerie van Veiligheid en Justitie bestaat uit vijf IdP's, drie SP's en twee IdP-Proxy's, waarvan één IdP Proxy en drie IdP's in beheer zijn van SSC-ICT Haaglanden. Dit deel van de omgeving is in het verleden neergezet als Proof of Concept, waarbij niet of nauwelijks is gekeken naar zaken als beveiliging, schaalbaarheid, beschikbaarheid en beheerbaarheid. Onder druk van de opdrachtgever is deze omgeving vervolgens ingezet als productieomgeving, waarbij te weinig aandacht is geweest voor het beheer (omgevingen zijn niet homogeen, testomgeving is niet aanwezig), beveiliging en de documentatie van het geheel. Hierdoor is een directe behoefte ontstaan om een nieuw ontwerp te bedenken voor de federatie waarin wél rekening gehouden wordt met bovenstaande problemen.

3. Project

3.1 Opdrachtomschrijving

Als gevolg van bovenstaande verloopt het beheer van de omgevingen moeizaam, terwijl de druk vanuit de klant toeneemt om dit jaar nog meer SP's en IdP's op de federatie aan te sluiten. Hiernaast moeten een aantal applicaties op een veilige manier via de federatie naar het internet ontsloten worden. Hierdoor is een directe behoefte ontstaan om een nieuw ontwerp te bedenken voor de federatie waarin wél rekening gehouden wordt met bovenstaande problemen. Hierbij zal ook gekeken worden naar de huidige gebruikte software en eventuele alternatieven.

Gedurende het afstudeerproject zal aan de hand van de huidige eisen en wensen een nieuw ontwerp voor de VenJ Federatieve Service opgeleverd worden. Het ontwerp zal als onderdeel van de opdracht ook gerealiseerd worden in een nieuw in te richten testomgeving. Deze testomgeving zal als prototype gaan dienen voor de reeds bestaande acceptatie- en productieomgeving.

3.1.1 Probleemstelling

Als gevolg van gedane concessies op het gebied van beveiliging, schaalbaarheid, beschikbaarheid en beheerbaarheid verloopt het beheer van de omgevingen moeizaam, wat de uitbreiding van deze omgevingen in de weg staat.

3.1.2 Doelstelling

Het doel van de opdracht is om nog dit jaar nieuwe IdP's en SP's op een veilige manier aan te kunnen sluiten op de federatie, zonder dat dit de beheerlast onnodig vergroot.

3.1.3 Resultaat

Het resultaat van de opdracht is een nieuw ontwerp, wat rekening houdt met de eisen en wensen van de opdrachtgever en waarin verbeteringen zijn aangebracht op het gebied van beheerbaarheid, beveiliging en schaalbaarheid. Het ontwerp wordt gerealiseerd in een nieuw op te zetten testomgeving.

3.2 Scope

- Het ontwerp richt zich op de gehele VenJ federatie;
- De realisatie in de testomgeving beperkt zich tot het deel van de federatie wat bij SSC-ICT Haaglanden in beheer is

3.3 Randvoorwaarden

- De scope van de opdracht verandert niet drastisch;
- Het ontwerp gaat zoveel mogelijk uit van het hergebruik van bestaande componenten;
- Voortgangsgesprekken met de bedrijfsmentor en/of opdrachtgever vinden wekelijks plaats.

3.4 Projectorganisatie

Voor dit afstudeerproject zijn de volgende rollen gedefinieerd:

Opdrachtgever	
Naam	**Rol**
Dhr. R.P. van Kruistum	Opdrachtgever

Coördinatie	
Naam	**Rol**
Dhr. M.R. Heeren	Bedrijfsmentor
Dhr. J.P.M. de Vreught	1e examinator
Dhr. P. Burghouwt	2e examinator

Uitvoering	
Naam	**Rol**
Dhr. T. van Dijen	Aannemer, afstudeerder

Contactgegevens		
Naam	**Email**	**Telefoon**
Dhr. M.R. Heeren	m.r.heeren@gdi.minvenj.nl	079-8883411
Dhr. R.P. van Kruistum	r.p.kruistum@gdi.minvenj.nl	079-3302387
Dhr. T. van Dijen	t.van.dijen@gdi.minvenj.nl	079-3302246
Dhr. J.P.M. de Vreught	J.P.M.deVreught@hhs.nl	070-4458521
Dhr. P. Burghouwt	P.Burghouwt@hhs.nl	015-2606288

3.5 Risicoanalyse

Zoals elk project kent ook dit project een aantal risico's, welke geïnventariseerd zijn in onderstaande tabel. Voor de dreiging zijn drie niveaus gedefinieerd: Laag, Middel, Hoog. Dezelfde niveaus zijn ook voor Impact gedefinieerd.

#	Risico	Dreiging	Impact	Preventie	Uitwijk
1	De klant ziet af van de doorontwikkeling van de dienst uit bijv. politieke of kostenoverwegingen	Middel	Laag	Preventie niet mogelijk	Ja, SSC-ICT kan zelf besluiten de dienst door te ontwikkelen
2	Crisissituatie	Laag	Hoog	Preventie niet mogelijk	Nee, tijdens crisissituaties gelden er andere prioriteiten en mogen er geen wijzigingen worden uitgevoerd. Het project loopt uit.
3	De infrastructurele voorzieningen kunnen niet op tijd geleverd worden voor de realisatie	Middel	Hoog	Tijdig beginnen met aanvragen van de benodigde machines, changes, enz.	Ja deels; er kan lokaal met virtual machines gewerkt worden.
4	Er is onvoldoende medewerking vanuit de betrokken partijen om informatie te leveren	Middel	Middel	Tijdig beginnen met vragen stellen, rappelleren en desnoods escaleren	Nee, er kan geen gedegen definitiestudie gedaan worden. Dit heeft impact op het ontwerp en het eindresultaat.

3.6 Kwaliteit

Om de kwaliteit van de op te leveren producten te waarborgen zal elk product door de bedrijfsmentor worden nagekeken op volledigheid en taal. Waar relevant zal ook een peer-review gedaan worden door iemand met inhoudelijke kennis.

4. Mijlpalen en planning

Oriëntatiefase:
Doorlooptijd: 1 week
Oplevering: Week 35
Mijlpaal: Plan van Aanpak
Activiteiten:
- Verhelderen van de opdracht
- Risico's analyseren
- Planning opstellen

Definitiefase:
Doorlooptijd: 5 weken
Oplevering: Week 40
Mijlpaal: Definitiestudie
Activiteiten:
- Inlezen in de materie
- Analyseren van de huidige situatie
- Analyseren beveiliging
- Analyseren schaalbaarheid
- Analyseren beschikbaarheid
- Analyseren beheerbaarheid
- Achterhalen van de behoeften van de klant en die van de beheerders.
- Bepalen systeemeisen

Ontwerpfase:
Doorlooptijd: 5 weken
Oplevering: Week 45
Mijlpaal: Ontwerprapport
Activiteiten:
- Ontwerp architectuur
- Uitwerken van één of meerdere alternatieven
- Laten bepalen van de oplossingsrichting door de opdrachtgever
- Ontwerpen van het nieuwe prototype

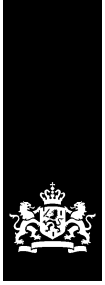
Realisatiefase:
Doorlooptijd: 6 weken
Oplevering: Week 51
Mijlpaal: Testrapportage
Activiteiten:
- Aanvragen van servers, certificaten, infrastructuur
- Installatie en configuratie van verschillende componenten
- Testen
- Overdracht aan beheerorganisatie

Tijdens het tweewekelijks overleg met de opdrachtgever zal de voortgang worden bewaakt. Er wordt gewerkt op basis van een 36-urige werkweek, van maandag t/m donderdag.

5. *Issuelogboek*

Eventuele issues die gedurende het project voorkomen worden weergegeven in onderstaand logboek en worden tijdens de wekelijkse voortgangsgesprekken.
Zo houdt iedereen een goed beeld van de issues en de ondernomen acties. Hiermee wordt ook de communicatie tussen de opdrachtgever en de uitvoerder versterkt.

#	Datum	Issue	Actie
1			
2			
3			
4			
5			



Ministerie van Veiligheid en Justitie

Aan: SSC-ICT

Directie Informatisering en Inkoop

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Datum
6 augustus 2015

Projectnaam
Functionele Specificaties - Doorontwikkeling VenJ Federatieve Dienst

Ons kenmerk
VenJ / DI&I

memo

Functionele Specificaties - Doorontwikkeling VenJ Federatieve Dienst

Directie Informatisering en Inkoop

Datum
6 augustus 2015

Ons kenmerk
VenJ / DI&I

1 Inleiding

Deze notitie beschrijft de functionele specificaties voor de doorontwikkeling van de VenJ Federatieve Dienst. Er wordt ingegaan op de huidige situatie van de VenJ Federatieve Dienst, de probleemstelling, het pakket met functionele eisen, het eindbeeld van de doorontwikkeling en tot slot de opdrachtdefinitie van DI&I aan SSC-ICT voor uitvoeren van een impact analyse naar de organisatorische en technische consequenties van de doorontwikkeling.

2 Aanleiding en achtergrond

Binnen de rijksoverheid zijn diverse ontwikkelingen waarneembaar in het verbeteren van het digitale contact en de dienstverlening met het Rijk[1]; ICT-voorzieningen dienen toegankelijker te worden gemaakt voor partijen[2] die organisatie-overschrijdend samenwerken in verschillende netwerken en keteninformatisering; Rijksmedewerkers moeten (vanuit oogpunt Het Nieuwe Werken) kunnen bepalen waar, hoe en wanneer zij werken en gebruik kunnen maken van ICT-voorzieningen (in deze notitie aangeduid als applicaties).

Deze ontwikkelingen hebben in bepaalde gevallen een duidelijk raakvlak met de VenJ Federatieve Dienst en hebben concreet geleid tot behoeften van de verschillende VenJ-sectoren om de dienst hierop uit te willen breiden c.q. door te ontwikkelen. Zo heeft DJI de behoefte gesteld om ICT-voorzieningen via internet cloud-diensten aan te willen bieden, en wil CJIB diensten naar de burger toe kunnen bieden middels eHerkenning/DigID.

Er is een belangrijke beweging gaande in een bredere ontsluiting van ICT-voorzieningen, en dan niet alleen voor generieke voorzieningen maar ook voor voorzieningen binnen het primaire proces en informatieketen van het departement. Bovendien heeft deze behoefte betrekking op een toenemende ontwikkeling voor de externe samenwerking met ketenpartners.

3 Huidige situatie VenJ Federatieve Dienst

Single Sign On (SSOn) stelt eindgebruikers in staat om eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere ICT-voorzieningen. Wanneer de eindgebruiker is ingelogd op zijn werkplek, neemt de SSOn software het inlogproces voor andere ICT-voorzieningen en systemen over. De software zorgt na een controle op de authenticiteit voor een automatische login voor de ICT-voorziening waarvoor de eindgebruiker toegang heeft.
Een gebruiker kan op basis van zijn claim; identiteit, rol en eigenschappen/werkrelatie de juiste ingang/autorisatieniveau in de ICT-voorziening krijgen. De eindgebruiker hoeft dan niet telkens bij het opstarten van een applicatie opnieuw in te loggen. Bovendien als de gebruiker vervolgens uitlogt op één van deze applicaties of systemen, dan is zijn sessie bij zowel deze als bij de overige applicatie of systemen beëindigd (single sign-off).

Om SSOn als functionaliteit VenJ-breed te faciliteren is dit binnen DWR (Digitale Werkomgeving Rijk) als volgt opgezet:
1. Het realiseren van een VenJ-brede 'single sign-on' dienst, te weten de VenJ Federatieve Dienst
2. Gebruik van federatieve authenticatie als concept voor de SSOn functionaliteit
3. Applicatie-integratie met deze dienst; aansluiten van generieke ICT voorzieningen Rijksportaal, SWF en P-Direkt)

[1] Hervormingsagenda en Digitaal 2017

[2] Ketenpartners, onderzoeksinstituten, bondgenoten (EU, NAVO), sourcing-partners tot lagere overheden

4. Organisaties – de VenJ-sectoren en uitvoeringsorganisaties - die aansluiten op de VenJ Federatieve Dienst.
5. Een dienst die is ingericht conform de vigerende beleidskaders van DWR, BIR

Door het implementeren van de VenJ Federatieve Dienst wordt met name veel gewonnen op het gebied van gebruikersgemak en heeft de gebruiker met slechts één gebruikersnaam/wachtwoordcombinatie toegang tot meerdere informatiebronnen, worden servicedesks ontlast doordat zij minder vragen ontvangen of verzoeken voor password/account-resets, voldoet de dienst aan de BIR, en is de 'veilige' inzet van de dienst getoetst door de NBV (Nationaal Bureau Verbindingsbeveiliging).

De dienst wordt via 'federatieve authenticatie' gefaciliteerd, waarmee het mogelijk wordt om met processen, standaarden en technologie op een gecontroleerde manier digitale toegang te regelen.
Er is bij 'federatieve authenticatie' sprake van externalisering van authenticatie, wat wil zeggen dat het door een centrale voorziening wordt uitgevoerd in plaats van door elke ICT-voorziening afzonderlijk. De architectuur is volgens dit principe opgebouwd, bestaande uit de volgende services:

<u>Werkplek-services:</u>
De werkplek-services bestaan uit de volgende gebruikersgroepen:
- Rijksmedewerkers
- Externe gebruikers

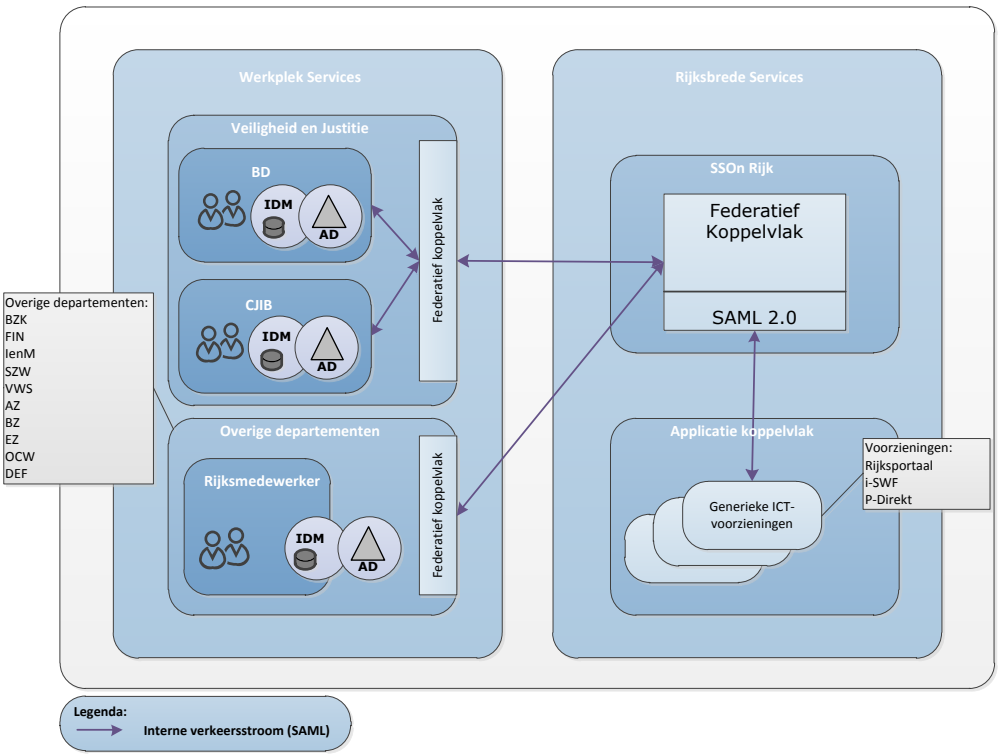
De afspraak is dat elk departement een eigen federatief koppelvlak heeft, waar ook de achterliggende sectoren en uitvoeringsorganisaties van dat departement op zijn aangesloten. Dit is mede gedaan uit beheermatigheid van het aantal verbindingen.

<u>VenJ Applicatie Services:</u>
De Access Gateway en IdP-Proxy vormen als ware het zenuwcentrum van de VenJ Federatieve Dienst. In de rol van respectievelijk centrale Identity Provider en centrale Service Provider wordt toegang verstrekt tot de aangesloten ICT voorzieningen en worden VenJ-identiteiten beschikbaar gesteld. Toegang tot een ICT-voorziening wordt ingesteld aan de hand van (claim-based) policies.

Functioneel betekent dit het volgende:
Een Rijksmedewerker 'claimt' zijn toegang tot een ICT voorziening, nadat hij is ingelogd op zijn digitale werkomgeving. Zijn inloggegevens worden dan door de Identity Provider gecontroleerd en bijgehouden. Van te voren is dan ook bepaald - via de WAYF-pagina - van welk VenJ-onderdeel de Rijksmedewerker afkomstig is. Op basis van de authenticatie (identiteit, wachtwoord en bijbehorende attributen) uit de sectorale Active Directory wordt door de IdP het zogenaamde toegangsbewijs voor de Rijksmedewerker gemaakt. De creatie van zo'n bewijs gebeurt via het standaard protocol SAML. Met behulp van dit toegangsbewijs verleent de Access Gateway de Rijksmedewerker zijn toegang tot de ICT voorziening.

Sectoren stellen de eigen identiteiten beschikbaar. De 'provisioning' (creatie, onderhoud en verwijderen) van een identiteit en de autorisatie binnen de ICT-voorziening maken geen onderdeel uit van de VenJ Federatieve Dienst en is een verantwoordelijkheid van respectievelijk het departement en de informatie-eigenaar.

<u>Rijksbrede Applicatie Services:</u>
De via de centrale rijksbrede Service Provider ontsloten generieke ICT voorzieningen; Rijksportaal, i-SWF en P-Direkt.



Figuur 1 Architectuur Huidige situatie VenJ Federatieve Dienst i.c.m. Rijksbrede koppelvlak

4 Probleemstelling

Zoals in de aanleiding staat beschreven, ziet VenJ diverse rijksbrede ontwikkelingen in relatie tot het verbeteren van het digitale contact, de dienstverlening en (externe) samenwerking. Sectoren zien graag (en het liefst zo snel mogelijk) dat ter ondersteuning van deze ontwikkelingen dit via de VenJ Federatieve Dienst wordt ingevuld.
De VenJ Federatieve Dienst in de huidige situatie is echter ontwikkeld volgens een gesloten organisatiemodel en gesloten netwerkinfrastructuur (Rijksweb-VPN). Dit houdt in dat alleen de departementen als een ' federatie' digitaal samen kunnen werken in het gebruik van de aangesloten ICT voorzieningen, en biedt dit "gesloten karakter" onvoldoende mogelijkheden tot de digitale samenwerking met andere externe partijen over de organisatiegrenzen heen.
Het belemmert daardoor niet alleen de toegang tot overheidsinformatie en ICT-voorzieningen, bedoeld voor de externe samenwerking, maar heeft ook de nodige beperkingen voor de Rijksmedewerker om via het internet toegang te kunnen krijgen tot ICT-voorzieningen.

De VenJ Federatieve Dienst dient daarom op basis van gestelde behoeftes, maar ook vanwege de huidige situatie en de beperkingen die dat met zich meebrengt, doorontwikkeld te worden. De vraag voor de doorontwikkeling is het leveren van een bijdrage aan het verbeteren van het digitale contact en de digitale dienstverlening, waarbij afgestapt zal worden van het zogenaamde "gesloten karakter" zonder dat dit een groot afbreukrisico vormt op het gebruiksgemak, de dienstverlening en (vertrouwelijke) informatie.
Met name op het gebied van het betrouwbaarheidsniveau dienen de nodige veiligheidsmaatregelen getroffen te worden om voldoende bescherming te kunnen

bieden en te voorkomen dat anderen van buiten, anders dan vooraf toegestane gebruikers, toegang verkrijgen of dat er ongeautoriseerde wijzigingen aan gegevens plaatsvinden, of erger, moedwillig gegevens worden ontvreemd en/of gemanipuleerd.
Indien de VenJ Federatieve Dienst echter niet wordt doorontwikkeld vergroot dit de kans op een verdere groei aan suboptimale oplossingen van departementen, hogere kosten, onbeheersbare situaties met een verminderde controle op rechtmatige en veilige toegang tot vertrouwelijke informatie.

5 Functionele specificaties doorontwikkeling VenJ Federatieve Dienst

Om invulling te geven aan het verandertraject naar de gewenste situatie van de VenJ Federatieve Dienst, zijn door DI&I diverse workshops met de sectoren en de technisch beheerder SSC-ICT georganiseerd. Doel van deze workshops was om aan de hand van de behoeftes te komen tot een reële en bruikbare set aan functionele eisen. Allereerst is in de workshops gestart om de use cases inzichtelijk te krijgen die een raakvlak hebben met de doorontwikkeling. Vervolgens zijn vanuit deze use cases de functionele eisen gedefinieerd die op hun beurt weer hebben geleid tot een eindbeeld van de VenJ Federatieve Dienst. In dit onderdeel wordt stil gestaan bij de uitwerking van deze workshops met respectievelijk de uitgangspunten van de doorontwikkeling, de use cases, de functionele eisen en het eindbeeld van de VenJ Federatieve Dienst.

<u>Ad. Uitgangspunten doorontwikkeling VenJ Federatieve Dienst</u>
Als vertrekpunt voor de functionele specificaties zijn de volgende uitgangspunten gedefinieerd voor de doorontwikkeling van de VenJ Federatieve Dienst, waarbij:

1. DI&I de systeemeigenaar, JustID de functioneel eigenaar en SSC-ICT de technisch beheerder is.
2. De VenJ Federatieve Dienst aansluit op, of rekening houdt met, de vigerende doelarchitecturen/beleidskaders van BIR, WBP, DWR, DA Toegang, I-Strategie en Hervormingsagenda/Digitaal 2017.
3. De VenJ Federatieve Dienst een afhankelijkheid heeft met de concrete resultaten/producten van het programma Toegang; Rijkspas (logische toegang), RidM, en RIN.
4. De VenJ Federatieve Dienst gebaseerd is op Open Standaarden; SAML (en Kerberos) en bij voorkeur gebruik maakt van Open Source-producten.
5. De huidige situatie is ingericht en wordt verricht conform de aansluitvoorwaarden van het rijksbrede koppelvlak (SSOn Rijk).
6. SSOn Rijk de centrale identity provider is voor alle rijksidentiteiten en centrale service provider voor de aangesloten generieke ICT voorzieningen Rijksportaal, SWF en P-Direkt.
7. De VenJ Federatieve Dienst zoveel mogelijk aan hergebruik doet van bestaande bouwstenen, kennis en kunde.
8. Er voor het gebruik van de VenJ Federatieve Dienst een vertrouwensrelatie is tussen de aangesloten sectoren en de dienstverlener SSC-ICT in het gebruik, opslag en veiligheid van de Rijksidentiteiten binnen de dienst.
9. De VenJ Federatieve Dienst volgens PDC Generieke-I, dienstverleningsniveau B wordt geleverd.

<u>Ad. Use cases</u>
Tijdens de workshops is uitgebreid stilgestaan bij de use cases van de sectoren en relatie tot de gestelde behoeftes. Deze zijn uiteindelijk als algemene use cases verwoord, en is per use case aangegeven welke ICT voorzieningen (niet limitatief) daarop betrekking hebben. Uit gesprekken naderhand met DJI en CJIB zijn daar nog extra use cases aan toegevoegd:

#	Use-Case(s)	ICT Voorziening(en)
1.	Een Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst die gehost wordt buiten het Rijk (en dus buiten Rijksweb-VPN/Rijks-cloud).	OMS
2.	Een Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt gehost bij een externe dienstverlener (als extensie van het Rijksweb-VPN/Rijks-cloud).	OMS
3.	Een Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een departement.	DigiJust
4.	Een Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een (gefedereerd) departement, maar wordt gehost bij een externe dienstverlener (als extensie van het domein van het (gefedereerde) departement).	Bestandenpostbus
5.	Rijksmedewerker krijgt vanuit een digitale 'untrusted' omgeving (internet) met zijn mobiele device toegang tot een informatiedienst, die wordt gehost in Rijksweb-VPN/Rijks-cloud.	Bestandenpostbus OMS GOOD
6.	Een "derde" krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt gehost in Rijksweb-VPN/Rijks-cloud.	OMS
7.	Een "derde" krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een departement.	CJIB Boeteapplicatie
8.	Een "derde" krijgt vanuit een digitale 'untrusted' omgeving (internet) met zijn mobiele device toegang tot een informatiedienst, die wordt gehost in Rijksweb-VPN/Rijks-cloud.	CJIB Boeteapplicatie Bestandenpostbus GOOD

Ad. Pakket Van ((non)functionele) Eisen (PvE)
Het PvE is de vertaling van de use cases naar (non)functionele eisen en wensen, en is opgebouwd uit de onderdelen Algemeen, Proces, Organisatie, Techniek en Informatie. Per eis is waar nodig de relatie gelegd met de ontwikkelpunten, en dient per eis/wens te worden aangegeven of de technisch beheerder hieraan kan voldoen. De hierboven beschreven use cases zijn ook vastgelegd in het PvE (werkblad Algemeen). Zie bijlage I voor de uitwerking van de (non)functionele eisen en wensen.

Ad. Eindbeeld gewenste situatie VenJ Federatieve Dienst
Op basis van het PvE wordt richting gegeven aan het eindbeeld van de gewenste situatie. Dit is uiteengezet in de volgende architectuurplaat. Van het eindbeeld zijn tevens de delta's van het verandertraject van IST naar SOLL op de services in kaart gebracht.

Let op: het eindbeeld geeft niet aan wanneer of hoe het migratiescenario eruit komt te zien naar de gewenste situatie. Dit zal pas duidelijk worden na uitvoering van de impactanalyse. Er kan dus een tijdlang sprake zijn van een 'hybride'-situatie totdat het eindbeeld is bereikt.

Werkplek services:
De werkplekservices wordt opgedeeld in een werkplekservices intern en een werkplekservices extern.
De Werkplekservices intern bestaat uit de gebruikersgroepen zoals ook bekend zijn vanuit de IST-situatie:
- DWR gebruikers
- overige gebruikers Rijksoverheid.

De werkplekservices Extern bestaan uit:
- gebruikersgroep Overige gebruikers Extern;
  bestaande uit ketenpartners en uit de 'externe gebruiker' (bijv. ZZP-er), die vanuit doelmatigheid als individu bijvoorbeeld van OMS gebruik moet maken;
- koppelvlak e-ID (e-Herkenning, DigiD) voor het digitale contact met burgers en bedrijven.

  Het onderscheid tussen de koppeling van ketenpartners[3] en de koppeling met burgers/bedrijven is gelegen in de voorziening waarvan gebruik moet worden gemaakt, maar ook in de wijze van ontsluiten; ketenpartners worden elk via een eigen federatief koppelvlak ontsloten, terwijl burgers en bedrijven gebruiken maken van het e-herkenning/DigiD koppelvlak.

Middels HomeRealmDiscovery (HRD) moet de VenJ Federatieve Dienst in staat zijn om te bepalen van welke (rijks of ketenpartner-)organisatie de gebruiker afkomstig is. Dit is van belang in de aansluiting van ICT-voorzieningen en waartoe een gebruiker toegang moet krijgen.

VenJ Federatieve Service
Voor de *Werkplekservices Intern* behouden sectoren hun eigen federatieve koppelvlak en blijven zij verbonden in zijn rol als sectorale Identity- en/of Service Provider. De delta t.o.v. de bestaande situatie is dat een sector dan ook als service provider gepositioneerd kan worden met het aanbieden van sector-specifieke en/of intersectorale ICT-voorzieningen.

3 Ketenpartners hebben een samenwerkingsverband met het Rijk als gevolg van een gemeenschappelijk doel, belang en/of bedrijfsprocessen, gedeelde informatiebehoeften binnen dezelfde informatieketen.

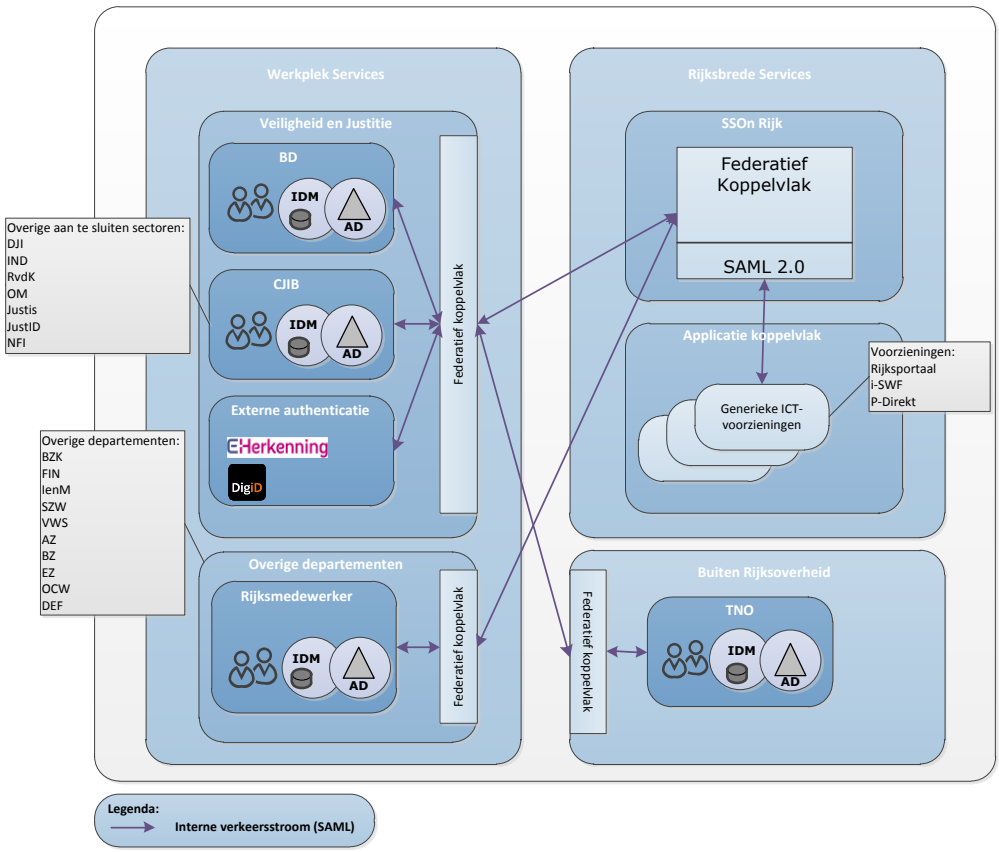
De VenJ Federatieve Dienst wordt volgens het eindbeeld gehost binnen het daarvoor ingericht veilige koppelvlak (de DMZ). Binnen dit veilige koppelvlak zijn aanvullende IT-veiligheidsmaatregelen getroffen waarmee minimaal BIR-compliancy en maximaal het ambitieniveau Dep-V hoge dreiging zou kunnen worden bereikt, zoals:

- scheiding (fysiek en logisch) van externe en interne verkeerstromen naar de SSOn systemen. Deze worden ook gescheiden over het Rijksnetwerk getransporteerd;
- vanwege de hoge beschikbaarheid een redundante uitvoering van de SSOn systemen;
- introductie van multi-factor authenticatie (MFA);
  De impact van compromittering van de credentials, wordt met single sing-on evenredig groter wat al snel reden kan zijn om sterkere authenticatie met verschillende authenticatiemiddelen toe te willen passen.
  De informatie-eigenaar van een ICT-voorziening bepaalt straks zelf welk authenticatieniveau vereist is voor toegang. Als het authenticatieniveau hoger is dan waarmee de gebruiker is ingelogd, ontvangt deze gebruiker een melding met het verzoek op een hoger niveau in te loggen (bijvoorbeeld met SMS-authenticatie / One Time Password, token, smartcard-login, etc.), en wordt in de federatie het hogere inlogniveau geregistreerd.
- gebruik van PKIo-servercertificaten voor het leggen van federatieve trustrelaties tussen de VenJ Federatieve Dienst en de verschillende sectoren;
- gebruik van e-herkenning, DigiD als koppelvlak voor het digitale contact met burgers en bedrijven;
- systeemlogging en rapportage (SIEM) volgens audit-based computing.

Het toetsen of de dienst aan het gevraagde betrouwbaarheidsniveau voldoet, en na de doorontwikkeling live kan gaan, wordt mede bepaald aan de hand van een nog uit te voeren Security Analysis Assurance Method-analyse (SAAM) door de NBV. Bovendien dient er ook een organisatorische vertrouwensrelatie (juridisch via een convenant) te worden aangaan tussen het Ministerie van Veiligheid en Justitie en elk aangesloten (keten)partner. Hiermee wordt ook de organisatorische veiligheidsmaatregelen georganiseerd en daarmee de verantwoordelijkheid bepaald voor het gecontroleerd gebruik van identiteiten en toegang tot de ICT-voorzieningen door externe (keten)partners.

SAML 2.0 blijft binnen de VenJ Federatieve Dienst het preferente standaard protocol. Dit is vooral bedoeld voor gebruik van de webservices, oftewel de functionaliteit die voor de gebruiker bereikbaar is via de webbrowser. De doorontwikkeling gaat echter ook uit van de inzet van OAUTH. Deze twee protocollen zijn binnen VenJ vooral van toepassing in het gebruik van mobile apps en devices. Waar mogelijk wordt het gebruik van Kerberos als standaardprotocol voor authenticatie op services vervangen door SAML.

<u>Applicatie-services</u>
In het eindbeeld wordt de ontsluiting van ICT-voorzieningen niet meer beperkt tot alleen de generieke voorzieningen Rijksportaal, i-SWF en P-Direkt.
Het is dadelijk onder strikte randvoorwaarden mogelijk specifieke voorzieningen vanuit het primaire proces te ontsluiten, waardoor een sector de rol van Service Provider kan gaan vervullen.



Figuur 2 Eindbeeld doorontwikkeling VenJ Federatieve Dienst

6 Opdrachtdefinitie, planning en financiering doorontwikkeling

Om de technische en organisatorische consequenties van de functionele specificaties te onderzoeken, wordt als vervolgstap in het proces een impactanalyse uitgevoerd door de technisch beheerder van de dienst, SSC-ICT. Na de impactanalyse wordt vastgesteld op welke wijze invulling kan worden gegeven aan het verandertraject. Bedoeling is dat het resultaat van deze processtap volgens een project ten uitvoer zal worden gebracht. De impactanalyse vormt daarop de voorbereidingsfase van het project. Voor de impactanalyse is de volgende opdracht van toepassing:

<u>Opdracht:</u>
Hoofdvraag – en tevens de opdracht - aan SSC-ICT:

Onderzoek met een impactanalyse de haalbaarheid en uitvoerbaarheid van de doorontwikkeling van de VenJ Federatieve Dienst. De impactanalyse geeft antwoord in de (on)mogelijkheden, complicaties en consequenties van de betreffende doorontwikkeling op het gebied van techniek/product/processen, tijd, geld en risico's met behulp van de volgende subvragen:

- aan welke eisen en wensen van het bijgevoegd PvE (zie hoofdstuk 5) de technisch beheerder wel of niet kan voldoen?
  Dit dient te worden aangegeven via 'comply or explain', eventueel (voor de compliancy) met aanvullende randvoorwaarden;
- hoe wordt de doorontwikkeling technisch gefaciliteerd voor organisatie/gebruiker/infrastructuur;

- welke (extra) maatregelen moeten worden getroffen in ICT-infrastructuur (apparaat, datacommunicatie, backoffice), licenties, certificaten, beveiliging (BIR), authenticatiemiddelen, functionaliteit;
- hoe ziet het beheer (inclusief de service levels) en helpdeskondersteuning eruit;
- wat zijn de project, ontwikkel- en exploitatiekosten en/of mogelijke besparingen;
- wat technische architectuur / ontwerp van de SOLL-situatie;
- hoe ziet het realisatieplan eruit, wat is daarvan de doorlooptijd (en roadmap) om te komen tot de SOLL-situatie;
- wat is het implementatie/migratiescenario;
- wat zijn de risico's voor de totale dienstverlening van de uitvoerende organisatie;
- andere (nog niet nader genoemde) punten; gemiste kansen en "witte vlekken"?

Planning:
De impactanalyse maakt integraal onderdeel uit van de doorontwikkeling en dient als apart 'processtap' binnen 3 maanden - na opdracht van DI&I - te zijn uitgevoerd door SSC-ICT. Voorlopig wordt de volgende planning van doorontwikkeling aangehouden, met daarin opgenomen de planning voor de impactanalyse:

	2015				2016				2017			
Fasen:	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Fase 1: Impactanalyse / Vooronderzoek												
Fase 2: Realisatie doorontwikkeling												
Fase 3: Migratie bestaande voorziening naar eindbeeld												
Fase 4: Nazorg en afsluiting project												

Bovenstaande conceptplanning is een indicatieve planning, waarvan alleen de impactanalyse concreet volgens deze opdrachtdefinitie qua doorlooptijd is opgenomen.
Een definitieve planning voor het project wordt pas bekend op basis van de uitkomsten van de impactanalyse.

(tussen-)producten:
Plan van aanpak; Voorafgaand aan de uitvoering van de impactanalyse wordt een offerte met een plan van aanpak opgeleverd aan de opdrachtgever. In het plan van aanpak zijn opgenomen de mensen, middelen, aanpak, planning en budget die nodig zijn voor de uitvoering van deze opdracht.
Eindrapportage; met de concrete beantwoording van hoofd- en subvragen. Uitkomsten van de rapportage, en met name het realisatieplan, implementatiescenario zullen als input gebruikt gaan worden voor de vervolgfasen van het project.

Financiering:
De impactanalyse wordt gefinancierd uit het doorontwikkelingsbudget VenJ.

Het is op dit moment lastig een opgaaf te doen van de totale doorontwikkelingskosten. Vandaar dat DI&I dit via de impactanalyse boven tafel wil krijgen.
Dit zal meteen een duidelijk beeld geven in hoeverre financiële dekking bestaat voor het realisatietraject, en wat de financiële effecten zullen zijn op de exploitatie van de dienst.

Governance:

- Opdrachtgever impactanalyse is DI&I (systeemeigenaar VenJ Federatieve Dienst).
- Voor de uitvoering van de impactanalyse stelt SSC-ICT een aanspreekpunt aan, die als single point of contact naar DI&I optreedt. Deze persoon is ook bij SSC-ICT ook verantwoordelijk voor de uitvoering van de impactanalyse.
- Sectoren worden opgeroepen actief deel te nemen tijdens de impactanalyse. Doel hiervan is om in samenwerking met andere sectoren te fungeren als klankbord voor de gepresenteerde (tussen)resultaten.
- De eindrapportage wordt ter besluitvorming voorgelegd aan de opdrachtgever.

Directie Informatisering en Inkoop

Datum
6 augustus 2015

Ons kenmerk
VenJ / DI&I

Bijlage I – Pakket Van Eisen

Document: *Doorontwikkeling VenJ Federatieve Dienst - Pakket Van Eisen v1.0*

Revisie

Document:
Doorontwikkeling VenJ Federatieve Dienst - Pakket Van Eisen

Inleiding:
Overzicht van de functionele en non-functionele specificaties voor de doorontwikkeling van de VenJ Federatieve Dienst

Versie:	Datum:	Auteur:	Wijzigiging:
0.1	25-jul-15	DI&I	Initiele versie Gebaseerd op input/review SSOn workshops door BD, CJIB, DJI, IND, RvdK en SSC-ICT
1.0	1-aug-15	DI&I	N.a.v. review #1 DI&I

REQUIREMENTS -

Nr:	Prio:	T/F:	MoSCoW
DO-001	H	F	Sh
DO-002	H	T	M
DO-003	H	T	M
DO-004	H	T	M
DO-005	H	T	M
DO-006	L	T	M

Let op: De hier beschreven ontwikkelpunten vormen de basis voor de Doorontwikkeling VenJ Federatieve Dienst, en komen voort uit de diverse behoeftes zoals die door de verschillende sectoren zijn ingediend.
Ter referentie van de functionele eisen en/of wensen is eventueel het betreffende ontwikkelpunt toegekend.

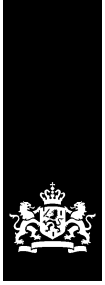
(NON)FUNCTIONAL REQUIREMENTS - ALGEMEEN										
#	Omschrijving	F/N	Use Cases				EIS/WENS	ICT Beheerder	
			BD	DJI	IND	RVDK		Comply	Explain
REQ-ALG-001	VenJ verstrekt als 'broker' toegang tot interne en externe Identity Providers en Service Providers aan Rijksmedewerkers, particulieren, bedrijven en ketenpartners, kennis/opleidingsinstituten met wie het rijk samenwerkt. Toegang tot de ICT voorziening wordt ingesteld met policies. De IdP dient op basis van authenticatie (ID en bijbehorende attributen) het benodigde SAML-token te vervaardigen voor de Sevice Providers.	N	X	X	X	X	EIS		
REQ-ALG-002	In relatie tot REQ-ALG-001 moet toegang ook mogelijk zijn buiten het overheidsdomein (voor aangesloten IdP/SP)	N	X	X	X		EIS		
REQ-ALG-003	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst die gehost wordt buiten het Rijk (en dus buiten Rijksweb-VPN/Rijkscloud).	F		X			EIS		
REQ-ALG-004	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt gehost bij een externe dienstverlener (als extensie van het Rijksweb-VPN/Rijkscloud)	F					EIS		
REQ-ALG-005	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een departement.	F	X				EIS		
REQ-ALG-006	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een (gefedereerd) departement, maar wordt gehost bij een externe dienstverlener (als extensie van het domein van het (gefedereerde) departement).	F	X				EIS		
REQ-ALG-007	Rijksmedewerker krijgt vanuit een digitale 'untrusted' omgeving (internet) met zijn mobiele device toegang tot een informatiedienst, die wordt gehost in Rijksweb-VPN/rijkscloud.	DI&I	Bestandenpostbus	OMS			EIS		
REQ-ALG-008	Een "derde" krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt gehost in Rijksweb-VPN/Rijkscloud. *Een derde kan zijn een gebruiker van een ketenpartner, lagere overheid, onderzoeksinstituut, sourcing partij, leverancier, student, externe gebruiker (niet van de eerder genoemde organisaties) of burger/bedrijf (via e-EID), etc.*	DI&I				e-SWF	EIS		
REQ-ALG-009	Een "derde" krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een departement. *Een derde kan zijn een gebruiker van een ketenpartner, lagere overheid, onderzoeksinstituut, sourcing partij, leverancier, student, externe gebruiker (niet van de eerder genoemde organisaties) of burger/bedrijf (via e-EID), etc.*	F	VenJ transactiemodule				EIS		
REQ-ALG-010	Een "derde" krijgt vanuit een digitale 'untrusted' omgeving (internet) met zijn mobiele device toegang tot een informatiedienst, die wordt gehost in rijksweb-VPN/rijkscloud. *Een derde kan zijn een gebruiker van een ketenpartner, lagere overheid, onderzoeksinstituut, sourcing partij, leverancier, student, externe gebruiker (niet van de eerder genoemde organisaties) of burger/bedrijf (via e-EID), etc.*	F	VenJ transactiemodule			e-SWF	EIS		

(NON) FUNCTIONAL REQUIREMENTS - PROCES									
#	Omschrijving	F/N	Use Cases				EIS/WENS	ICT Beheerder	
			BD	DJI	IND	RVDK		Comply	Explain
REQ-PRC-001	Maakt gebruik van Audit Based Access Control; toegang tot informatie gebeurt als de persoon over de juiste attributen/claims beschikt, maar het draait vooral om achteraf afleggen van controle en verantwoording.	N	X	X	X	X	EIS		
REQ-PRC-002	Moet via het proces Life cyclemanagement worden onderhouden. *Er is nog geen functioneel beheer op de VenJ Federatieve dienst, alleen technisch, lijst opstellen met gewenste updates op onderdelen.*	N	X	X	X	X	EIS		
REQ-PRC-003	Heeft een koppeling met het (de)provisioning proces. Met "provisioning" wordt hier niet alleen gedoeld op "het aanmaken van het ICT-account", maar hieronder valt ook het beheren van de attributen bij het ICT-account gedurende de levenscyclus van het account tot en met het buiten werking stellen van het account op het moment dat de persoon geen werkrelatie meer heeft met de Rijksoverheid en daardoor ook geen toegang mag hebben tot de aangesloten ICT-voorzieningen.	N	X	X	X	X	EIS		
REQ-PRC-004	Sessie parameters: Opzetten van de eerste authenticatieoverdracht is de maximale wachttijd: 2-8 seconden Maximum sessieduur: 8 uur Maximum sessie idle time: 60 minuten Maximaal aantal concurrent sessies per gebruiker: 2 Instandhouding van een sessie (waarbij doorgaans ook authenticatieoverdracht plaatsvindt) is niet merkbaar voor de eindgebruiker	N	X	X	X	X	EIS		
REQ-PRC-005	Applicatiespecifieke sessies worden geïnvalideerd door de ICT-voorziening zelf.	N	X	X	X	X	EIS		
REQ-PRC-006	Ondersteunt het (tijdelijk) ongedaan maken van een reeds uitgevoerde authenticatie (logoff) teneinde inloggen op meervoudige dienstverbanden/werkrelaties te ondersteunen.	N	X	X	X	X	EIS		
REQ-PRC-007	Is geschaald zodat wordt voldaan aan het aantal concurrent login request op de piekmomenten.	DI&I	X	X	X	X	EIS		
REQ-PRC-008	Indien niet voldaan blijft worden aan de aansluitvoorwaarden (compliancy), kan de IdP en/of SP worden afgesloten voor de dienstverlening.	DI&I	X	X	X	X	EIS		
REQ-PRC-009	Borgen en monitoren dat aanbiedende leveranciers (IdP en/of SP) voldoen aan afgesproken aansluitvoorwaarden. Juridische dienstverleningsovereenkomsten (contracten) afsluiten tussen aansluitende partijen, en het proces regelmatig auditen in opzet, bestaan en werking.	N	X	X	X	X	EIS		

(NON) FUNCTIONAL REQUIREMENTS - ORGANISATIE									
			Use Cases					ICT Beheerder	
#	Omschrijving	F/N	BD	DJI	IND	RVDK	EIS/WENS	Comply	Explain
REQ-ORG-001	Regel de omgang van 'onzichtbaren' in de keten (vertrouwelijke identiteiten).	N	X	X	X	X	EIS		
REQ-ORG-002	Het is alleen mogelijk om persoonsgebonden accounts te gebruiken.	F	X	X	X	X	EIS		
REQ-ORG-003	Een gebruiker kan op basis van zijn claim; identiteit, rol en eigenschappen/werkrelatie de juiste ingang/autorisatieniveau in de ICT-voorziening toebedeeld krijgen.	F	X	X	X	X	EIS		

(NON) FUNCTIONAL REQUIREMENTS - TECHNIEK										
			Use Cases					ICT Beheerder	
#	Omschrijving	F/N	BD	DJI	IND	RVDK	EIS/WENS	Comply	Explain
REQ-TNK-001	Dient zowel “rich client”, mobile devices en het gebruik van webbrowser en (mobile) applicaties te ondersteunen.	N	X	X	X		EIS		
REQ-TNK-002	Dient ook externe federatie te ondersteunen buiten het overheidsdomein (zie tevens REQ-ALG-002). ***.rijksweb.nl** zone voldoet alleen voor interne ICT-voorzieningen, en biedt met deze eis de mogelijkheid om diensten buiten rijksweb dns te kunnen ontsluiten.	F		X	X	X	EIS		
REQ-TNK-003	Gebruik van 2-way trust tussen de centrale IdP/SP en decentrale SP/IDP's	N	X	X	X	X	EIS		
REQ-TNK-004	Binnen het verzorgingsgebied van SSC-ICT moet het mogelijk zijn om achterliggende sectoren van de departementen binnen het verzorgingsgebied van SSC-ICT aan te sluiten.	N	X	X	X	X	EIS		
REQ-TNK-005	Rapportagemogelijkheid voor aangesloten diensten t.b.v. logging en auditing. Heeft systeemlogging die configurabel moet zijn, en interoperabel kunnen werken met SIEM-oplossingen	N	X	X	X	X	WENS		
REQ-TNK-006	Gebruik van SAML-scoping (met IdP whitelist/blacklist functionaliteit) Lijst met aanbod van de Identity Providers die mogen inloggen bij een Service Provider	N	X	X	X	X	EIS		
REQ-TNK-007	Heeft een koppelvlak met het eID-stelsel (e-Herkenning / DigiD), en dient deze te borgen in de keten-infrastructuur	DI&I	X	X	X	X	EIS		
REQ-TNK-008	Het gebruik van Kerberos / SPNEGO voor gebruik ICT-voorzieningen dient te worden uitgefaseerd. Voor bestaande ICT-voorzieningen wordt een migratieplan op gesteld (en de migratie daadwerkelijk uitgevoerd) om de ICT-voorziening SAML geschikt te maken.	DI&I	X	X	X	X	EIS		
REQ-TNK-009	Het authenticatiebewijs bevat minimaal één attribuut dat de Service Provider in staat stelt deze te relateren aan één of meerdere identiteiten. Autorisatie gebeurt binnen de ICT-voorziening (claim based rules) op basis van relevante attributen.	N	X	X	X	X	EIS		
REQ-TNK-010	Kan authenticatiebewijzen (tokens) doorgeven aan service providers (van mobiele apps).	F					WENS		
REQ-TNK-011	Het Mobile device management platform moet hergebruik van authenticatiebewijzen voor mobile apps faciliteren binnen de geldigheid van het authenticatiebewijs (FOLLOW ME-principe)	N					WENS		
REQ-TNK-012	Werken met pseudo id's (zodat interne identiteiten niet zichtbaar worden in de onvertrouwde buitenwereld (internet))	F	CIOT				EIS		
REQ-TNK-013	Indien gefedereerde ICT-voorzieningen of organisaties van buiten de Haagse ring benaderd moeten kunnen worden, dan is het gebruik van reverse proxy's vereist om de Identity Providers naar buiten toe beschikbaar te maken.	N	X	X	X	X	EIS		

(NON) FUNCTIONAL REQUIREMENTS - INFORMATIE & VEILIGHEID										
			Use Cases					ICT Beheerder	
#	Omschrijving	F/N	BD	DJI	IND	RVDK	EIS/WENS	Comply	Explain
REQ-INF-001	Uitwisseling van authenticatiebewijzen is veilig; - versleuteling volgens SHA256 - spoofing/replay is onmogelijk	N	X	X	X	X	EIS		
REQ-INF-002	De dienstverlening is BIR-compliant met een minimaal geadviseerd beveiligingsniveau van 2 (voorheen WBP-2). Gegevensclassificatie is tot en met departementaal vertrouwelijk (niet staatsgeheim, tm hoge dreiging) Een SAAM-analyse (in opdracht van DI&I en uitgevoerd door het NBV) maakt onderdeel uit van het doorontwikkeltraject om het geadviseerde beveiligingsniveau 2 aan te tonen.	N	X	X	X	X	EIS		
REQ-INF-003	Dient ongevoelig te zijn voor DDOS attacks en SQL injections.	N	X	X	X	X	EIS		
REQ-INF-004	Is in staat om Multi-factor authentication (1, 2 en Step-up varianten) midddelen aan te sluiten en doelmatig te beheren.	N	X	X	X	X	EIS		
REQ-INF-005	Gebruik van compartimentering tussen intern en externe diensten.	N	X	X	X	X	EIS		
REQ-INF-006	Per aan te sluiten IdP of SP wordt een berichtenboek (met SAML profielen) opgesteld. Een berichtenboek legt vast op basis van welke gegevens interfacing plaatsvindt.	N	X	X	X	X	WENS		
REQ-INF-007	De back-office systemen staan opgesteld in een vertrouwd en veilig netwerk van de Rijksoverheid. Netwerkfilters zorgen er voor dat kwaadaardige data wordt geblokkeerd voordat de systemen besmet of gecompromitteerd kunnen worden.	DI&I	X	X	X	X	EIS		
REQ-INF-008	Het netwerkverkeer op het overheidsnetwerk moet continu intensief geïnspecteerd worden op signalen van besmetting en compromittering. Op signalen van compromittering wordt snel en effectief gereageerd.	DI&I	X	X	X	X	EIS		
REQ-INF-009	Beheerders (technisch en functioneel) maken gebruik van sterke authenticatie (met betrouwbare beperking van het aantal login pogingen) voor toegang tot de beheerfuncties van de dienst.	N	X	X	X	X	EIS		
REQ-INF-010	Het identificerende attribuut is het departementale UserPrincipalName, emailadres of RIN.	N	X	X	X	X	EIS		
REQ-INF-011	De services (ICT-voorzieningen) die worden aangeboden moeten om kunnen gaan met externe identiteiten (van vertrouwde partijen)	N	X	X	X	X	EIS		



SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Doorontwikkeling Federatieve Service

Definitiestudie

Auteur: Tim van Dijen

Opdrachtgever: Dhr. R. P. van Kruistum

Datum: 2 november 2015
Versie: 1.1
Status: Definitief

Colofon

Afzendgegevens	**DG Organisatie Bedrijfsvoering Rijk** SSC-ICT Haaglanden Pijler 2 Luxemburglaan 2 2711 BC Zoetermeer Postbus 7385 2701 AJ Zoetermeer
Contactpersoon	T. van Dijen T 079 330 22 00 F 079 330 22 22
Projectnaam	Doorontwikkeling VenJ Federatieve Dienst
Auteurs	T. van Dijen

Documenthistorie

Versie	Status	Datum	Wijzigingen
0.1	Concept	1-11-2015	Eerste versie
1.0	Definitief	3-11-2015	Vastgesteld i.o.m. opdrachtgever
1.1	Definitief	4-11-2015	Spelling

Inhoudsopgave

1. Inleiding

Voorliggende rapportage is een technische analyse van de huidige situatie van de federatieve dienst van het Ministerie van Veiligheid en Justitie. Ook geeft het rapport inzicht in de gewenste situatie.

1.1 Opdracht

De opdracht is een onderzoek met een impactanalyse voor de doorontwikkeling van de federatieve dienst van het Ministerie van Veiligheid en Justitie. De impactanalyse geeft een beeld van de (on)mogelijkheden, complicaties en consequenties van de betreffende doorontwikkeling op het gebied van techniek, producten, processen, tijd, geld en risico's. Dit beeld wordt gevormd aan de hand van de volgende sub-vragen:

- Welke (extra) maatregelen moeten worden getroffen in de ICT infrastructuur (hardware, datacommunicatie, backoffice), licenties, certificaten, beveiliging (Baseline Informatiebeveiliging Rijksdienst), authenticatiemiddelen en functionaliteit;
- Hoe ziet het beheer (inclusief de service levels) en helpdeskondersteuning eruit;
- Wat zijn de project, ontwikkel- en exploitatiekosten en/of mogelijke besparingen;
- Wat is de technische architectuur / het ontwerp van de gewenste situatie;
- Hoe ziet het realisatieplan eruit, wat is daarvan de doorlooptijd (en roadmap) om te komen tot de gewenste situatie;
- Wat is het implementatie/migratiescenario;
- Wat zijn de risico's voor de totale dienstverlening van de uitvoerende organisatie;
- Andere (nog niet nader genoemde) punten; gemiste kansen en "witte vlekken"?

1.2 Bronnen

Nr.	Titel	Datum / Versie	Bron
01	Functioneel ontwerp (Departementaal Vertrouwelijk)		MinVenJ
02	Doelarchitectuur Toegang	30-5-2015 / v0.8	MinBZK - Tactische Regie op de Generieke ICT (TBGI)
03	Functionele specificaties	V1.0	DI&I
04	Pakket van eisen	V1.0	DI&I
05	Impactanalyse doorontwikkeling Rijks-SSOn (Departementaal Vertrouwelijk)	V1.0	MinBZK - TBGI
06	Baseline Informatiebeveiliging Rijksdienst – Technisch Normenkader	1-12-2012 / v1.0	MinBZK - TBGI

1.3 Leeswijzer

Hoofdstuk 2 bevat de achtergrond van de opdracht en de eisen/wensen van zowel de opdrachtgever als de beheerder.

Hoofdstuk 3 bevat een overzicht van de huidige situatie.

Hoofdstuk 4 bevat een analyse van de huidige technische situatie, de authenticatiescenario's en een voorgestelde oplossing.

Hoofdstuk 5 is een impactanalyse van de governance-aspecten van een federatieve dienst.

Hoofdstuk 6 is een impactanalyse op de informatiebeveiliging van de federatieve dienst.

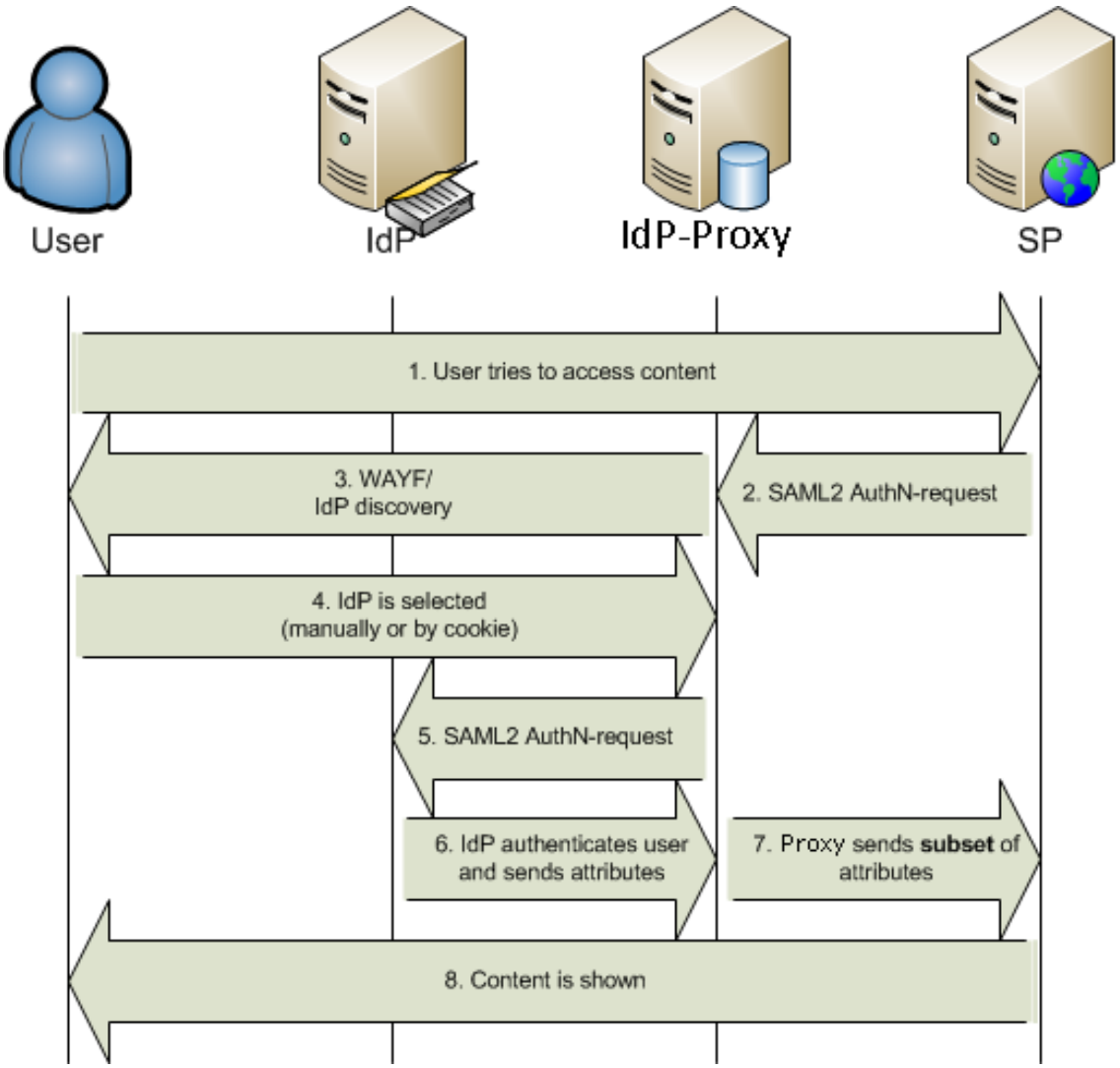
Hoofdstuk 7 bevat de bijlagen behorende bij dit document.

2. Achtergrond Federation

Een federatie in zijn meest simpele vorm bestaat uit een Identity Provider (IdP) en een Service Provider (SP). Door middel van een Identity Provider Proxy (IdP-Proxy, ook wel broker of bridge genoemd) kunnen ook complexe federatieve ketens gemaakt worden. De SP is een webapplicatie, welke zelf geen eigen identity store heeft. Een gebruiker die naar de webapplicatie gaat, en nog geen geldige security token heeft, zal worden doorverwezen naar de IdP. Hier moet worden ingelogd, waarna de gebruiker met een security token weer wordt teruggestuurd naar de webapplicatie. Door de onderlinge vertrouwensrelatie tussen de SP en de IdP, zal de gebruiker worden toegelaten tot de applicatie. Deze vertrouwensrelatie is gebaseerd op PKI (Public Key Infrastructure). Het onderlinge berichtenverkeer verloopt middels het SAML protocol. Zie Figuur 1 op de volgende pagina voor een voorbeeld van federatieve authenticatie.

Een voorbeeld van een dergelijke omgeving binnen de publieke sector is DigID. Diverse overheidssites (SP's) vereisen dat een bezoeker zich authentiseert bij DigID (IdP). De SP's vertrouwen hierbij op de authenticatie van deze IdP. Op deze manier hoeft niet elke website een eigen identity store te hebben.

Aanvullend op het concept van de federatieve dienst kan voor eindgebruikers een Single Sign-On (SSO) ervaring worden gecreëerd, zodat zij niet bij elke federatief ontsloten applicatie apart moeten inloggen. De authenticatie vindt dan plaats bij het inloggen op het werkstation, waarbij een Kerberos-token wordt verkregen. Wanneer de gebruiker via een Service Provider naar een Identity Provider wordt gestuurd (1), zal de browser het Kerberos-token meesturen. De Identity Provider kan deze tegen de achterliggende identity store verifiëren (2, 3, 4, 5), waarna de gebruiker automatisch en volledig transparant voorzien wordt van een SAML-token en weer wordt teruggestuurd naar de Service Provider (6, 7).



Figuur 1: Voorbeeld federatieve authenticatie

3. Huidige situatie

De federatieve dienst van het Ministerie van Veiligheid en Justitie bestaat uit vijf IdP's, twee SP's en twee IdP-Proxy's, waarvan één IdP-Proxy en drie IdP's in beheer zijn van SSC-ICT. De overige componenten worden beheerd door de Justitiële Informatiedienst (JustID). Het SSC-ICT-deel van de omgeving is in het verleden neergezet als Proof of Concept, waarbij niet of nauwelijks is gekeken naar zaken als beveiliging, schaalbaarheid, beschikbaarheid en beheerbaarheid. Onder druk van de opdrachtgever is deze omgeving vervolgens ingezet als productieomgeving, waarbij te weinig aandacht is geweest voor het beheer (omgevingen zijn niet homogeen, testomgeving is niet aanwezig), beveiliging en de documentatie van het geheel. Hierdoor is een directe behoefte ontstaan om een nieuw ontwerp te bedenken voor de federatie waarin wél rekening gehouden wordt met bovenstaande problematiek.

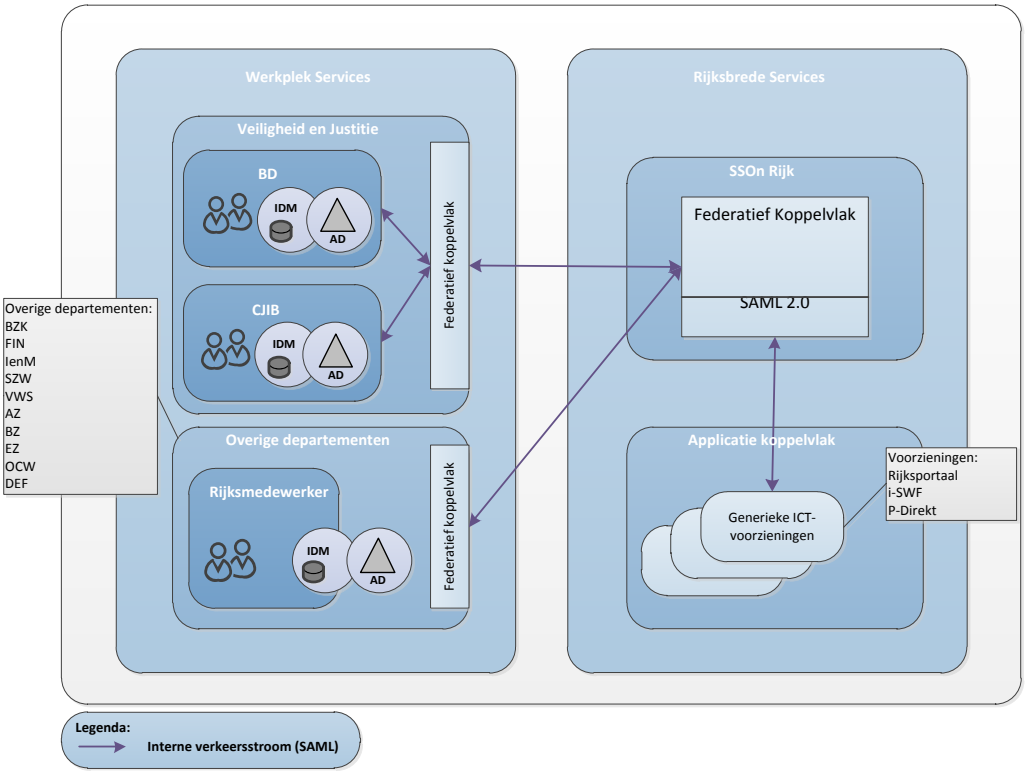
3.1 Perspectief opdrachtgever

Vanuit het perspectief van de opdrachtgever is de ontwikkeling van de VenJ federatieve service te langzaam gegaan. Er zijn sinds 2013 slechts twee van de beoogde drieëntwintig VenJ-onderdelen ontsloten op de VenJ-federatie en de kosten voor het beheer zijn onevenredig groot. Daarnaast is de omgeving niet flexibel genoeg om op veranderende behoeften in te spelen, zoals het gefedereerd kunnen aanbieden van legacy applicaties.

3.2 Perspectief beheerder

Vanuit het perspectief van de beheerder is het lastig om de omgevingen adequaat te beheren. Er wordt gewerkt met verschillende producten voor verschillende componenten, de gelijke componenten zijn anders ingericht/geconfigureerd, het product wat voor de IdP-Proxy in gebruik is heeft in het verleden de nodige problemen gehad waarbij oplostijden bij de fabrikant te wensen over liet, documentatie ontbreekt en het aantal componenten is te groot. Verder verloopt het contact met andere beheerpartijen moeizaam.

De huidige VenJ federatieve dienst bestaat uit een vijftal IdP's, twee proxy's en twee SP's, verdeeld over twee beheerpartijen (SSC-ICT en JustID). Totaal moet er worden samengewerkt met vier partijen (SSC-ICT, JustID, CJIB en het bestuursdepartement). Hiernaast zijn er ook nog een overheidspartij en een commerciële partij die delen van de technische infrastructuur beheren. Zie figuur 2 voor een overzicht van de bestaande VenJ federatieve dienst.



Figuur 2: Huidige situatie VenJ Federatieve Dienst

3.3 Componenten

Binnen de VenJ-federatie zijn er verschillende componenten die elk hun eigen functie hebben. De verschillende onderdelen worden hieronder beschreven.

3.3.1 Rijks-SSOn

De Rijks-SSOn is een koppelvlak op basis van Microsoft ADFS, bedoeld voor de ontsluiting van de verschillende departementen naar de rijksbrede federatie. Ook worden hier service providers aangesloten die een rijksbreed doel hebben, zoals bijvoorbeeld de Samenwerkruimten (rijksbrede Sharepoint-omgeving) en P-direkt (HRM-systeem van het rijk). Vrijwel alle departementen zijn hier op aangesloten.

Dit koppelvlak is géén onderdeel van de VenJ federatieve dienst. Wel wordt er ook op rijksbreed niveau gekeken naar een doorontwikkeling.

3.3.2 IdP-Proxy

De IdP-Proxy is het koppelvlak voor de talloze VenJ-onderdelen. Zij kunnen hierop aansluiten met hun eigen Identity Provider. Dat kan zowel door het VenJ-onderdeel zelf gedaan worden, of door SSC-ICT Haaglanden. Momenteel zijn hierop alleen het bestuursdepartement en het CJIB aangesloten. De IdP-Proxy voorziet eveneens in een koppeling naar de rijksbrede federatie en naar de VenJ Access Gateway. Deze omgeving draait op NetIQ Access Manager.

3.3.3 VenJ Access Gateway

De VenJ Access Gateway is het koppelvlak waarop VenJ-applicaties worden aangesloten en draait op Anoigo programmatuur. De applicaties kunnen zowel interne applicaties als applicaties die op internet worden aangeboden zijn, zoals de CJIB-boeteapplicatie. De VenJ Access Gateway heeft dan ook een oprit naar het internet en naar externe Identity Providers zoals DigID (overheid <> burgers) en eHerkenning (overheid <> bedrijfsleven).

3.3.4 Identity Providers

Per VenJ-onderdeel wordt er een Identity Provider aangesloten op de IdP-Proxy. De Identity Provider verzorgt de authenticatie van eindgebruikers behorende bij het VenJ-onderdeel. Identity providers zijn er op basis van Microsoft ADFS of het open source SimpleSAMLphp en kunnen zowel door SSC-ICT Haaglanden als door het VenJ-onderdeel zelf worden beheerd.

3.4 Problematiek

De verschillende componenten, maar ook de federatie als geheel kennen zo hun problemen. De bedoeling is om deze problemen in deze paragraaf te benoemen. Deze problemen zijn opgemaakt uit de verschillende interviews en uit een analyse van de componenten welke in het kader van deze definitiestudie is uitgevoerd.

Algemeen:
- Gebrek aan (keten-)regie, wat het doorvoeren van wijzigingen bemoeilijkt;
- Geen gemeenschappelijke visie of roadmap, waardoor de beheerpartijen elk hun eigen plan trekken;
- Geen beheerafspraken met relevante partijen, wat het oplossen van problemen bemoeilijkt;
- Verouderde documentatie, wat troubleshooten bemoeilijkt;
- Groot aantal betrokken partijen, wat leidt tot hoge doorlooptijden;
- Hoge kosten, wat leidt tot ontevredenheid van de klant;
- Gebrek aan een testomgeving, wat troubleshooten bemoeilijkt.

VenJ Access Gateway:
- Kan maximaal 20 aansluitingen aan, wat de ontwikkeling van de dienst beperkt;
- Geen consistent gebruik van PKIoverheid-certificaten, wat het beheer complexer maakt;

IdP-Proxy:
- Veel software-bugs die traag worden verholpen, wat de ontwikkeling van de dienst beperkt;
- Complex product waarvan slechts een klein deel benut wordt, wat leidt tot moeizaam beheer en verhoudingsgewijs hoge licentiekosten;
- Geen CRL-controle op certificaten, waardoor ingetrokken certificaten ongemerkt gebruikt kunnen blijven worden;
- Maatwerk-aanpassingen nodig om aan de wensen van de klant te voldoen, wat leidt tot hoge ontwikkelkosten;
- Product wordt oneigenlijk gebruikt voor iets waar het niet voor bedoeld is, wat de ondersteuning vanuit de leverancier bemoeilijkt;
- Werkt niet goed samen met de overige producten door gebrek aan standaarden-compliancy, specifiek de SAML-standaard. Dit heeft er toe geleidt dat bijvoorbeeld encryptie van het SAML-berichtenverkeer tot op heden niet mogelijk is geweest.

Identity Providers:
- Verschillende producten in gebruik, wat meer kennis vereist en het beheer complexer maakt;
- Gelijke componenten zijn niet gelijk ingericht, wat leidt tot complex beheer;
- Maakt onversleutelde verbinding met de achterliggende directory service, wat het afluisteren van wachtwoorden mogelijk maakt;
- Platform is niet gehardend, wat met het oog op toekomstige internetontsluiting ongewenst is vanuit beveiligingsoogpunt;
- Machines zijn niet gecompartimenteerd, wat eveneens onwenselijk is vanuit beveiligingsoogpunt.

3.5 Ontwikkelingen Rijks-SSOn

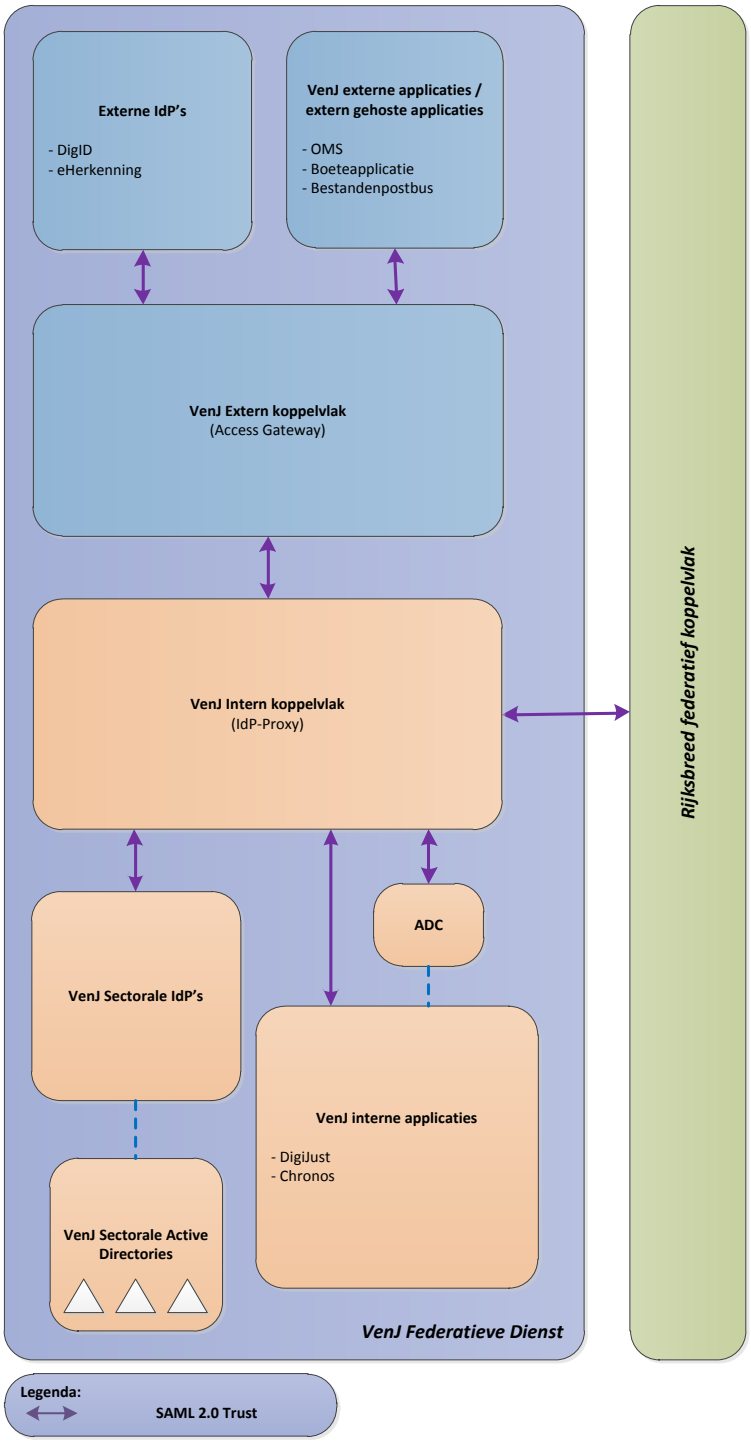
Op rijksbreed niveau vindt ook een her-/doorontwikkeling plaats van de federatieve dienst. Bewegingen op rijksniveau zijn van belang voor het maken van de juiste keuzes voor de federatieve dienst van VenJ. De belangrijkste punten uit de gedane impactanalyse zijn:

- Er moet een koppelvlak komen voor externe Identity Providers als DigID en eHerkenning, zodat niet alle departementen dit voor zich hoeven te regelen.
- Moet voldoen aan rijksbrede standaarden als de Baseline Informatiebeveiliging Rijksdienst (BIR), het Digikoppeling-stelsel en het eID-stelsel.
- Moet passen in de rijksbrede doelarchitectuur Toegang.
- Zoveel mogelijk gebruik van open source en open standaard (comply or explain) volgens het rijksbrede beleid.
- Volledig gebaseerd op SAML 2.0, legacy applicaties achter een Access Gateway.

Eén product waar heel aandachtig naar gekeken wordt is OpenConext, wat ontwikkeld is door SurfNet, open-source is, volledig SAML 2.0 compliant en beproefde technologie is.

4. Referentiearchitectuur

De referentiearchitectuur voor de VenJ Federatieve Dienst 2.0 zal gevormd worden door een federatieve service voor sectorale, sectorale/departementale SP's, externe SP's en externe IdP's. De IdP-Proxy voorziet in een koppeling naar de rijksbrede federatieve koppelvlak. Zie Figuur 3.



Figuur 3: Referentiearchitectuur

De Identity Providers en Service Provider worden ontsloten op basis van SAML2.0.

SAML 2.0 is een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen een Identity Provider en een op SAML gebaseerde applicatie (SP). Het probleem is dat (nog) lang niet alle applicaties (standaard softwarepakketten of maatwerkapplicaties) SAML 2.0 ondersteunen. Om SSO te implementeren op basis van SAML zal voor Non-SAML applicaties een SAML-Gateway functie beschikbaar moeten zijn die in staat is om het SAML protocol om te zetten naar een identificatie/autorisatie mechanisme van de betreffende applicatie. Een SAML-Gateway functie dient bij voorkeur altijd netwerk-technisch dicht bij de applicatie te staan omdat het applicatieverkeer altijd via de Gateway moet worden gerouteerd. De meest logische plaats voor de SAML-Gateway is een Application Delivery Controller (ADC), in zijn meest simpele vorm ook wel Load Balancer genoemd.

Binnen SSC-ICT maken ADC's van verschillende producenten deel uit van de standaard technische infrastructuur architectuur (TI-Architectuur). De inzet van de ADC is momenteel beperkt tot de Load Balancing functionaliteit, maar kan door aanschaf van extra softwarelicenties fungeren als een SAML-Gateway. De technologie stelt SSC-ICT in staat om te standaardiseren op basis van SAML terwijl backend applicaties nog gebruik maken van legacy identificatie/autorisatie protocollen.

4.1 Voorgestelde oplossing

De volgende uitgangspunten zijn gehanteerd om te komen tot de voorgestelde oplossing:

- De opdracht betreft doorontwikkeling van bestaande dienst naar de VenJ Federatieve Dienst 2.0;
- Waar mogelijk hergebruik makend van reeds beschikbare middelen zoals Netscalers;
- Waar mogelijk hergebruik van proven technologie zoals die van SurfNet;

Op basis van bovenstaande uitgangspunten kunnen de authenticatiescenario's uit tabel 2 gerealiseerd worden in een gefaseerde roadmap.

#	Gebruiker Type	Identiteiten-leverancier (IdP)	Werkomgeving (Client)	Applicatieomgeving (SP)	Dienst versie
1	VenJ-medewerker	Sector	Sector	Eigen sector	2.0
2	VenJ-medewerker	Sector	Sector	Ander departement	2.0
3	VenJ-medewerker	Sector	Sector	Andere sector	2.0
4	VenJ-medewerker	Sector	Sector	Extern	2.0
5	VenJ-medewerker	Sector	Extern	Extern	2.0
6	Rijksmedewerker	Sector	Extern	Extern	2.0
7	Rijksmedewerker	Sector	Sector	Departement (VenJ)	2.0
8	Rijksmedewerker	Sector	Sector	Sector (VenJ)	2.0
9	Rijksmedewerker	Sector	Sector	Extern	2.0
10	Derden	Extern	Extern	Departement (VenJ)	2.0
11	Derden	Extern	Extern	Extern	2.0

Tabel 1: Authenticatiescenario's voor roadmap

Voorgesteld wordt om de volgende roadmap te hanteren voor de realisatie:

Fase 1 "Intern"
- Infrastructuur - Authenticatiescenario's 1, 2, 3, 7 en 8 - Voorbereiding Fase 2

Fase 2 "Extern"
- Authenticatiescenario's 5 en 6 - Voorbereiding Fase 3

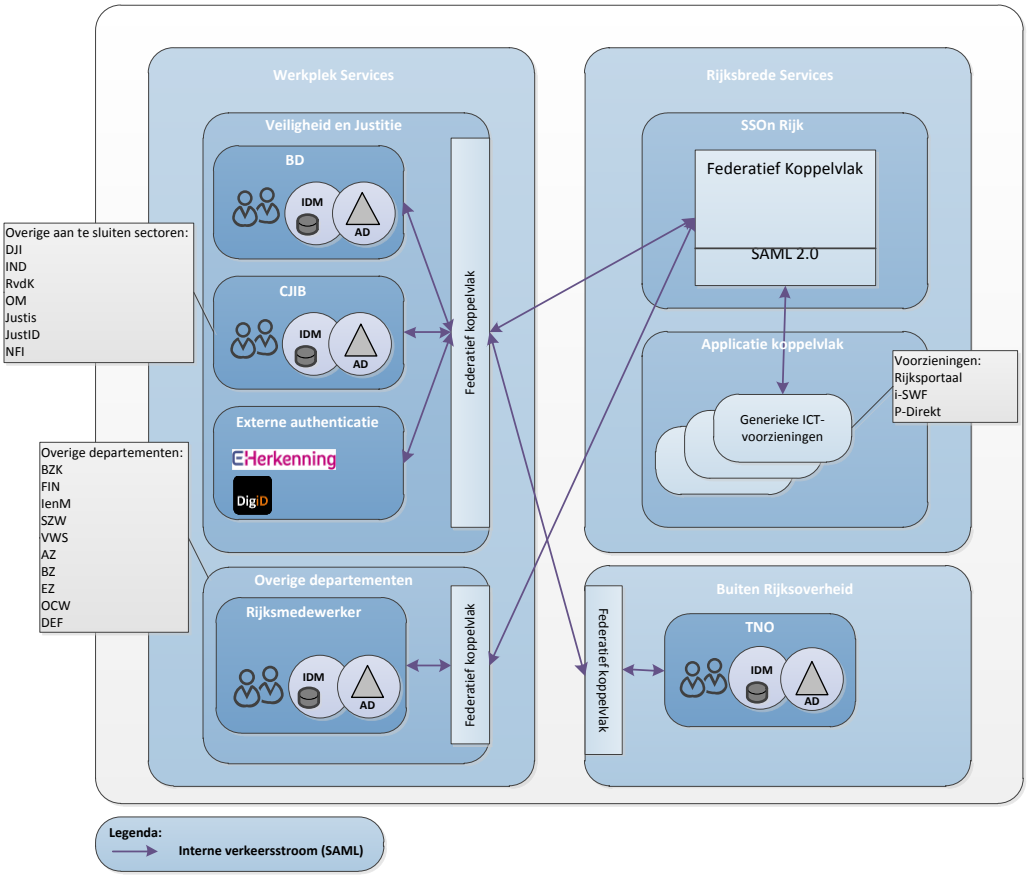
Fase 3 "Derden"
- Authenticatiescenario's 9, 10 en 11

4.2 Beantwoording Pakket van Eisen

De beantwoording van eisen, gesteld in het Pakket van Eisen, is terug te vinden in Bijlage 1 – Beantwoording Pakket van Eisen.

5. Impactanalyse techniek

Onder leiding van DI&I zijn met verschillende belanghebbenden de wensen en eisen verwoord in de functionele specificaties en het programma van eisen voor de gewenste doorontwikkeling. Er zijn onder andere use cases opgesteld voor de doorontwikkeling van de VenJ Federatieve Dienst in samenwerking met de verschillende VenJ-onderdelen (sectoren). Onderstaande schematische voorstelling is een overzicht van de gewenste VenJ Federatieve Dienst.



Figuur 4: Gewenste situatie VenJ Federatieve Dienst

Een Rijksmedewerker kan vanuit de eigen sectorale ICT-werkomgeving of extern (buiten de Rijksoverheid) toegang nodig hebben tot applicaties in verschillende applicatie-omgevingen, te weten applicaties binnen het eigen departement, applicaties op VenJ-niveau, binnen een VenJ-onderdeel, binnen een ander departement, Rijksbrede applicaties of applicaties buiten de Rijksoverheid, bijvoorbeeld op internet. De identiteiten en attributen van de Rijksmedewerker wordt geleverd vanuit het eigen departement of sector en beschikbaar gesteld binnen de rijksbrede omgeving. Wanneer de Rijksmedewerker werkt vanuit een externe omgeving (buiten de Rijksoverheid) en toegang wenst tot externe, rijksbrede, departementale of sectorale applicaties, zal hij via beveiligde faciliteiten kunnen inloggen op een eigen ICT-werkomgeving.

Derden kunnen vanuit een externe ICT-werkomgeving toegang nodig hebben tot applicaties in verschillende applicatieomgevingen, zijnde sector, departement, Rijksomgeving of externe omgeving. De identiteiten en attributen van derden worden geleverd door externe identiteitenleveranciers zoals eHerkenning en DigiD, eID of een eigen federatieve service.

5.1 Principes en standaarden

Uit de ontvangen informatie en richtlijnen van de Rijksoverheid en het Ministerie van Veiligheid en Justitie zijn de volgende standaarden en principes van toepassing.

Standaarden:
- BIR-2012
- Doelarchitectuur Toegang definitief van 2012 en concept van 2015

Beleidsrichtlijnen:
- Private keys van PKIo-certificaten welke gebruikt worden voor transport moeten worden afgestaan aan ASP4all ten behoeve van Deep Packet Inspection (DPI).

Principes:
- Er worden drie gebruikerstypen onderscheiden: VenJ-medewerkers, Rijksmedewerkers en Derden.
- Gebruikerstypen hebben verschillende betrouwbaarheidsniveaus.
- Een gebruiker heeft maar één identiteit voor de VenJ federatieve dienst.
- Een identiteit wordt primair geleverd door IdP binnen het eigen departement of de eigen sector.
- Gekoppelde applicatie op de federatie delegeert haar authenticatie naar de authenticatievoorziening.
- Attributen komen in drie soorten voor: primair, secundair en tertiaire.
- Attribuutprovider is een voorziening in combinatie van de IdP.
- Authenticatiemiddelen zijn aanvullend op de federatieve voorziening.
- De VenJ federatieve dienst maakt gebruik van SAML2.0.
- Deelnemers aan de federatie verplichten zich aan de aansluitvoorwaarden te houden.
- De applicatie-aanbieder bepaalt het gewenste niveau van authenticatie.

5.2 Authenticatiescenario's

Om de wensen en eisen voortkomend uit het Programma van Eisen en de Functionele Specificaties te vertalen naar techniek, hebben we de onderkende authenticatie scenario's, impliciet voortkomend uit bovengenoemde documenten, als vertrekpunt genomen voor de technische beschrijving van de gewenste situatie. Als we al deze situaties in ogenschouw nemen zijn er dertien potentiële authenticatiescenario's mogelijk. Zie tabel 1.

#	Gebruiker Type	Identiteiten-leverancier (IdP)	Werkomgeving (Client)	Applicatieomgeving (SP)	Dienst versie
1	VenJ-medewerker	Sector	Sector	Eigen departement	1.0
2	VenJ-medewerker	Sector	Sector	Eigen sector	2.0
3	VenJ-medewerker	Sector	Sector	Ander departement	2.0
4	VenJ-medewerker	Sector	Sector	Andere sector	2.0
5	VenJ-medewerker	Sector	Sector	Rijksomgeving	1.0
6	VenJ-medewerker	Sector	Sector	Extern	2.0
7	VenJ-medewerker	Sector	Extern	Extern	2.0
8	Rijksmedewerker	Sector	Extern	Extern	2.0
9	Rijksmedewerker	Sector	Sector	Departement (VenJ)	2.0
10	Rijksmedewerker	Sector	Sector	Sector (VenJ)	2.0
11	Rijksmedewerker	Sector	Sector	Extern	2.0
12	Derden	Extern	Extern	Departement (VenJ)	2.0
13	Derden	Extern	Extern	Sector (VenJ)	1.0
14	Derden	Extern	Extern	Extern	2.0

Tabel 2: Authenticatiescenario's

Authenticatiescenario's #1, #5 en #13 worden niet verder besproken omdat deze scenario's onderdeel zijn van de bestaande VenJ Federatieve Dienst.

Scenario #2: Een VenJ-medewerker wenst toegang tot een applicatie van de eigen sector. Voor dit authenticatiescenario zijn de volgende stappen op hoofdlijnen nodig:

- De VenJ-medewerker gaat naar de applicatie bij de eigen sector en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de VenJ-medewerker toegang tot de interne sectorale applicatie.

Scenario #3: Een VenJ-medewerker wenst toegang tot een applicatie bij een ander departement. Voor dit authenticatiescenario zijn de volgende stappen op hoofdlijnen nodig:

- De VenJ-medewerker gaat naar de applicatie bij het andere departement en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de VenJ-medewerker toegang tot de interne departementale applicatie.

Scenario #4: Een VenJ-medewerker wenst toegang tot een applicatie bij een andere sector. Voor dit authenticatiescenario zijn de volgende stappen op hoofdlijnen nodig:

- De VenJ-medewerker gaat naar de applicatie bij de andere sector en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de VenJ-medewerker toegang tot de interne VenJ-applicatie.

Scenario #6: Een VenJ-medewerker wenst toegang tot een externe applicatie buiten de Rijksoverheid. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De VenJ-medewerker gaat naar de externe applicatie en vraagt toegang
- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de VenJ-medewerker toegang tot de externe VenJ-applicatie.

Scenario #7: Een VenJ-medewerker wenst vanaf internet toegang tot een externe VenJ-applicatie buiten de Rijksoverheid. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De VenJ-medewerker gaat naar de externe applicatie van VenJ en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de VenJ-medewerker toegang tot de VenJ-applicatie.

Scenario #8: Een Rijksmedewerker wenst vanaf internet toegang tot een externe VenJ-applicatie buiten de Rijksoverheid. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De Rijksmedewerker gaat naar de externe applicatie van VenJ en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;

- Na een succesvolle authenticatie krijgt de Rijksmedewerker toegang tot de VenJ-applicatie

Scenario #9: Een Rijksmedewerker wenst toegang tot een VenJ-applicatie. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De Rijksmedewerker gaat naar de interne applicatie van VenJ en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de Rijksmedewerker toegang tot de VenJ-applicatie.

Scenario #10: Een Rijksmedewerker wenst toegang tot een applicatie bij een VenJ-sector. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De Rijksmedewerker gaat naar de interne applicatie van de VenJ-sector en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de Rijksmedewerker toegang tot de interne VenJ-applicatie.

Scenario #11: Een Rijksmedewerker wenst toegang tot een externe VenJ-applicatie. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De Rijksmedewerker gaat naar de externe VenJ-applicatie en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de Rijksmedewerker toegang tot de externe VenJ-applicatie.

Scenario #11: Een Rijksmedewerker wenst vanaf internet toegang tot een externe VenJ-applicatie buiten de Rijksoverheid. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De Rijksmedewerker gaat naar de externe applicatie van VenJ en vraagt toegang;

- De applicatie verwijst door naar de Identity Provider van het rijksbrede koppelvlak;
- De gebruiker kiest van welk departement hij afkomstig is en wordt doorverwezen naar de Identity Provider van het eigen departement;
- De gebruiker kiest van welke sector hij afkomstig is en wordt doorverwezen naar de Identity Provider van de eigen sector;
- Na een succesvolle authenticatie krijgt de Rijksmedewerker toegang tot de VenJ-applicatie

Scenario #12: Een derde wenst vanaf internet toegang tot een interne VenJ-applicatie. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De derde gaat via het reguliere toegangskoppelvlak naar de interne departementale VenJ-applicatie en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het externe koppelvlak;
- De gebruiker kiest een authenticatiemethode en wordt doorverwezen naar de betreffende Identity Provider;
- Na een succesvolle authenticatie krijgt de derde toegang tot de interne applicatie.

Scenario #14: Een derde wenst vanaf internet toegang tot een externe VenJ-applicatie. Voor dit authenticatie scenario zijn de volgende stappen op hoofdlijnen nodig:

- De derde gaat naar de externe VenJ-applicatie en vraagt toegang;
- De applicatie verwijst door naar de Identity Provider van het externe koppelvlak;
- De gebruiker kiest een authenticatiemethode en wordt doorverwezen naar de betreffende Identity Provider;
- Na een succesvolle authenticatie krijgt de derde toegang tot de interne applicatie.

5.3 Hergebruik

Voor de huidige VenJ Federatieve Dienst is NetIQ Access Manager en het opensource SimpleSAMLphp ingezet. SimpleSAMLphp wordt bijzonder succesvol gebruikt door SurfNet voor hun SurfConext/OpenConext dienst. SSC-ICT richt met SimpleSAMLphp een hosted IdP-dienst in voor verschillende VenJ-onderdelen.

Binnen VenJ wordt ook gebruikt gemaakt van een IdP-Proxy opzet. Deze heeft primair de functie van het doorsturen van SAML authenticatieverzoeken naar andere IdP's. Het is een doorgeefluik voor SAML verkeer. Voor de huidige bestaande IdP-Proxy wordt door SSC-ICT technologie in gezet op basis van NetIQ Access Manager.

Daarnaast maakt de VenJ Federatieve Dienst van een Access Gateway. De Access Gateway ontsluit applicaties naar eindgebruikers en bevat een aantal belangrijke functies zoals reverse proxying en protocoltranslatie van en naar SAML 2.0. SSC-ICT heeft een succesvolle PoC uitgevoerd om deze functionaliteit in te laten vullen door bijvoorbeeld Netscalers van Citrix of F5, dicht bij de applicatie.

6. Impactanalyse governance

Binnen de rijksoverheid zijn diverse ontwikkelingen waarneembaar in het verbeteren van het digitale contact en de dienstverlening met het Rijk; ICT-voorzieningen dienen toegankelijker te worden gemaakt voor partijen die organisatie-overschrijdend samenwerken in verschillende netwerken en keteninformatisering; Rijksmedewerkers moeten (vanuit oogpunt Het Nieuwe Werken) kunnen bepalen waar, hoe en wanneer zij werken en gebruik kunnen maken van ICT-voorzieningen.

De huidige VenJ Federatieve Dienst is echter ontwikkeld volgens een gesloten organisatiemodel en gesloten netwerkinfrastructuur (Rijksweb-VPN). De dienst dient daarom op basis van gestelde behoeftes, maar ook vanwege de huidige situatie en de beperkingen die dat met zich meebrengt, doorontwikkeld te worden. Hierbij dient te worden afgestapt van het zogenaamde "gesloten karakter" zonder dat dit een groot afbreukrisico vormt op het gebruiksgemak, de dienstverlening en (vertrouwelijke) informatie.

Wanneer de VenJ Federatieve Dienst echter niet wordt doorontwikkeld (0-optie) vergroot dit de kans op een verdere groei aan suboptimale oplossingen van VenJ-sectoren, hogere kosten, onbeheersbare situaties met een verminderde controle op rechtmatige en veilige toegang tot vertrouwelijke informatie.

6.1 Huidige situatie

De VenJ Federatieve Dienst is een gesloten dienst waarbij SSC-ICT als technisch beheerder in de praktijk alleen generieke oplossingen aanbiedt aan de partijen (sectoren) die zijn aangesloten. De VenJ Federatieve Dienst is als oplossing opgenomen in de Producten- en Dienstencatalogus. Naast deze dienstbeschrijving wordt ook verwezen naar aansluitvoorwaarden, deze zijn echter niet terug te vinden.

Openingstijden	10x5 (Op werkdagen van 07:30 tot 17:30 uur) er is geen ondersteuning bij incidenten buiten de openingstijden*
Productie-window	24x7 uitgezonderd onderhoudsuren is de dienst beschikbaar
Onderhouds-window	Gepland onderhoud na 21:00 uur met uitzondering van minor releases die om 18:00 uur starten
Backup-window	Volgens PDC
Beschikbaarheid	98% gedurende openingstijden

*) Voor de openingstijden is een addendum opgesteld voor 24x7 dienstverlening.

6.2 Gewenste situatie

Met de wens om extern te federeren en intern ook specifieke applicaties federatief te kunnen ontsluiten wordt een impact gecreëerd op de governance. Op basis van uitgangspunten, triggers en actoren is een Governance referentiemodel opgesteld uitgaande van de bestaande situatie. De impact is hierbij vanuit de dienst bepaald en niet alleen voor wat betreft SSC ICT.

Vanuit het Pakket van Eisen zijn de belangrijkste triggers van de doorontwikkeling geïnventariseerd. Deze triggers initiëren aanpassingen in het bestaande Governance-model. De belangrijkste triggers zijn:

- Externe & Interne partijen kunnen toegang krijgen tot applicaties die zich bevinden in zowel de Secure Zone, DMZ / Extranet.
- Beheermatige complexiteit neemt toe met het aantal partijen
- Externe partijen worden gezien als onvertrouwde partijen
- Externe partijen zijn niet onderhevig aan security beheerkaders als BIR2012
- Samenwerking tussen Departementen en SSC ICT in rol van IdP én SP én generieke infrastructurele diensten vragen om ketenregie in geval van incidenten, problems en changes
- Niet alle applicaties zijn SAML 2.0 aware.
- Het VenJ-breed inrichten van een federatieve dienstverlening vereist standaardisatie op Identity management en het gebruik van attributen. Met name Identity management kent meerdere implementaties en is daarmee suboptimaal.

Binnen de VenJ Federatieve Dienst zijn de navolgende actoren onderkend die een rol binnen de doorontwikkeling van de Governance spelen. De actoren betreffen:

• Systeemeigenaar	DI&I
• Functioneel- en tactisch beheerder	JustID
• Technisch beheerder	SSC-ICT en JustID
• Identity provider (IdP)	Potentieel alle VenJ-sectoren
• Service Provider (SP)	
• Gebruiker	

Om de impact van de gewenste veranderingen ten aanzien van de doorontwikkeling te bepalen zijn er de navolgende uitgangspunten c.q. afspraken onderkend:

- Aanvragen voor het aanbieden en afnemen van diensten via de VenJ Federatieve Dienst worden beoordeeld door de functioneel beheerder die, indien akkoord, de technische beheerder een opdracht geeft voor realisatie en eventuele projectmatige implementatie en/of ondersteuning.
- Afstemming over aansluitvoorwaarden; (gegevens en attributen) standaarden, processen, beveiligingsmaatregelen, tussen Idp's, SP's en afnemers vallen onder de verantwoordelijkheid van de functioneel beheerder.
- Een collectieve schaalgrootte, eenduidig beheerde infrastructurele voorzieningen in combinatie met standaardisatie bepalen in belangrijke mate het succes van de dienst.

- Flexibiliteit ten aanzien van implementatie (korte- en lange termijn maar ook ad hoc dient mogelijk te zijn).
- Planning van het realiseren, prioriteren en de kosten van nieuwe koppelingen ligt bij de functioneel beheerder.
- SSC-ICT is een infrastructurele dienstverlener van een generieke dienst.
- De doorontwikkeling betreft een federatieve infrastructurele dienst die volgens gangbare (BIR-)normen wordt opgebouwd en beheerd.
- Gericht op één gezamenlijk extern (Onvertrouwd/Semi-vertrouwd/Vertrouwd) koppelvlak voor federatieve ontsluiting, beschikbaar voor alle aangesloten partijen. Op de grenzen zullen maatregelen worden genomen.
- De VenJ federatieve dienst heeft een verhoogde beschikbaarheid, kent uitwijk en is 24x7 beschikbaar voor gebruik en onderhoud.
- Sectoren zijn en blijven autonoom ten aanzien van hun federatieve Dienstverlening.
- Informatie-eigenaar (SP) is verantwoordelijk voor het aanbieden van zijn oplossing aan federatieve partijen. Daarmee verantwoordelijk voor de specifieke security (hardening), autorisatie tot de applicatie, goedkeuring van autorisatiemiddelen én toegang tot hun oplossing.

6.3 Referentiemodel Governance

Op basis van de eisen in het Pakket van Eisen, uitgangspunten, triggers en actoren is het Referentiemodel Governance opgesteld en als bijlage 2 bijgesloten. Hierbij is de basis de bestaande SSOn Rijks dienst. In het algemeen kan gesteld worden dat met de gewenste veranderingen de volledig dienst op een hoger plan moet gaan komen.

JustID als functioneel beheerder zal vraag en aanbod bij elkaar brengen. Dat werd voorheen door DI&I gedaan, maar JustID zal meer als kadersteller gaan optreden voor de specifieke diensten die federatief ontsloten dienen te gaan worden. Hierbij spelen zaken als het vertrouwd maken van de nu overtrouwde partijen (sluiten van convenanten), borgen van standaardisatie, stellen van prioriteiten, bewaken van de kwaliteit en borgen dat toegezegde veranderingen ook daadwerkelijk als een "verbeterplan" binnen de gestelde termijnen worden doorgevoerd.

Voor SSC-ICT zal er voor wat betreft het technische beheer, naar verwachting niet veel veranderen. Het koppelvlak wordt meer complex in de zin dat op het interne koppelvlak ook Service Providers geïntroduceerd worden. Hiermee heeft SSC-ICT ruime ervaring. Op termijn zullen de beide vestigingen van SSC nauwer en intensiever gaan samenwerken. Verder zullen er meerdere partijen en meerdere gebruikers gebruik gaan maken van de dienst. Hierdoor wordt het incident en change management complexer (de beheerketen wordt langer en het aantal partijen neemt toe). Onder druk van de snelle technologische ontwikkelingen op het gebied van federatie, en naar verwachting ook een diversiteit van federatieve implementaties, zal ook de noodzaak tot actief problem management toenemen. Ervaring bij SSC-ICT heeft geleerd dat het onderhouden van de dienst voor de gebruikers steeds vaker minder goed uitkomt.

De huidige dienst is hoog redundant, waardoor delen van de oplossingen eenvoudig buiten gebruik kunnen worden gezet (met behulp van load balancers) om changes door te voeren en te valideren op goede werking. Om de changes optimaal te kunnen voorbereiden is het noodzakelijk om een testomgeving op te bouwen naast de reeds bestaande acceptatie- en productieomgeving.

Boven op de infrastructurele dienst ontwikkelt zich ook de noodzaak tot het ontwikkelen van implementatiediensten op het gebied van federatieve ontsluiting. Niet alleen is de technische kennis rondom federatie beperkt beschikbaar, ook neemt de noodzaak toe om expertise op te bouwen en te behouden voor derdelijns support, standaardisatie op techniek en implementatie. Al hoewel de sectoren autonoom zijn ten aanzien van de VenJ Federatieve Dienst kan SSC-ICT ondersteuning bij de implementatie aanbieden aan specifieke partijen. Met name het ondersteunen van Service Providers (SP's) stelt hoge eisen aan expertise die vaak niet voldoende bij de Service Provider, applicatieleverancier of de sector aanwezig is.

Risico: Binnen het complexe werkgebied van federation heeft de Service Provider de centrale sleutel rol. Hij beslist over het wel/niet delen van informatie, opleggen van aanvullende security maatregelen wanneer informatie te gevoelig is, opstellen van aanvullende overeenkomsten, beheren van business case, etc.. Kortom, de belangrijkste rol is de rol van de Service Provider, echter is er te weinig kennis en expertise aanwezig, en is de gemiddelde Service Provider niet klaar voor het invullen van deze rol. Traditioneel is de leverancier van de applicatie de rechterhand van de informatie-eigenaar. SSC-ICT Haaglanden zou, als rijksbrede dienstverlener, deze rol kunnen vervullen.

6.4 Governance producten

Voor de doorontwikkeling van de VenJ Federatieve Dienst dienen de navolgende producten aangepast dan wel ontwikkeld te worden:

- Beleidsnotitie ter ondersteuning van federatieve ontsluiting waarbij het credo "vertouwen eerst controle later" uitgedragen wordt.
- Update PDC met dienstbeschrijving VenJ Federatieve Dienst 2.0
- Juridisch normenkader VenJ Federatieve Dienst 2.0
- Raamovereenkomst dienstverlening
- Aansluitvoorwaarden
- Change management
- Problem management
- Architectuur, Technisch Ontwerp, Functioneel Ontwerp
- Installatiehandleidingen
- Servicedesk referentiekaart
- Klant-specifieke afspraken rondom dienstverlening, afgestemd en vastgelegd in een DAP

Bij het (door)ontwikkelen van deze producten kunnen aanzienlijke besparingen gerealiseerd worden door hergebruik. Met name binnen SurfNet is er ruime en praktische ervaring met federatieve dienstverlening in al zijn facetten.

6.5 Exploitatie

De huidige exploitatie van de VenJ Federatieve Dienst dient te gaan veranderen conform het Pakket van Eisen. De dienst en ook de betrokken rollen dienen te veranderen en naar een hoger niveau getild te worden. Een hoger niveau vereist veelal investeringen en ook hogere beheerkosten. De verwachting is dat federeren aanzienlijke besparingen zal gaan leveren. De zijn hierbij vaak decentraal terwijl de kosten centraal worden gerealiseerd. De VenJ Federatieve Dienst is daarmee een enabler en kent een brede werking (generieke dienst). De impact op de exploitatie als gevolg van de doorontwikkeling is in termen van technisch beheer vergelijkbaar aan die van de huidige dienst. Daarbij zijn er op dit moment een aantal ontwikkelingen binnen SSC-ICT gaande waardoor we niet specifieker in kunnen gaan op de gevraagde impact op de exploitatie van de doorontwikkeling. De belangrijkste ontwikkeling is dat SSC-ICT aan een nieuw kostprijs model werkt.

Voorgesteld wordt om gedurende de definitie- en realisatiefase inzicht te geven in de exploitatie. De exploitatie van de dienst zal bewaakt en jaarlijks geëvalueerd worden.

De aanvullende dienstverlening voor de "Federatieve implementatiediensten" zal projectmatig worden begroot en worden gerealiseerd. Dit team zal ook 3de lijns support op zich nemen.

7. Impactanalyse informatiebeveiliging

Onderdeel van de opdracht was ook om een impactanalyse op te stellenop het gebied van informatiebeveiliging. Om dit goed uit te kunnen voeren is het van belang om de scope van de analyse te bepalen. De scope is de VenJ Federatieve Dienst waarbij de volgende stelling uit de BIR 2012 van groot belang is:

> *11.5.2. Gebruikersidentificatie en –authenticatie*
> *Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.*

Invulling van de bovenstaande stelling betekent dat de authenticatiedienst vertrouwt op het vaststellen van de identiteiten. Om dit meetbaar te maken is één van de voorwaarden dat het vaststellen van de identiteiten voldoet aan de aansluitvoorwaarden. De aansluitvoorwaarden zijn in dit geval een gemeenschappelijk overeen gekomen kader welke door alle partijen gedragen wordt.

Bij het opstellen van deze impactanalyse voor de VenJ Federatieve Dienst dienen de volgende punten beantwoord te worden:

- Welk dreigingsniveau is van toepassing?
- Welke eisen worden gesteld aan de betrouwbaarheid (Confidentiality, Integrity & Availability)?
- Welke WBP-regelgeving is van toepassing?
- Hoe wordt invulling gegeven aan de BIR-2012?
- Is het een kritische voorziening voor VenJ, gekoppeld aan Te Beschermen Belangen (TBB)?
- Hoe wordt de dienst getest op basis van penetratietests?

7.1 Dreigingsniveau

De opdrachtgever heeft aangegeven dat het dreigingsprofiel DEP-V is. Dit betekent concreet dat er boven op de BIR extra maatregelen genomen moeten worden. Aangezien de authenticatiedienst al beveiligd is, is de enige maatregel die toegevoegd dient te worden om het niveau van DEP-V te bereiken de monitoringfunctie. De monitoringfunctie wordt ingevuld door het SOC, waarbij logging en SIEM-tooling de hoofdrol spelen. Het SOC gaat pro-actief aanvallen detecteren met behulp van de SIEM-tooling en achteraf aanvallen analyseren aan de hand van secure logging tooling.

7.2 Betrouwbaarheid

De betrouwbaarheid is opgebouwd uit beschikbaarheid, vertrouwelijkheid en integriteit. Als we dit verder analyseren dan komen we tot het volgende:

- Beschikbaarheid: de authenticatieoplossing gaat gebruikt worden voor applicaties die aangeboden worden binnen en buiten het Rijk. Tevens zullen bepaalde applicaties 7 dagen per week, 24 uur per dag beschikbaar moeten zijn. Dit betekent dat er een dienstverlening van 24x7 uur wordt verwacht. Het uitvallen van de dienst zal een negatieve impact hebben op het imago

van SSC-ICT, wanneer gebruikers niet meer kunnen inloggen op diverse applicaties.
- Vertrouwelijkheid: om ervoor te zorgen dat alleen de geautoriseerde IdP's gebruik kunnen maken van deze voorziening dient de vertrouwelijkheid van de authenticatieservice gewaarborgd te worden. Om dit te realiseren worden alleen geautoriseerde partijen toegevoegd en worden verbindingen versleuteld. Daarnaast kan de inhoud van het token informatie bevatten die hogere eisen stelt aan de vertrouwelijkheid van een attribuut. In die gevallen kan het attribuut versleuteld worden.
- Integriteit: om ervoor te zorgen dat de inhoud van het token niet aangepast kan worden is het verstandig om de inhoud van het token te ondertekenen, zodat de integriteit van het token gehandhaafd kan worden.

7.3 Wet bescherming persoonsgegevens

Binnen de VenJ federatieve dienst worden privacy-gerelateerde zaken verzonden in het SAML token. Omdat het om persoonsgegevens gaat, strekt het de aanbeveling een Privacy Impact Assessment (PIA) uit te voeren. In verband met het gebruik van privacygegevens is instemming van de OR noodzakelijk. Tevens levert de PIA input voor de beveiligingseisen die van toepassing zijn op de VenJ Federatieve Dienst. De beveiligingseisen uit de PIA dienen door de opdrachtgever en het project vertaald te worden naar maatregelen. Belangrijk is in deze dat we te maken hebben met meerdere sectoren en dat de instemming van de OR's voor alle sectoren doorlopen dient te worden.

7.4 BIR-compliancy

De hele VenJ Federatieve Dienst dient te voldoen aan de BIR. Dit betekent dat er een risicoanalyse door de opdrachtgever uitgevoerd moet worden. De resultaten van de risicoanalyse zijn input voor het project. Het project zal de resultaten van de risicoanalyse gebruiken om te bepalen welke BIR-maatregelen van toepassing zijn. Daarnaast zal het project een technische risicoanalyse uitvoeren zodat duidelijk wordt welke technische risico's niet afgedekt worden door de standaard BIR-maatregelen.

Fysieke beveiliging	Fysieke beveiliging is vaak belegd bij Facility Management of bewakingsdiensten. Zij zijn verantwoordelijk voor de beveiliging van percelen, panden en ruimtes.
ICT-diensten en ICT-infrastructuren	De ICT-diensten en -infrastructuren zijn ondersteunend aan bijna alle processen. De eisen die aan ICT-voorzieningen gesteld worden, zijn hierdoor zeer ingrijpend en bepalen voor een significant deel de inrichting van het ICT-landschap.
Applicatie-eigenaren en systeemeigenaren	Applicatie-eigenaren en systeemeigenaren zijn verantwoordelijk voor de veilige en correcte verwerking van de relevante data binnen de applicatie. Een belangrijk onderdeel van informatiebeveiliging vormen de eindgebruikers. Zij dienen kennis te hebben van de gevolgen van hun gedrag op beveiliging.

7.5 Kritisch systeem gekoppeld aan TBB's

De verwachting is dat de VenJ Federatieve Dienst wordt aangemerkt als kritische voorziening, omdat deze onder de generieke basisvoorzieningen valt. Dit betekent dat de voorziening onder de TBB's valt en dat jaarlijks over de BIR-compliancy gerapporteerd moet worden.

7.6 Penetratietests

Om decharge van het project door de opdrachtgever te bespoedigen is het van belang dat aangetoond wordt dat de applicatie veilig is. Dit wordt aangetoond door middel van de security acceptatie criteria en een penetratietest. Tijdens de penetratietest, door een gerenommeerde partij, wordt de applicatie binnenstebuiten gekeerd en de resultaten worden gebruikt om een oordeel te geven over de veiligheid van de voorziening. Een positief oordeel kan worden gebruikt om aan te tonen dat de voorziening veilig is.

7.7 Koppelvlakken

Op de overgangen naar de verschillende componenten (koppelvlakken) worden eisen gesteld. Deze eisen zijn aansluitvoorwaarden om gebruik te maken van de VenJ Federatieve Dienst. De aansluitvoorwaarden zijn de gemeenschappelijke basis waarop men elkaar kan vertrouwen. Het is daarom verstandig om jaarlijks een verklaring op te vragen waarin men aangeeft aan de aansluitvoorwaarden te voldoen.

Bijlagen

De volgende bijlagen maken deel uit van de definitiestudie - Doorontwikkeling Federatieve Service:

- Bijlage 1: Beantwoording Pakket van Eisen
- Bijlage 2: Referentiemodel Governance
- Bijlage 3: Begroting doorontwikkeling VenJ Federatieve Service

Bijlage 1 – Beantwoording Pakket van Eisen

Revisie

Document:
Doorontwikkeling VenJ Federatieve Dienst - Pakket Van Eisen

Inleiding:
Overzicht van de functionele en non-functionele specificaties voor de doorontwikkeling van de VenJ Federatieve Dienst

Versie:	Datum:	Auteur:	Organisatie:	Wijzigiging:	Akkoord:
0.1	25-jul-15	D. Appelboom	DI&I	Initiele versie Gebaseerd op input/review SSOn workshops door BD, CJIB, DJI, IND, RvdK en SSC-ICT	
1.0	01-aug-15	D. Appelboom	DI&I	N.a.v. review #1 DI&I	

(NON)FUNCTIONAL REQUIREMENTS - ONTWIKKELPUNTEN VenJ Federatieve Dienst

Nr:	Prio:	T/F:	Release	MoSCoW	Vraag
DO-001	H	F	Minor	Sh	Richt Life cyclemanagement in.
DO-002	H	T	Major	M	Uitbreiden van HomeRealmDiscovery voor het aansluiten van ZBO's, uitvoeringsorganisaties van kerndepartement
DO-003	H	T	Major	M	Ontsluiten van internettoegang en afschermen van eindgebruikers naar de onvertrouwde buitenwereld (o.a. internet).
DO-004	H	T	Major	M	Ondersteuning van het authenticatiemechanisme voor security level Dep-V.
DO-005	H	T	Major	M	Gebruik van SSOn met mobiele devices en mobiele apps.
DO-006	L	T	Major	M	Ontsluiting van buiten het rijk (via internet) van toeleveranciers, niet rijksambtenaren.

Let op: De hier beschreven ontwikkelpunten vormen de basis voor de Doorontwikkeling VenJ Federatieve Dienst, en komen voort uit de diverse behoeftes zoals die door de verschillende sectoren zijn ingediend.
Ter referentie van de functionele eisen en/of wensen is eventueel het betreffende ontwikkelpunt toegekend.

(NON)FUNCTIONAL REQUIREMENTS - ALGEMEEN												
				Use Cases						ICT Beheerder	
#	Omschrijving	F/N	Ontwikkelpunt	BD	CJIB	DJI	IND	RVDK	EIS/WENS	Comply	Explain
REQ-ALG-001	VenJ verstrekt als 'broker' toegang tot interne en externe Identity Providers en Service Providers aan Rijksmedewerkers, particulieren, bedrijven en ketenpartners, kennis/opleidingsinstituten met wie het rijk samenwerkt. Toegang tot de ICT voorziening wordt ingesteld met policies. De IdP dient op basis van authenticatie (ID en bijbehorende attributen) het benodigde SAML-token te vervaardigen voor de Sevice Providers.	N	DO-003 DO-006	X	X	X	X	X	EIS	JA	
REQ-ALG-002	In relatie tot REQ-ALG-001 moet toegang ook mogelijk zijn buiten het overheidsdomein (voor aangesloten IdP/SP)	N	DO-003 DO-006	X	X	X	X		EIS	JA	
REQ-ALG-003	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst die gehost wordt buiten het Rijk (en dus buiten Rijksweb-VPN/Rijkscloud).	F	DO-003			X			EIS	JA	
REQ-ALG-004	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt gehost bij een externe dienstverlener (als extensie van het Rijksweb-VPN/Rijkscloud)	F			X				EIS	JA	
REQ-ALG-005	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een departement.	F		X					EIS	JA	
REQ-ALG-006	Rijksmedewerker krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een (gefedereerd) departement, maar wordt gehost bij een externe dienstverlener (als extensie van het domein van het (gefedereerde) departement).	F		X	X				EIS	JA	
REQ-ALG-007	Rijksmedewerker krijgt vanuit een digitale 'untrusted' omgeving (internet) met zijn mobiele device toegang tot een informatiedienst, die wordt gehost in Rijksweb-VPN/rijkscloud.	F	DO-003	Bestandenpostbus		OMS			EIS	JA	
REQ-ALG-008	Een "derde" krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt gehost in Rijksweb-VPN/Rijkscloud. *Een derde kan zijn een gebruiker van een ketenpartner, lagere overheid, onderzoeksinstituut, sourcing partij, leverancier, student, externe gebruiker (niet van de eerder genoemde organisaties) of burger/bedrijf (via e-EID), etc.*	F	DO-006		X			e-SWF	EIS	JA	
REQ-ALG-009	Een "derde" krijgt vanuit zijn digitale werkomgeving toegang tot een informatiedienst, die wordt geleverd door een departement. *Een derde kan zijn een gebruiker van een ketenpartner, lagere overheid, onderzoeksinstituut, sourcing partij, leverancier, student, externe gebruiker (niet van de eerder genoemde organisaties) of burger/bedrijf (via e-EID), etc.*	F	DO-006	VenJ transactiemodule	X				EIS	JA	
REQ-ALG-010	Een "derde" krijgt vanuit een digitale 'untrusted' omgeving (internet) met zijn mobiele device toegang tot een informatiedienst, die wordt gehost in rijksweb-VPN/rijkscloud. *Een derde kan zijn een gebruiker van een ketenpartner, lagere overheid, onderzoeksinstituut, sourcing partij, leverancier, student, externe gebruiker (niet van de eerder genoemde organisaties) of burger/bedrijf (via e-EID), etc.*	F	DO-006	VenJ transactiemodule	X			e-SWF	EIS	JA	

(NON) FUNCTIONAL REQUIREMENTS - PROCES												
				Use Cases						ICT Beheerder		
#	Omschrijving	F/N	Ontwikkelpunt	BD	CJIB	DJI	IND	RVDK	EIS/WENS	Comply	Explain	
REQ-PRC-001	Maakt gebruik van Audit Based Access Control; toegang tot informatie gebeurt als de persoon over de juiste attributen/claims beschikt, maar het draait vooral om achteraf afleggen van controle en verantwoording.	N		X	X	X	X	X	EIS		NEE, Audit Based Access Control is een nieuw concept buiten federation om waarvoor de spelregels nog niet duidelijk zijn. Om te komen tot een ABAC-voorziening zal eerst onderzoek moeten plaatsvinden rondom de technische en niet-technische zaken zoals processen. Deze requirement is daarom buiten scope geplaatst.	
REQ-PRC-002	Moet via het proces Life cyclemanagement worden onderhouden. *Er is nog geen functioneel beheer op de VenJ Federatieve dienst, alleen technisch, lijst opstellen met gewenste updates op onderdelen.*	N	DO-001	X	X	X	X	X	EIS	JA		
REQ-PRC-003	Heeft een koppeling met het (de)provisioning proces. Met "provisioning" wordt hier niet alleen gedoeld op "het aanmaken van het ICT-account", maar hieronder valt ook het beheren van de attributen bij het ICT-account gedurende de levenscyclus van het account tot en met het buiten werking stellen van het account op het moment dat de persoon geen werkrelatie meer heeft met de Rijksoverheid en daardoor ook geen toegang mag hebben tot de aangesloten ICT-voorzieningen.	N		X	X	X	X	X	EIS	JA		
REQ-PRC-004	Sessie parameters: Opzetten van de eerste authenticatieoverdracht is de maximale wachttijd: 2-8 seconden Maximum sessieduur: 8 uur Maximum sessie idle time: 60 minuten Maximaal aantal concurrent sessies per gebruiker: 2 Instandhouding van een sessie (waarbij doorgaans ook authenticatieoverdracht plaatsvindt) is niet merkbaar voor de eindgebruiker	N		X	X	X	X	X	EIS	JA, configureerbaar in SimpleSAMLphp		
REQ-PRC-005	Applicatiespecifieke sessies worden geïnvalideerd door de ICT-voorziening zelf.	N		X	X	X	X	X	EIS	JA		
REQ-PRC-006	Ondersteunt het (tijdelijk) ongedaan maken van een reeds uitgevoerde authenticatie (logoff) teneinde inloggen op meervoudige dienstverbanden/werkrelaties te ondersteunen.	N		X	X	X	X	X	EIS	JA		
REQ-PRC-007	Is geschaald zodat wordt voldaan aan het aantal concurrent login request op de piekmomenten.	N		X	X	X	X	X	EIS	JA		
REQ-PRC-008	Indien niet voldaan blijft worden aan de aansluitvoorwaarden (compliancy), kan de IdP en/of SP worden afgesloten voor de dienstverlening.	N		X	X	X	X	X	EIS	JA		
REQ-PRC-009	Borgen en monitoren dat aanbiedende leveranciers (IdP en/of SP) voldoen aan afgesproken aansluitvoorwaarden. Juridische dienstverleningsovereenkomsten (contracten) afsluiten tussen aansluitende partijen, en het proces regelmatig auditen in opzet, bestaan en werking.	N		X	X	X	X	X	EIS	JA		

(NON) FUNCTIONAL REQUIREMENTS - ORGANISATIE												
				Use Cases						ICT Beheerder	
#	Omschrijving	F/N	Ontwikkelpunt	BD	CJIB	DJI	IND	RVDK	EIS/WENS	Comply	Explain
REQ-ORG-001	Regel de omgang van 'onzichtbaren' in de keten (vertrouwelijke identiteiten).	N	DO-004	X	X	X	X	X	EIS	JA, zie REQ-TNK-012	
REQ-ORG-002	Het is alleen mogelijk om persoonsgebonden accounts te gebruiken.	F		X	X	X	X	X	EIS	JA	
REQ-ORG-003	Een gebruiker kan op basis van zijn claim; identiteit, rol en eigenschappen/werkrelatie de juiste ingang/autorisatieniveau in de ICT-voorziening toebedeeld krijgen.	F		X	X	X	X	X	EIS	JA	

(NON) FUNCTIONAL REQUIREMENTS - TECHNIEK

#	Omschrijving	F/N	Ontwikkelpunt	Use Cases					EIS/WENS	ICT Beheerder	
				BD	CJIB	DJI	IND	RVDK		Comply	Explain
REQ-TNK-001	Dient zowel “rich client”, mobile devices en het gebruik van webbrowser en (mobile) applicaties te ondersteunen.	N	DO-005	X	X	X	X		EIS	JA	
REQ-TNK-002	Dient ook externe federatie te ondersteunen buiten het overheidsdomein (zie tevens REQ-ALG-002). ***.rijksweb.nl** zone voldoet alleen voor interne ICT-voorzieningen, en biedt met deze eis de mogelijkheid om diensten buiten rijksweb dns te kunnen ontsluiten.	F	DO-003 DO-006		X	X	X	X	EIS	JA	
REQ-TNK-003	Gebruik van 2-way trust tussen de centrale IdP/SP en decentrale SP/IDP's	N		X	X	X	X	X	EIS	JA	
REQ-TNK-004	Binnen het verzorgingsgebied van SSC-ICT moet het mogelijk zijn om achterliggende sectoren van de departementen binnen het verzorgingsgebied van SSC-ICT aan te sluiten.	N	DO-002	X	X	X	X	X	EIS	JA	
REQ-TNK-005	Rapportagemogelijkheid voor aangesloten diensten t.b.v. logging en auditing. Heeft systeemlogging die configurabel moet zijn, en interoperabel kunnen werken met SIEM-oplossingen	N	DO-004	X	X	X	X	X	WENS	JA, wanneer hiervoor een voorziening beschikbaar is	
REQ-TNK-006	Gebruik van SAML-scoping (met IdP whitelist/blacklist functionaliteit) Lijst met aanbod van de Identity Providers die mogen inloggen bij een Service Provider	N		X	X	X	X	X	EIS	JA, mogelijk met SimpleSAMLphp, niet met ADFS	
REQ-TNK-007	Heeft een koppelvlak met het eID-stelsel (e-Herkenning / DigiD), en dient deze te borgen in de keten-infrastructuur	N		X	X	X	X	X	EIS	JA	
REQ-TNK-008	Het gebruik van Kerberos / SPNEGO voor gebruik ICT-voorzieningen dient te worden uitgefaseerd. Voor bestaande ICT-voorzieningen wordt een migratieplan op gesteld (en de migratie daadwerkelijk uitgevoerd) om de ICT-voorziening SAML geschikt te maken.	N		X	X	X	X	X	EIS	JA, mogelijk met inzet van bijv. NetScalers als ADC	
REQ-TNK-009	Het authenticatiebewijs bevat minimaal één attribuut dat de Service Provider in staat stelt deze te relateren aan één of meerdere identiteiten. Autorisatie gebeurt binnen de ICT-voorziening (claim based rules) op basis van relevante attributen.	N		X	X	X	X	X	EIS	JA	
REQ-TNK-010	Kan authenticatiebewijzen (tokens) doorgeven aan service providers (van mobiele apps).	F	DO-005		X				WENS	JA	
REQ-TNK-011	Het Mobile device management platform moet hergebruik van authenticatiebewijzen voor mobile apps faciliteren binnen de geldigheid van het authenticatiebewijs (FOLLOW ME-principe)	N	DO-005		X				WENS	JA	
REQ-TNK-012	Werken met pseudo id's (zodat interne identiteiten niet zichtbaar worden in de onvertrouwde buitenwereld (internet))	F	DO-004	CIOT					EIS	JA	
REQ-TNK-013	Indien gefedereerde ICT-voorzieningen of organisaties van buiten de Haagse ring benaderd moeten kunnen worden, dan is het gebruik van reverse proxy's vereist om de Identity Providers naar buiten toe beschikbaar te maken.	N	DO-003 DO-006	X	X	X	X	X	EIS	JA, mogelijk op basis van hashing zoals door SurfNet toegepast	

(NON) FUNCTIONAL REQUIREMENTS - INFORMATIE & VEILIGHEID												
				Use Cases						ICT Beheerder	
#	Omschrijving	F/N	Ontwikkelpunt	BD	CJIB	DJI	IND	RVDK	EIS/WENS	Comply	Explain
REQ-INF-001	Uitwisseling van authenticatiebewijzen is veilig; - versleuteling volgens SHA256 - spoofing/replay is onmogelijk	N	DO-004	X	X	X	X	X	EIS	JA	
REQ-INF-002	De dienstverlening is BIR-compliant met een minimaal geadviseerd beveiligingsniveau van 2 (voorheen WBP-2). Gegevensclassificatie is tot en met departementaal vertrouwelijk (niet staatsgeheim, tm hoge dreiging) Een SAAM-analyse (in opdracht van DI&I en uitgevoerd door het NBV) maakt onderdeel uit van het doorontwikkeltraject om het geadviseerde beveiligingsniveau 2 aan te tonen.	N	DO-004	X	X	X	X	X	EIS		NEE, Aanvulende beveilingsmaatregelen boven op BIR om dreiging te beperken vallen binnen de verantwoordelijkheid van de informatie-eigenaar. Voorgeschreven maatregelen kunnen waar nodig doorgevoerd worden in opdracht van de informatie-eigenaar. SSC-ICT levert standaard WBP2 en DEP-V (BIR-niveau) voor de infrastructuur. Dit zegt niets over het niveau op applicatiegebied.
REQ-INF-003	Dient ongevoelig te zijn voor DDOS attacks en SQL injections.	N	DO-004	X	X	X	X	X	EIS		NEE, ongevoeligheid voor DDOS is praktisch onmogelijk. Wel zijn er geavanceerde voorzieningen getroffen om de impact te beperken. SQL-injections liggen op het gebied van de applicatie (slechte invoervalidatie of geen gebruik van stored procedures) waarbij er data uit de database wordt getrokken. Wat er gevraagd wordt zijn applicatie-specifieke maatregelen.
REQ-INF-004	Is in staat om Multi-factor authentication (1, 2 en Step-up varianten) midddelen aan te sluiten en doelmatig te beheren.	N	DO-004	X	X	X	X	X	EIS	JA	
REQ-INF-005	Gebruik van compartimentering tussen intern en externe diensten.	N	DO-004 DO-005	X	X	X	X	X	EIS	JA	
REQ-INF-006	Per aan te sluiten IdP of SP wordt een berichtenboek (met SAML profielen) opgesteld. Een berichtenboek legt vast op basis van welke gegevens interfacing plaatsvindt.	N		X	X	X	X	X	WENS	JA	
REQ-INF-007	De back-office systemen staan opgesteld in een vertrouwd en veilig netwerk van de Rijksoverheid. Netwerkfilters zorgen er voor dat kwaadaardige data wordt geblokkeerd voordat de systemen besmet of gecompromitteerd kunnen worden.	N	DO-004	X	X	X	X	X	EIS	JA	
REQ-INF-008	Het netwerkverkeer op het overheidsnetwerk moet continu intensief geïnspecteerd worden op signalen van besmetting en compromittering. Op signalen van compromittering wordt snel en effectief gereageerd.	N	DO-004	X	X	X	X	X	EIS	JA	Taak van het Security Operations Center van SSC-ICT
REQ-INF-009	Beheerders (technisch en functioneel) maken gebruik van sterke authenticatie (met betrouwbare beperking van het aantal login pogingen) voor toegang tot de beheerfuncties van de dienst.	N	DO-004	X	X	X	X	X	EIS	JA	
REQ-INF-010	Het identificerende attribuut is het departementale UserPrincipalName, emailadres of RIN.	N		X	X	X	X	X	EIS	JA	
REQ-INF-011	De services (ICT-voorzieningen) die worden aangeboden moeten om kunnen gaan met externe identiteiten (van vertrouwde partijen)	N		X	X	X	X	X	EIS	JA	

Bijlage 2 – Referentiemodel Governance

Referentiemodel Governance Doorontwikkeling VenJ Federatieve Dienst

Op basis van het Programma van Eisen doorontwikkeling VenJ Federatieve Dienst is het Referentiemodel Governance opgezet met als doel om de gewenste kwaliteit van de dienstverlening, in zijn geheel (dus niet alleen uit het perspectief van SSC-ICT) te kunnen borgen. Hierbij worden de uitgangspunten, belangrijkste triggers en actoren rondom de dienstverlening in relatie gebracht met de gevolgen en mogelijke oplossingsrichting. Hierbij is de bestaande dienstverlening het beginpunt.

Uitgangspunten	• Aanvragen voor het aanbieden en afnemen van diensten via het interne of externe koppelvlak worden beoordeeld door de functioneel beheerder die, indien akkoord, de technische beheerder een opdracht geeft voor realisatie en eventuele projectmatige implementatie en/of ondersteuning. • Afstemming over aansluitvoorwaarden, (gegevens- en attributen-) standaarden, processen, beveiligingsmaatregelen tussen IdP's, SP's en afnemers is de verantwoordelijkheid van de functioneel beheerder. • Planning van het realiseren, prioriteren en de kosten van nieuwe koppelingen ligt bij de functioneel beheerder. • SSC-ICT is een infrastructurele dienstverlener van een generieke dienst • Sectoren zijn en blijven autonoom ten aanzien van hun federatieve dienstverlening. • Informatie-eigenaar is verantwoordelijk voor het aanbieden van zijn oplossing aan federatieve partijen en daarmee verantwoordelijk voor security (hardening), autorisatie tot de applicatie, goedkeuring van autorisatiemiddelen en toegang tot hun oplossing. • De business case voor federatieve ontsluiting ligt bij de gebruikersorganisatie en de specifieke Service Provider/ Systeem- of informatie-eigenaar. • De doorontwikkeling betreft een federatieve infrastructurele dienst die volgens gangbare (BIR-normen) wordt opgebouwd en beheerd. • Gericht op één gezamenlijk extern (Onvertrouwd/Semi-vertrouwd/Vertrouwd) koppelvlak voor federatieve ontsluiting, beschikbaar voor alle aangesloten partijen. Op de grenzen zullen maatregelen worden genomen ten aanzien van security. • Een collectieve schaalgrootte, eenduidig beheerde infrastructurele voorziening. • Flexibiliteit ten aanzien implementatie (korte en lange termijn, maar ook ad hoc) dient mogelijk te zijn. • De VenJ Federatieve Dienst heeft een verhoogde beschikbaarheid, kent uitwijk is 24x7 beschikbaar voor gebruik en onderhoud. *Sectoren kunnen zelf hun eigen externe federaties aangaan echter, de VenJ Federatieve Dienst dient een economisch rendabel alternatief te bieden.*
Belangrijkste Triggers	1. Externe & Interne partijen kunnen toegang krijgen tot applicaties die zich bevinden in zowel de Secure Zone, DMZ / Extranet.
	2. Beheermatige complexiteit neemt toe met het aantal partijen
	3. Externe partijen worden gezien als onvertrouwde partijen
	4. Externe partijen zijn niet onderhevig aan security beheerkaders als BIR-2012
	5. Samenwerking tussen departementen/sectoren en SSC-ICT in rol van IdP én SP én generieke infrastructurele diensten vraagt om ketenregie in geval van incidenten, problems en changes
	6. Niet alle applicaties zijn SAML 2.0 aware
	7. Het VenJ-breed inrichten van een federatieve dienstverlening vereist standaardisatie op Identity management en gebruik van attributen. Met name Identity Management kent meerdere implementaties en is daarmee suboptimaal.

Actoren		Trigger	Gevolgen	Oplossingsrichting
Systeemeigenaar	DI&I	2	Kosten van beheer nemen toe	Vergroting van de schaalgrootte. Investeren in Procesbeschrijvingen (Incident & Change management, Problem en Security management), ontwikkeling formulieren, standaarden, opbouwen Wiki, handleidingen e.d.
Systeemeigenaar	DI&I	1	Vertraging in acceptatie als gevolg van niet direct omarmen van innovatieve beveiligingsconcepten	Idealiter; het vormen én uitdragen van dit beleid
Systeemeigenaar	DI&I	7	Federatief ontsluiten kan aantrekkelijker gemaakt worden door alternatieve oplossingen te faciliteren	Verder uitwerken of een SAML-Gateway of vergelijkbare oplossingen centraal kunnen worden aangeboden zodat deze de specifieke business case voor de betrokken SP positief beïnvloeden.
Functioneel beheerder	JustID	1	Externe partijen zijn niet vertrouwd en mogen geen Departementaal Vertrouwelijke informatie inzien.	Externe partijen (semi) vertrouwd maken door opstellen (en ondertekenen) van Juridisch sluitend convenant (Raamovereenkomst) • Raamovereenkomst met iedere partner afsluiten, inclusief de verantwoordelijkheden ten aanzien van de rollen IdP en SP nader uitgewerkt op generiek niveau. (door de SP kunnen op basis van de generieke eisen aanvullende specifiekere eisen gesteld worden aan de federatie) o Verantwoordelijkheid voor doen en laten van haar gebruikers o Evt. boetebeding o Expliciet uitsluiten van aansprakelijkheid o Specifieke afspraken inzake ter beschikking stellen applicatie in separate bijlage (aanvullend) op de raamovereenkomst. o Speciale aandacht voor Intellectuele Eigendom (IP), WBP en vertrouwelijkheid ➔ Juridische Normenkader Cloud Services Hoger Onderwijs is een zeer goed inspiratiepunt (Hergebruik)
Functioneel beheerder	JustID		Afdwingen Standaardisatie	Uitgangspunt is om aan te sluiten bij de gangbare of overeengekomen standaarden. Partijen die hieraan niet voldoen dienen te streven (verbeterplan) om aan de standaarden te kunnen voldoen.
Functioneel beheerder	JustID		Bewaken kwaliteit van dienstverlening	• Kwantitatief: Administratie, Exploitatie van de dienst • Kwalitatief: Auditing, bewaking gemaakte afspraken, bewaken van verbeterplannen
Technisch Beheerder	SSC ICT	2	Complexe oplossingen • Hoogwaardige specifiek ingerichte ICT-beveiligingsvoorziening	Investeren in • Procesbeschrijvingen (Incident & Change management), Ketenregie (kennispartij) • ontwikkelen formulieren, standaarden,

			en.
			• Extern onvertrouwd/vertrouwd koppelvlak
			• Hoge eisen aan beheer vanuit onder meer Logius
			• Groter aantal federatieve partners zowel met diversiteit in oplossingen
			• Gedelegeerde verantwoordelijkheden naar lokale partijen zoals externe partners en sectoren
				• opbouwen Wiki, handleidingen e.d.
				• Bijhouden van specifieke afspraken in DAP/Wiki
				  ○ Met Servicedesks, investeren in handleidingen voor Servicedesks (1st level Problem Determination)
				  ○ met 2de lijnsondersteuning bij de federatieve partners
				  ○ Afspraken over beschikbaarheid tijdens gepland onderhoud en doorvoeren van wijzigingen
				• Inrichten derdelijns ondersteuning bij SSC-ICT.
				• Streven naar standaardisatie door onder meer de ontwikkeling van handleidingen voor het beheer van federatieve oplossingen.
				• Redundantie & capaciteit om 24x7 uur operatie mogelijk te maken
				• Representatieve acceptatieomgeving, evt. ook testomgeving.

Technisch Beheerder	SSC-ICT	1	Aanpassen dienstverlening VenJ Federatieve Dienst	Aanpassen van de Dienstbeschrijving:
				• Meer commercieel en informeren welke mogelijkheden geboden worden.
				• Taken en verantwoordelijkheden van; IDP, SP, gebruikers, DI&I, etc
				• Hoe de dienst kan worden aangevraagd en bij wie.
				• Exploitatiemodel
				• Verwijzing naar:
				  ○ Aansluitvoorwaarden
				  ○ Handleidingen c.q. implementatierichtlijnen
				  ○ Incident, Change en Problem management

Gebruiker		1,3,4	Binnen de vertrouwensketen zijn gebruikers traditioneel de zwakste schakel	Gebruikers vallen expliciet onder de verantwoordelijkheid van de eigen organisatie. De eigen organisatie dient toe te zien op: • Gebruikers hebben een geheimhoudingverklaring getekend, beschikken over een VOG of geldige screening • Gebruikers dienen security-aware te zijn bij het gebruik van informatiesystemen • Toegang tot informatie is gebaseerd op “Need to know” • Gebruikers dienen zich bewust te zijn van wet en regelgeving die op hen of hun organisatie van toepassing is (de belangrijkste: Intellectueel eigendom, WBP) en van vertrouwelijkheid • Gebruikers dienen zich bij het gebruiken van gefedereerde systemen expliciet akkoord te verklaren

				met de nadere regels en voorwaarden (vinkje in check box voorzien van de mogelijkheid om de specifieke voorwaarden nader in te zien. Wanneer voorwaarden veranderen dient deze check wederom aan de gebruikers getoond te worden. • Instemming dient geregistreerd te worden. • Bij het verlenen van toegang tot een applicatie kan, op basis van beleid van de SP/informatie-eigenaar, de gebruiker welkom worden geheten middels een e-mail. In de e-mail kunnen dan nadere instructies, richtlijnen tip & tricks, functionele ondersteuning en andere nuttige zaken gedeeld worden. De gebruiker kan ook gevraagd worden om de e-mail te beantwoorden, zijn instemming te overtuigen e.d. waarna de dienst daadwerkelijk kan worden opengesteld.
Identity provider (IdP)		8	Gedegen beheer van identiteiten ten behoeve van het IdP-systeem dient zoveel mogelijk gestandaardiseerd te verlopen maar kent lokale interpretatie verschillen	Dit is een al langer bestaand en gesignaleerd issue. Het streven is om op termijn tot een uniform proces te komen. Het vormt ook de uitdaging van het Programma Toegang. De verwachting is dat er op dit gebied stappen gemaakt gaan worden zoals het RIN en het realiseren van de Rijks Identity Store (RIS). - Ondertussen zal er suboptimaal gewerkt worden met de bestaande implementatie en zullen bewerkingen zoals ontdubbelen, ondersteuning van meerdere rollen, issues met werkrelaties uitgevoerd worden. Deze inefficiëntie zal geaccepteerd moeten worden en zal ook de kwaliteit voor sommige "Werkrelaties" verminderen.
Identity provider (IdP)		8	Invulling geven aan WBP-vereisten	Omdat er persoonsgegevens van gebruikers worden uitgewisseld tussen de organisatie als Identity Provider en de Service Provider, vereist de Wet bescherming persoonsgegevens dat er expliciet toestemming moet worden gegeven voor het vrijgeven van attributen aan een Service Provider. • Onderzoeken welke persoonsgegevens er daadwerkelijk gebruikt worden en in hoeverre deze onder of buiten de WBP-kaders vallen. • Bovengenoemde dient generiek in de aansluitvoorwaarden te zijn opgenomen als basis. • Op oplossingsniveau dient het een aandachtspunt te zijn tussen de lokale IdP en de SP. Door encryptie* van SAML-tokeninformatie met als doel authenticatie wordt deze informatie afgeschermd. Voor auditing is het belangrijk dat het tot een natuurlijk persoon moet kunnen worden getraceerd.

				**) het encrypten van een SAML-token kan resulteren in een aanzienlijke beheerlast, omdat informatie in het token niet geraadpleegd kan worden. Dit kan een onderdeel zijn van Departementaal Vertrouwelijk, echter SAML-tokens worden getransporteerd via een met encryptie beveiligde tunnel.*
Identity provider (IdP)		1	Externe partijen beheren identiteiten naar eigen inzicht	Waar intern Rijk partijen gebonden zijn aan de BIR-richtlijnen hoeven externe partijen niet aan de BIR te voldoen. De verwachting is dat de externe federatieve partijen een vergelijkbaar (ISO-27002) ICT-beveiligingskader volgen en dat met name het Identity Management proces borgt dat de identiteit te koppelen valt aan een persoon en dat het beheer volgens de procedures wordt uitgevoerd. Deze eis dient deel uit te gaan maken van de aansluitvoorwaarden • Het Identity Management proces dient op aangeven van de Systeemeigenaar (DI&I) geaudit te kunnen worden. • Uitgangspunt dient te zijn dat de processen niet al te veel zullen afwijken van de BIR-2012 en dat waar ze afwijken dit volgens afspraken verbeterd zal gaan worden.
Identity provider (IdP)			Het toegang verlenen tot applicaties zal plaatsvinden op basis van attributen die voor een deel bij de lokale IdP verkregen dienen te worden in een SAML-token.	Uitgangspunt zou moeten zijn om zoveel mogelijk aan de standaarden te conformeren. Dit is een eis in de aansluitvoorwaarden. • SAML-attributen zijn in het format van de xmlsoap namespace (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/) • De unieke identifer is op dit moment het e-mailadres maar doel is dat dit het RIN gaat worden voor Rijksmedewerkeers. Dit omdat er uit e-mailadressen informatie te onttrekken is. • Niet Rijksmedewerkers hebben geen RIN! Mogelijk dat er gewerkt kan worden met een personeelsnummer, mogelijk in combinatie met een ander attribuut zoals rol/functie om hiermee uniekheid en Need to Know te bewaken. (Punt van aandacht binnen ontwerpfase) • de ontwikkelingen rondom het RIN zijn voor de doorontwikkeling een afhankelijkheid met een punt op de nabije horizon. ○ Acceptatie dat op termijn een meer optimale beheersituatie zal ontstaan en daarmee het beheer nog niet geoptimaliseerd kan zijn.
Service Provider		1, 7	Applicaties aan derden partijen	Service Provider, en in het bijzonder de informatie-eigenaar,

(SP)			ter beschikking stellen vraagt een actieve rol van de informatie-eigenaar (SP)	is verantwoordelijk voor de technische en organisatorische ontsluiting van zijn applicatie aan federatieve partners. • De vertrouwelijkheid, integriteit en beschikbaarheid van de applicatie als mede de afweging hoe en aan wie (hardening) de applicatie ter beschikking wordt gesteld liggen in het domein van de SP • De applicaties dient bij voorkeur SAML 2.0 aware te zijn, echter wanneer dit niet mogelijk is dan kan een SAML-gateway overwogen worden. • Gebruikers expliciet en nader informeren over de voorwaarden waarop toegang is verleend. Dit via een e-mail, evt. na reply dat de gebruiker de voorwaarden accepteert en zal naleven, daadwerkelijke toegang vrijgeven. Reply op de e-mail dient te worden bewaard in een archief. 1. Voordat een overeenkomst wordt afgesloten met derden: 2. Uitvoeren van een risicoanalyse op de punten: o Voldoende kwaliteitsborging in de gebruikende organisatie aanwezig om aan de gestelde eisen (generieke + specifieke aansluitvoorwaarden) blijvend te kunnen voldoen o Is er een Need To Know (eventueel kwantificeerbaar in een win/win) o Is er een goede business case o Is de SP voldoende in control o Wat wil de gebruiker met de informatie doen. Is dit in overeenstemming met het doel van de applicaties, is er misschien een alternatieve niet gewenste mogelijkheid die door toegang te verlenen onbedoeld mogelijk wordt gemaakt. o Waar wordt eventuele informatie opgeslagen. In de Cloud? Willen we dit? Welke zekerheden hebben we. o Kan ik de gevraagde beschikbaarheidsniveaus bieden o Kan ik aansprakelijk worden gesteld 3. De voorwaarden waaronder de SP informatie ter beschikking stelt wordt in een separate bijlage, bij de aansluitvoorwaarden, (juridisch) vastgelegd. 4. Afspraken dienen binnen de DAP actueel gehouden te worden. 5. Ontsluiting dient vanuit de informatie-eigenaar

				geïnitieerd te worden naar de lokale Identity provider.
Service Provider (SP)		6	Informatie-eigenaar is verantwoordelijk voor dat aanvullende maatregelen ten aanzien van beveiliging worden afgedwongen en geïmplementeerd	Alleen de systeem/informatie-eigenaar kent de voorwaarden waaraan voldaan dient te worden om invulling te geven aan de aanvullende vereisten voor Departementaal Vertrouwelijk. • Kosten voor de additionele voorzieningen zullen vanuit de business case dienen te worden gedekt. • Zijn de voorzieningen meer generiek te gebruiken, dan dient er een afstemming plaats te vinden tussen; JustID, SP en zo nodig SSC-ICT.
Service Provider (SP)			Niet gestandaardiseerde attributen worden gebruikt binnen applicaties	Hoewel dit primair een verantwoordelijkheid is van de informatie-eigenaar kan niet worden uitgesloten dat, omwille van het succes van deze generieke dienst (business case), onderzocht wordt of er centrale voorzieningen getroffen kunnen worden die de tegemoet komen aan de uitdagingen voor de SP. • Dit is sterk applicatie-gerelateerd • Binnen Defensie is er gedachtegoed rondom Claims Transformatie ontwikkeld dat mogelijk een oplossingsrichting kan bieden. Dit zou nader onderzocht kunnen gaan worden.

Service Provider (SP)		5	De organisatie- en/of Taakvolwassenheid ten aanzien van de rol van Service Provider is nog niet op het gewenste niveau	Federatieve dienstverlening is een relatief nieuwe techniek en vereist bepaalde mate van gespecialiseerde kennis op dit gebied die vaak niet aanwezig is en zal moeten worden opgebouwd. Ook de verantwoordelijkheid voor de informatiebeveiliging welke bij de Informatie Eigenaar is neergelegd stelt hoge eisen aan de organisatie van de SP.
				• Primair de verantwoordelijkheid van de SP.
				• SSC-ICT kan de SP ondersteunen (Projectmatig/Adviseur) op het gebied van federatie door:
				  ○ SSC-ICT kan door schaalgrootte zijn specialistische kennis en ervaring bundelen en aan de individuele Service Providers als "Implementatiedienst" ter beschikking stellen.
				  ○ SSC-ICT kan ook invulling geven aan een selfservice loket gelijk aan Surfnet.
				  ○ Op aangeven van Functioneel Beheerder (JustID)

Bijlage 3 – Begroting doorontwikkeling VenJ Federatieve Service

Doorontwikkeling VenJ Federatieve Dienst	*tarieven*	€ 100	€ 125					
		Inspanning				*Indicative Begroting*		
		Intern	Extern	Totaal Werk	Doorlooptijd	Projectkosten	Investering	Onderhoud
Ontwerpfase		0	0	0		€ 0		
1	Opstellen TO	100	50	200		€ 23.750		
2	Aanpassen Technische beheerkaders	0	0	0		€ 0		
	Wiki & Kennis management	40	0	40		€ 4.000		
	Incident management	40	0	40		€ 4.000		
	Change management	40	0	40		€ 4.000		
	Problem management	40	0	40		€ 4.000		
	Security Management	40	0	40		€ 4.000		
3	Ontw. Blueprint Federatieve dienstverlening	80	0	80		€ 8.000		
		380	50	480	4 maanden	€ 51.750	€ 0	€ 0
Realisatiefase		0	0	0		€ 0		
1	Realisatie TO (bouwen & configureren)	0	0	0		€ 0		
1,1	Testomgeving	100	0	100		€ 10.000		
1,2	Acceptatieomgeving	80		80		€ 8.000		
1,3	Productieomgeving	80		80		€ 8.000		
2	Impl. Aangepaste Technsiche beheerkaders	0	0	0		€ 0		
	Update PDC	16	0	16		€ 1.600		
	Update DAP	8	0	8		€ 800		
	Incident management	20	0	20		€ 2.000		
	Change management	20	0	20		€ 2.000		
	Problem management	20	0	20		€ 2.000		
	Security management	20	0	20		€ 2.000		
	Instructie Servicedesk	24	0	24		€ 2.400		
	Update WiKi	16	0	16		€ 1.600		
3	Implementeren Federatieve dienstverlening	0	0	0		€ 0		
	Instructies voor gebruikers (e-mail/Schermen)	48	0	48		€ 4.800		
	Handleiding impl. Federatieve Ontsluiting	16	0	16		€ 1.600		
	Instructie IDP	24	0	24		€ 2.400		
	Instructie SP	24	0	24		€ 2.400		
	Instructies Servicedesk (niet SSC-ICT)	16	0	16		€ 1.600		
	Technische handleidingen	40	0	40		€ 4.000		
4	SAAM Analyse NBV	16	0	16		€ 1.600		
		628	0	628	2-3 maanden	€ 58.800	€ 0	€ 0
Operation fase		0	0	0		€ 0		
1	Overdracht naar Beheer	0	0	0		€ 0		
	Applicatiebeheer VenJ Federatieve Dienst	16	0	16		€ 1.600		
		16	0	16	1 week	€ 1.600	€ 0	€ 0
25%	Projectmanagement	0	281	281		€ 35.125		
	Inspanningsbegroting	1024	331	1405		€ 147.275	€ 0	€ 0
25%	Tolerantie					€ 36.819		
	Project budget					€ 184.094		

SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DG Organisatie
Bedrijfsvoering Rijk
SSC-ICT Haaglanden
GDI/BH/IAM

Contactpersoon
Dijen, T. van

T 079 330 22 46
t.van.dijen@gdi.minvenj.nl

Datum
17 september 2015

Notulist
Tim van Dijen

verslag

Interview opdrachtgever

Omschrijving	Gespreksverslag van het interview betreffende de doorontwikkeling van de VenJ Federatieve Dienst.
Vergaderdatum en -tijd	17 september 2015, 10.30 uur
Aanwezig	Tim van Dijen Paul van Kruistum

In welke hoedanigheid neem je deel aan dit gesprek?
Ik ben manager van de afdeling IAM en opdrachtgever voor de doorontwikkeling van de VenJ Federatieve Dienst. Ook fungeer ik als proxy voor de daadwerkelijke klant, de directie Informatisering en Inkoop van het Ministerie van Veiligheid en Justitie.

Hoe kijkt de klant aan tegen de dienst en de ontwikkeling hiervan?
De klant stelt vraagtekens bij de hoge kosten en in contrast daarmee de moeizame ontwikkeling van de dienst. Het beeld ontstaat dat SSC-ICT niet 'in control' is als het op het beheer aankomt.

Wat kunnen de gevolgen zijn voor SSC-ICT als er geen verbetering plaatsvindt?
Worst-case scenario zou zijn dat de klant een andere partij zoekt om mee in zee te gaan. Het beheer van de VenJ Federatieve Dienst is al verdeeld over twee beheerpartijen, namelijk SSC-ICT en JustID, dus een verschuiving van het speelveld ligt altijd op de loer. Het zou zonde zijn als we dit stukje dienstverlening kwijt zouden raken.

In welke hoek denk je dat de oplossing gezocht moet worden?
Dat de dienst momenteel te duur wordt gevonden door de klant kan ik heel goed begrijpen. Daar moet absoluut iets aan veranderen. Dan moet je al snel denken aan meer efficiëntie in werkzaamheden en kostenbesparingen. De kosten voor arbeid zijn altijd de grootste kostenpost. In dat licht ben ik zelf al aan het kijken of er intern iemand opgeleid kan worden om de huidige externe beheerder op termijn te kunnen vervangen.

DG Organisatie Bedrijfsvoering Rijk
SSC-ICT Haaglanden Pijler 2
GDI/BH/IAM

Datum
17 september 2015

Waar moet de uiteindelijke oplossing aan voldoen, vanuit jouw oogpunt als manager IAM?
Ik hoop de klant een dienst te kunnen bieden die hetzelfde, of liefst nog meer kan als de bestaande dienst, maar dan tegen gereduceerde kosten. Ook hoop ik meer flexibiliteit te kunnen bieden aan mijn klant, door bijvoorbeeld nieuwe VenJ-onderdelen veel sneller te kunnen aansluiten op de federatie. De klant let uiteindelijk vooral goed op zijn portemonnee, maar er zijn meer factoren die een rol spelen. Ik wil meer daadkracht en hands-on mentaliteit kunnen uitstralen, zodat de klant weer vertrouwen krijgt in SSC-ICT en in de dienst

Zijn er mensen binnen de organisatie die ik absoluut moet raadplegen in het kader van dit project?
Het lijkt me verstandig dat je in ieder geval met de huidige beheerder en met onze domeinarchitect gaat praten. De beheerder heeft vanuit zijn eigen rol ook een beeld van wat er moet veranderen. De architect kan je meer vertellen over beleidskaders en standaarden waar aan moet worden voldaan binnen de Rijksoverheid. Ook is hij recent betrokken geweest bij een doorontwikkelingstraject van de rijksbrede federatie. Ik kan me voorstellen dat hier (her)bruikbare ideeën uit voort gekomen zijn.

SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DG Organisatie
Bedrijfsvoering Rijk
SSC-ICT Haaglanden
GDI/BH/IAM

Contactpersoon
Dijen, T. van

T 079 330 22 46
t.van.dijen@gdi.minvenj.nl

Datum
21 september 2015

Notulist
Tim van Dijen

verslag

Interview beheerder

Omschrijving	Gespreksverslag van het interview betreffende de doorontwikkeling van de VenJ Federatieve Dienst.
Vergaderdatum en -tijd	21 september 2015, 10.00 uur
Aanwezig	Tim van Dijen Georg Grabner

In welke hoedanigheid neem je deel aan dit gesprek?
Ik ben als externe medewerker belast met het dagelijks beheer van het SSC-ICT-gedeelte van de VenJ Federatieve Dienst.

Hoe ervaar je die taak momenteel?
Alles gaat een beetje rommelig allemaal. Ik heb de taak een klein jaar geleden overgenomen van een voorganger die de organisatie ging verlaten. Zelf had ik op dat moment nog vrijwel geen ervaring met Federation.

Zijn er duidelijke oorzaken aan te wijzen voor de rommeligheid?
Allereerst is de kennis binnen de organisatie op het gebied van Federation erg beperkt. Er staat ook maar weinig op papier, zoals een TO, installatiehandleidingen of beheerafspraken. Verder zijn de omgevingen allemaal anders ingericht, dus ik zoek me telkens wezenloos naar bijvoorbeeld een logfile. Ook het feit dat het beheer over verschillende beheerpartijen is verdeeld maakt het er allemaal niet duidelijker op.

Daarnaast is het product voor de IdP-Proxy echt een ramp in alle opzichten; veel storingen/uitval en het doet vaak niet wat het zou moeten doen (volgens protocolspecificaties). Er is bij de initiële inrichting ook allemaal slecht gedocumenteerd maatwerk gedaan om maar aan de wensen van de klant te kunnen voldoen.

Zie je verder nog mogelijke problemen voor de toekomst?
Zoals ik al aangaf ben ik extern, dus ik loop eerdaags ook een keer de deur uit met het beetje kennis wat ik de afgelopen maanden heb opgedaan. Dit is vooral een risico voor SSC-ICT als organisatie.

DG Organisatie Bedrijfsvoering Rijk
SSC-ICT Haaglanden Pijler 2
GDI/BH/IAM

Datum
21 september 2015

Zijn er concrete dingen waarvan je denkt dat ze kunnen bijdragen aan de oplossing van de huidige problematiek?
Het gelijktrekken van gelijke componenten zou mij als beheerder al heel erg helpen in het dagelijks beheer. Verder heb ik als applicatiebeheerder niet zo veel infrastructurele kennis, maar ik kan me niet voorstellen dat er geen efficiëntieslag mogelijk moet zijn. Nu wordt er voor elk VenJ-onderdeel een aparte IdP of zelfs een cluster ingericht. Ik heb me laten vertellen dat er uiteindelijk drieëntwintig onderdelen moeten aansluiten, dus dat worden aardig wat machines! Dat valt straks niet meer te beheren op de huidige manier.

Zijn er nog dingen die niet direct gerelateerd zijn aan de problematiek, maar die je wel graag anders zou zien om jouw werk makkelijker en/of efficiënter te maken?
Als ik nu één van de geclusterde machines (proxy of IdP) benader in de browser, kan ik niet eenvoudig zien op welke node ik zit. Daar moet ik dan op alle nodes de logfiles voor gaan doorspitten. Dit is voor mij wel een grote ergernis. Ook het gebrek aan een testomgeving om bijvoorbeeld patches te kunnen testen is lastig.

SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DG Organisatie
Bedrijfsvoering Rijk
SSC-ICT Haaglanden
GDI/BH/IAM

Contactpersoon
Dijen, T. van

T 079 330 22 46
t.van.dijen@gdi.minvenj.nl

Datum
21 september 2015

Notulist
Tim van Dijen

verslag

Interview domeinarchitect

Omschrijving	Gespreksverslag van het interview betreffende de doorontwikkeling van de VenJ Federatieve Dienst.
Vergaderdatum en -tijd	21 september 2015, 14.00 uur
Aanwezig	Tim van Dijen Jan Over

In welke hoedanigheid neem je deel aan dit gesprek?
Ik ben domeinarchitect Identity & Access Management binnen SSC-ICT. Ik die rol bewaak ik de architectuur en toets ik wijzigingen op het naleven van architecturen en beleidsrichtlijnen.

Ik begrijp dat er binnen de Rijksoverheid een aantal normen en standaarden zijn waaraan moet worden voldaan. Waar is de VenJ Federatieve Dienst aan onderhevig?
Alles wat binnen de Rijksoverheid gedaan wordt moet hoe dan ook voldoen aan de BIR-2012. Dit is een standaard voor informatiebeveiliging, zoals bijvoorbeeld de ISO-27002. Vanuit mijn rol als architect zie ik graag dat de dienst ook voldoet aan de Doelarchitectuur Toegang 2015, onder het mom van: comply or explain. Tot slot weet ik dat er binnen VenJ beleid is omtrent de inspectie van netwerkverkeer.

Ben je bekend met de huidige problematiek met de VenJ Federatieve Dienst en hoe kijk je hier tegenaan?
Ik ben bekend met het feit dat de klant wat ontevreden is over de dienst en de kosten die daarmee gemoeid zijn. Als ik zie wat er nu staat dan kan ik me dat ook wel een beetje voorstellen. De opzet van het geheel is veel te groot en log. Ik kan in die zin de gedachtegang van de ontwerpers ook niet helemaal volgen. Volgens mij moet het allemaal veel compacter kunnen.

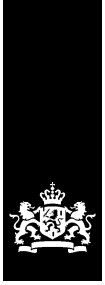
Ik heb ook begrepen dat je betrokken bent geweest bij de doorontwikkeling van de rijksbrede federatie. Zijn hier nog noemenswaardige dingen over te zeggen die wellicht ook van toepassing zijn bij dit project?
Op rijksbreed niveau is gekozen om de beweging naar een volledig open-source dienst in te zetten. De beslissing moet nog vallen, maar naar alle waarschijnlijkheid gaat men gebruik maken van SurfConext. Dit is een pakket ontwikkeld door SurfNet en is beproefde technologie. Het wordt binnen het hoger

onderwijs toegepast en kent vele tienduizenden eindgebruikers. Qua architectuur is er voor gekozen om een intern en een extern koppelvlak te definiëren, om hier een logische scheiding in te behouden.

Ook komt er een koppelvlak voor externe authenticatie, zoals DigID, met het idee dat alle onderliggende departementen hier in de toekomst gebruik van kunnen maken. Dit is gedaan uit economisch oogpunt, zodat niet alle departementen dit voor zichzelf gaan regelen.

DG Organisatie
Bedrijfsvoering Rijk
SSC-ICT Haaglanden Pijler 2
GDI/BH/IAM

Datum
21 september 2015



SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Doorontwikkeling Federatieve Service

Technisch ontwerp

Auteur: Tim van Dijen

Opdrachtgever: Dhr. R. P. van Kruistum

Datum: maandag 16 november 2015
Versie: 1.0
Status: Definitief

Colofon

Afzendgegevens	**DG Organisatie Bedrijfsvoering Rijk** SSC-ICT Haaglanden Pijler 2 Luxemburglaan 2 2711 BC Zoetermeer Postbus 7385 2701 AJ Zoetermeer
Contactpersoon	T. van Dijen T 079 330 22 00 F 079 330 22 22
Projectnaam	Doorontwikkeling VenJ Federatieve Dienst
Auteurs	T. van Dijen

Documenthistorie

Versie	Status	Datum	Wijzigingen
0.1	Concept	1-11-2015	Eerste versie
1.0	Definitief	16-11-2015	Vastgesteld i.o.m. opdrachtgever

Inhoudsopgave

1. Inleiding

Voorliggende rapportage is een technisch ontwerp ten behoeve van de doorontwikkeling van de federatieve dienst van het Ministerie van Veiligheid en Justitie. Het ontwerp is opgesteld aan de hand van het document "Definitiestudie – Doorontwikkeling VenJ Federatieve Service" versie 1.2.

1.1 Bronnen

Nr.	Titel	Datum / Versie	Bron
01	Opdrachtomschrijving Doorontwikkeling VenJ Federatieve Dienst	6-8-2015 / v1.0	DI&I
02	(Oude) Functioneel ontwerp (Departementaal Vertrouwelijk)	2012	MinVenJ
03	Doelarchitectuur Toegang	30-5-2015 / v0.8	MinBZK - Tactische Regie op de Generieke ICT (TBGI)
04	Impactanalyse doorontwikkeling Rijks-SSOn (Departementaal Vertrouwelijk)	V1.0	MinBZK - TBGI
05	Baseline Informatiebeveiliging Rijksdienst – Technisch Normenkader	1-12-2012 / v1.0	MinBZK - TBGI

1.2 Leeswijzer

Hoofdstuk 2 bevat een beschrijving van de dienst waarop dit Technisch Ontwerp van toepassing is.

Hoofdstuk 3 is een opsomming van de technische eisen die worden gesteld aan de verschillende federatieve componenten.

Hoofdstuk 4 geeft de Referentiearchitectuur / Logisch Ontwerp weer zoals opgesteld in de Definitiestudie v1.0.

Hoofdstuk 5 is het daadwerkelijke Technisch / Fysiek Ontwerp.

Hoofdstuk 6 beschrijft de ontwerpbeslissingen die ten grondslag liggen aan dit Technisch Ontwerp.

2. Dienstbeschrijving

Federatie gaat over het overdragen van gegevens tussen twee partijen. Dit kan zowel tussen organisaties en consumenten als tussen organisaties onderling plaatsvinden. Het doel van dit zogeheten federatieve identity management is vrijwel altijd het vertrouwen en/of authentiseren van personen buiten de eigen organisatie.

Een goed voorbeeld van federatie op grote schaal in Nederland is DigiD. Om de authenticiteit van een belastingaangifte te kunnen bewijzen richting de belastingdienst is verificatie van uw identiteit bij een vertrouwde derde partij (DigiD) nodig. De authenticatie (wie ben je?) vindt dus extern plaats. De autorisatie (wat mag je?) blijft in handen van de Belastingdienst.

Een ander goed voorbeeld is de rol die SURFnet vervult binnen de SURFfederatie. De SURFfederatie is een federatieve dienst die onderwijsinstellingen en derden met elkaar kan koppelen. Middels federatie en single sign-on (SSO) zal het voor studenten en medewerkers mogelijk zijn om na het aanmelden bij hun eigen instelling alle diensten (services) van derden te benaderen, zonder additioneel in te hoeven loggen. Een groot voordeel voor de studenten die geen extra identiteiten en wachtwoorden hoeven te onthouden.

Naast eindgebruikers ondervinden ook de aangesloten dienstverleners (Service Providers) grote voordelen van federatie. Afhankelijk van de opzet hoeft er namelijk weinig tot wellicht helemaal geen identiteit management plaats te vinden. De onderwijsinstelling (Identity Provider) word immers vertrouwd de juiste gegevens aan te leveren, op basis waarvan de dienstverlener toegang tot de relevante informatie kan bieden.

Zoals uit bovenstaande introductie blijkt is een federatieve koppeling eigenlijk meer een vertrouwensrelatie tussen minimaal twee partijen. Meestal zullen deze partijen een klant – dienstverlener relatie onderhouden. De klant is in deze niet altijd gelijk aan de eindgebruiker. De eindgebruikers maken dus gebruik van de diensten die door de dienstverlener worden aangeboden op basis van hun rol binnen een organisatie.

Een groot probleem binnen deze klant – dienstverlener relatie is het onderhoud van identiteiten. Eindgebruikers moeten weer een andere gebruikersnaam en wachtwoord onderhouden en eventuele extra gegevens (adres, email, etc.) onderhouden. De dienstverlener moet de gebruikersgegevens beschermen. De organisatie is niet gebaat bij de problemen die kunnen ontstaan door het bestaan van weer een set identiteitsgegevens in een extern systeem.

Er wordt een vertrouwensrelatie opgebouwd tussen de klant en de dienstverlener, met heldere afspraken over de gegevens die verstrekt moeten worden om een dienst te kunnen benutten. De klant stuurt alle relevante gegevens van de eindgebruiker mee tijdens de authenticatie, zodat de dienstverlener bijvoorbeeld autorisatie van de gebruiker en facturatie van de gebruikte functionaliteit kan uitvoeren.

Aangezien de dienstverlener de identiteitsgegevens niet hoeft op te slaan, hoeft de eindgebruiker geen additionele gebruikersnaam en wachtwoord te onthouden. Zolang hij maar is aangemeld bij het eigen interne systeem zal Single Sign-On worden toegepast. Hiermee wordt de aangeboden dienst een verlenging van het interne systeem.

2.1 Service Providers en Identity Providers

De termen Service Provider (SP) en Identity Provider (IDP) zijn al benoemd. In bovenstaande voorbeelden is het duidelijk dat de Belastingdienst bijvoorbeeld als dienstverlenende partij fungeert. In federatieve termen zijn zij dus de Service Provider.

De onderwijsinstellingen en DigiD uit het voorbeeld fungeren hierbij als de Identity Provider, de partij die de authenticatie uitvoert en de identiteit verifieert. Een partij kan tevens zowel als IDP en als SP optreden. Een universiteit bijvoorbeeld kan dienstverlener zijn (bijvoorbeeld de bibliotheek) en tegelijkertijd diensten afnemen.

Als we deze voorbeelden vertalen naar de VenJ-situatie komt daar een component bij. Zoals beschreven in de definitiestudie kent het niveau van VenJ een centraal distributiepunt voor de SAML-berichten, de IdP-Proxy. Op departementaal niveau staan immers geen databanken die zouden kunnen dienen als bron voor de Identity Provider.

De functionaliteiten waar het realisatieproject zich initieel op zal focussen op het intern en extern federeren voor rijksambtenaren, overeenkomstig met Fase 1 + 2 uit de definitiestudie. Een koppeling met eHerkenning en DigID (Fase 3) is reeds operationeel als Proof of Concept bij JustID. Gezien de ontwikkelingen op rijksbreed niveau wordt hier voorlopig van afgezien voor dit project.

Om de federatieve samenwerking te kunnen realiseren dienen de volgende componenten aanwezig te zijn op VenJ niveau:

- IdP-Proxy op JustitieNet om koppelingen met het achterland (VenJ-onderdelen) te leggen;
- Poort om toegang te verlenen voor diensten (Access Gateway) die door VenJ worden geleverd;
- Logging-faciliteit waarin de activiteiten van de IdP-Proxy en Acces Gateway gemonitord kunnen worden.

Omdat de diverse VenJ-onderdelen nog niet tot 1 standaard SAML-profiel hebben kunnen komen zullen bij de start meerdere profielen worden gedefinieerd. Dit is technisch haalbaar, maar wellicht praktisch minder gewenst. Buiten het beheer van de profielen zelf heeft dit ook impact op de IdM-keten, welke de zorg en verantwoordelijkheid draagt voor het aanleveren van de juiste gegevens.

De centrale – VenJ-brede – componenten van de VenJ Federatieve Dienst kunnen we zien als een snelweg voor het federatief samenwerken tussen instanties.
Op deze snelweg wordt verkeer (informatie) getransporteerd middels auto's met vaste routes. De “auto's” en “routes” zijn in deze analogie de Federatieve Koppeling of Trust. Trust betekend vertrouwen; de partijen vertrouwen elkaar over de informatie die wordt doorgegeven.

Enerzijds dienen dus de centrale componenten ingericht te worden (de snelweg). Anderzijds dienen de individuele trusts ingericht te worden (de auto en route). Uiteraard is er een sterke afhankelijkheid tussen de centrale componenten en de trusts; het moet op elkaar afgestemd zijn. De auto mag niet te breed zijn voor de weg en er moet wel een route mogelijk zijn. Deze afspraken zijn vastgelegd in de eerdergenoemde SAML-profielen.

Bij aanvang van de inrichting zijn een aantal federatieve koppelingen actief welke binnen deze oplossing opgenomen worden, of welke op de nominatie staan om ze in het federatieve landschap op te nemen. In de toekomst zullen er echter veel meer federatieve koppelingen actief worden in welke de generieke componenten een onderdeel vormen van deze koppeling. De generieke componenten van de VenJ Federatieve Dienst zullen derhalve aan een groot scala van functionaliteiten moeten voldoen om alle toekomstige toevoegingen te kunnen faciliteren.

Een aantal facetten zijn van belang bij het opstellen van de vereiste functionaliteit. Deze facetten (wie, wat en waar) hebben een grote invloed op de ontwikkeling van de federatieve infrastructuur:

De locatie van de gebruikersaccounts. Dit is eigenlijk het onderscheid tussen de accounts van VenJ-medewerkers en de accounts van de medewerkers van een vertrouwde partner. Vaak zal het zo zijn dat als een VenJ-dienst door medewerkers van vertrouwde partners gebruikt kan worden, ook VenJ-medewerkers de dienst gebruiken.

De locatie van de dienst of applicatie : Binnen het federatieve samenwerken is het van belang waar de dienst of applicatie zich bevindt. Dit kan binnen het VenJ-netwerk zijn of daarbuiten, bij een vertrouwde partner. Hierbij dient wel opgemerkt dat “binnen het VenJ-netwerk” kan betekenen dat het in de DMZ is opgenomen of binnen het interne netwerk.

De locatie van waarvandaan de gebruikers de dienst benaderen. Dit kan ook van binnen het VenJ-netwerk zijn, of daarbuiten. Alle use cases kunnen worden genormaliseerd in een aantal scenario's:

#	Gebruiker Type	Identiteiten-leverancier (IdP)	Werkomgeving (Client)	Applicatieomgeving (SP)	Dienst versie
1	VenJ-medewerker	Sector	Sector	Eigen departement	1.0
2	VenJ-medewerker	Sector	Sector	Eigen sector	2.0
3	VenJ-medewerker	Sector	Sector	Ander departement	2.0
4	VenJ-medewerker	Sector	Sector	Andere sector	2.0
5	VenJ-medewerker	Sector	Sector	Rijksomgeving	1.0
6	VenJ-medewerker	Sector	Sector	Extern	2.0
7	VenJ-medewerker	Sector	Extern	Extern	2.0
8	Rijksmedewerker	Sector	Extern	Extern	2.0
9	Rijksmedewerker	Sector	Sector	Departement (VenJ)	2.0
10	Rijksmedewerker	Sector	Sector	Sector (VenJ)	2.0
11	Rijksmedewerker	Sector	Sector	Extern	2.0
12	Derden	Extern	Extern	Departement (VenJ)	2.0
13	Derden	Extern	Extern	Sector (VenJ)	1.0
14	Derden	Extern	Extern	Extern	2.0

3. Technische eisen

Buiten de functionele eisen beschreven in het "Doorontwikkeling VenJ Federatieve Dienst - Functionele Specificaties – Versie 1.0" en "Definitiestudie – Doorontwikkeling VenJ Federatieve Dienst" zijn ook technische eisen van toepassing. Deze eisen zijn een afgeleide van functionele eisen, of komen voort uit Rijks- en/of VenJ-breed beleid. Hieronder worden de technische eisen per component beschreven.

3.1 Identity Providers

#	Requirement	Prioriteit
REQ01	De Identity Provider dient hoogbeschikbaar te zijn; als de dienst niet beschikbaar is kunnen gebruikers niet authentiseren.	1
REQ02	De Single Sign-On oplossing dient zowel browser, machine als "rich client" gebruik van applicaties te ondersteunen.	3
REQ03	De Identity Provider dient dusdanig geschaald te zijn dat kan worden voldaan aan het aantal gelijktijdige sessies op de piek momenten.	1
REQ04	De Identity Provider moet opgeschaald kunnen worden indien het aantal gelijktijdige sessies dat vereist.	1
REQ05	Gebruikers kunnen uniek geidentificeerd worden op basis van RIN, UPN of emailadres welke zijn opgenomen in het SAML-token.	1
REQ06	De Identity Provider dient SAML 2.0 te ondersteunen v.w.b. protocols, assertions bindings en profiles.	1
REQ07	De Identity Provider dient toegang te hebben tot User Directory van het betreffende VenJ-onderdeel.	1
REQ08	De Identity Provider dient ongevoelig te zijn voor DOS-aanvallen.	1
REQ09	De Identity Provider dient PKIoverheid-certificaten te ondersteunen	1
REQ10	De logging moet configureerbaar zijn en kunnen worden getransporteerd naar een SIEM-oplossing.	4

3.2 IdP-Proxy

#	Requirement	Prioriteit
REQ01	De IdP-Proxy dient hoogbeschikbaar te zijn; als de dienst niet beschikbaar is kunnen gebruikers niet authentiseren.	1
REQ02	De Single Sign-On oplossing dient zowel browser, machine als “rich client” gebruik van applicaties te ondersteunen.	3
REQ03	De IdP-Proxy dient dusdanig geschaald te zijn dat kan worden voldaan aan het aantal gelijktijdige sessies op de piek momenten.	1
REQ04	De IdP-Proxy moet opgeschaald kunnen worden indien het aantal gelijktijdige sessies dat vereist.	1
REQ05	Gebruikers kunnen uniek geidentificeerd worden op basis van RIN, UPN of emailadres welke zijn opgenomen in het SAML-token.	1
REQ06	De IdP-Proxy dient SAML 2.0 te ondersteunen v.w.b. protocols, assertions bindings en profiles.	1
REQ07	De IdP-Proxy dient ongevoelig te zijn voor DOS-aanvallen.	1
REQ08	De IdP-Proxy dient PKIoverheid-certificaten te ondersteunen	1
REQ09	De logging moet configureerbaar zijn en kunnen worden getransporteerd naar een SIEM-oplossing.	4
REQ10	De IdP-Proxy dient een voorziening te hebben voor home-realm discovery.	1
REQ11	De IdP-Proxy moet ondersteuning hebben voor SAML scoping.	1
REQ12	De IdP-Proxy moet ondersteuning bieden voor automatische home-realm discovery op basis van cookies.	2

3.3 Access Gateway

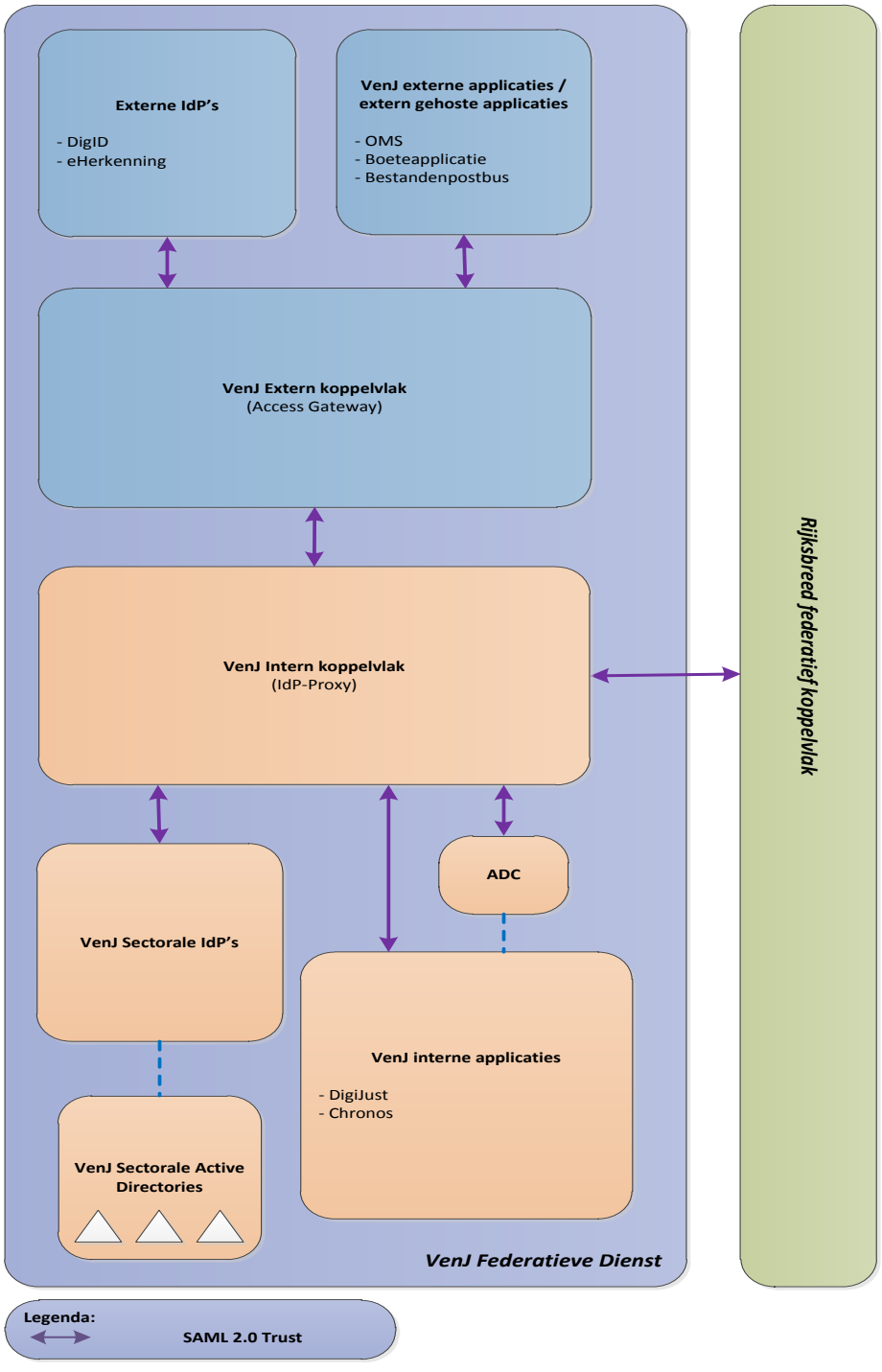
#	Requirement	Prioriteit
REQ01	De Access Gateway dient hoogbeschikbaar te zijn; als de dienst niet beschikbaar is kunnen gebruikers niet authentiseren.	1
REQ02	De Single Sign-On oplossing dient zowel browser, machine als “rich client” gebruik van applicaties te ondersteunen.	3
REQ03	De Access Gateway dient dusdanig geschaald te zijn dat kan worden voldaan aan het aantal gelijktijdige sessies op de piek momenten.	1
REQ04	De Access Gateway moet opgeschaald kunnen worden indien het aantal gelijktijdige sessies dat vereist.	1
REQ05	Gebruikers kunnen uniek geidentificeerd worden op basis van RIN, UPN of emailadres welke zijn opgenomen in het SAML-token.	1
REQ06	De Access Gateway dient SAML 2.0 te ondersteunen v.w.b. protocols, assertions bindings en profiles.	1
REQ07	De Access Gateway dient ongevoelig te zijn voor DOS-aanvallen.	1
REQ08	De Access Gateway dient PKIoverheid-certificaten te ondersteunen	1
REQ09	De logging moet configureerbaar zijn en kunnen worden getransporteerd naar een SIEM-oplossing.	4
REQ10	De Access Gateway dient een voorziening te hebben voor home-realm discovery.	1
REQ11	De Access Gateway moet ondersteuning hebben voor SAML scoping.	1
REQ12	De gateway dient ondersteuning te bevatten voor Service Provider virtualisatie.	1
REQ13	De Access Gateway moet ondersteuning bieden voor automatische home-realm discovery op basis van cookies.	2

3.4 Aansluitende partij (IdP)

#	Requirement	Prioriteit
REQ01	Eindgebruikers maken gebruik van een ondersteunde browser: Internet Explorer 9+ wanneer zij gebruik maken van de hosted Identity Provider.	1
REQ02	Het VenJ-onderdeel heeft toegang tot het Rijksweb-VPN.	1
REQ03	Het domein Rijksweb.nl is toegevoegd aan de 'Vertrouwde Intranet Sites' in de browser.	4
REQ04	De Internet Explorer security instellingen voor gebruikersauthenticatie moet voor de Intranet Zone op ‘Alleen automatisch aanmelden in Intranet Zone' staan.	4
REQ05	Het VenJ-onderdeel moet een keytab-file aanleveren t.b.v. Kerberos-authenticatie.	1
REQ06	Het VenJ-onderdeel moet de root-certificaten van de user directory aanleveren indien dit geen PKIoverheid is	2

4. Referentiearchitectuur (Logisch ontwerp)

De referentiearchitectuur voor de VenJ Federatieve Dienst 2.0 zal gevormd worden door een federatieve service voor sectorale, sectorale/departementale SP's, externe SP's en externe IdP's. De IdP-Proxy voorziet in een koppeling naar de rijksbrede federatieve koppelvlak. Zie Figuur 1.



Figuur 1: Referentiearchitectuur

5. Fysiek ontwerp

Het nu volgende fysieke ontwerp is een uitwerking van het logisch ontwerp uit het vorige hoofdstuk. Sommige logische componenten laten zich samenvoegen op één hardware-component.

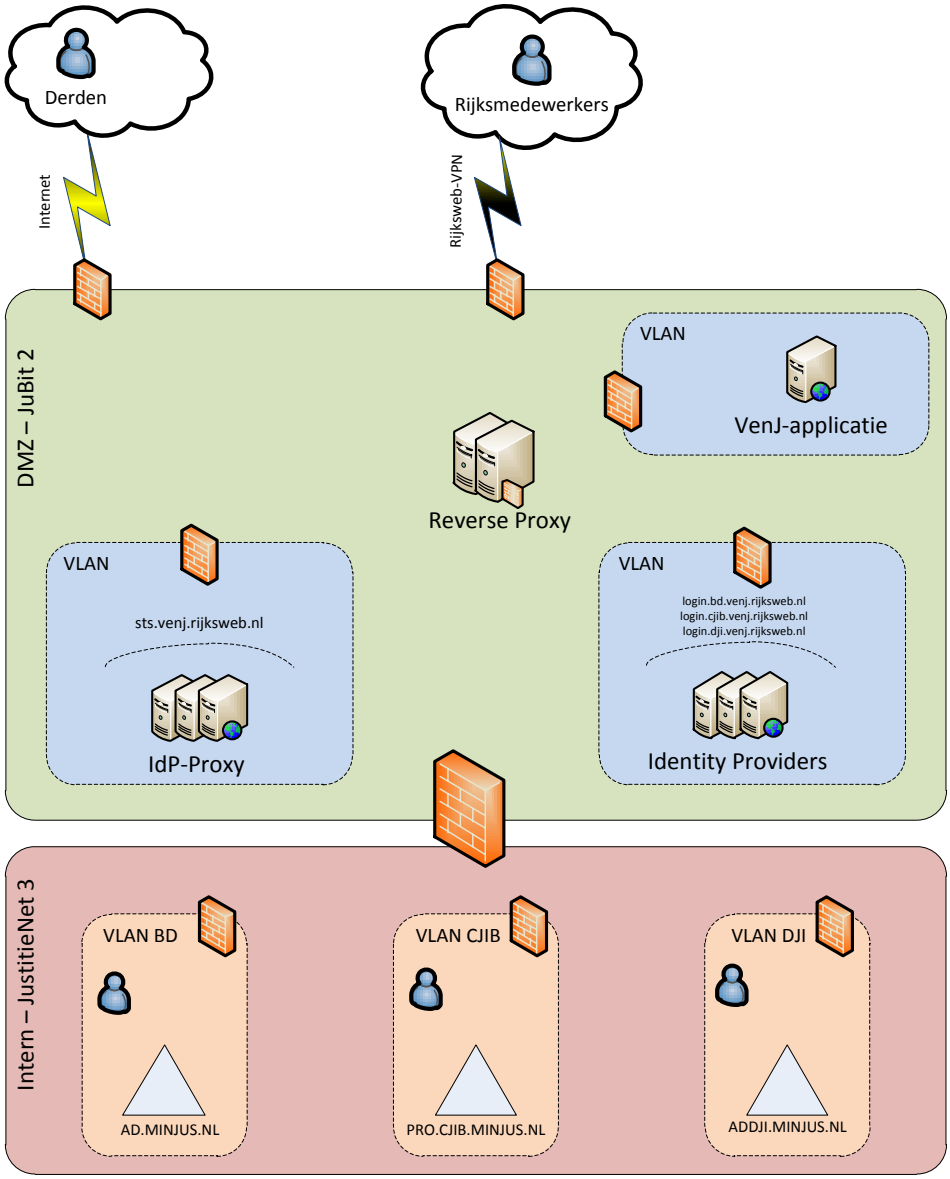
5.1 Hardware

Voor de servers zal gebruik gemaakt worden van de bestaande (gevirtualiseerde) servers. Deze voldoen in de bestaande situatie al aan de daaraan gestelde capaciteitseisen. Voor het faciliteren van beschikbaarheid en schaalbaarheid van de dienst zal gebruik worden gemaakt van de reeds bestaande load balancers.

5.2 Netwerk

In de huidige situatie staat de IdP-Proxy in de DMZ en staan de Identity Providers in het interne netwerk. Met het oog op het toelaten van partijen buiten VenJ, of zelfs buiten de overheid (via internet) is dit een zeer onwenselijke situatie. Door de Identity Providers in de DMZ te plaatsen, blijven eindgebruikers buiten het interne netwerk. Zie Figuur 2 op de volgende pagina voor de nieuwe situatie.

Een bijkomend voordeel van deze opstelling is dat alle Identity Providers kunnen profiteren van failover clustering en loadbalancing. Net als het geval bij de IdP-Proxy zal tenminste één node in een ander datacenter worden geplaatst in het kader van beschikbaarheid.



Figuur 2: Netwerkoverzicht nieuwe situatie

DNS Resolving

Alle componenten dienen zowel van binnen als van buiten het JustitieNet beschikbaar te zijn. Binnen het Justitie-netwerk wordt echter gebruik gemaakt van een split-DNS. Om resolving vanuit alle omgevingen goed te laten werken worden de machines opgenomen in het rijksweb.nl domein. Binnen de DMZ worden ze zodanig opgesteld dat ze onderdeel uitmaken van de "Haagse ring" (Rijksweb).

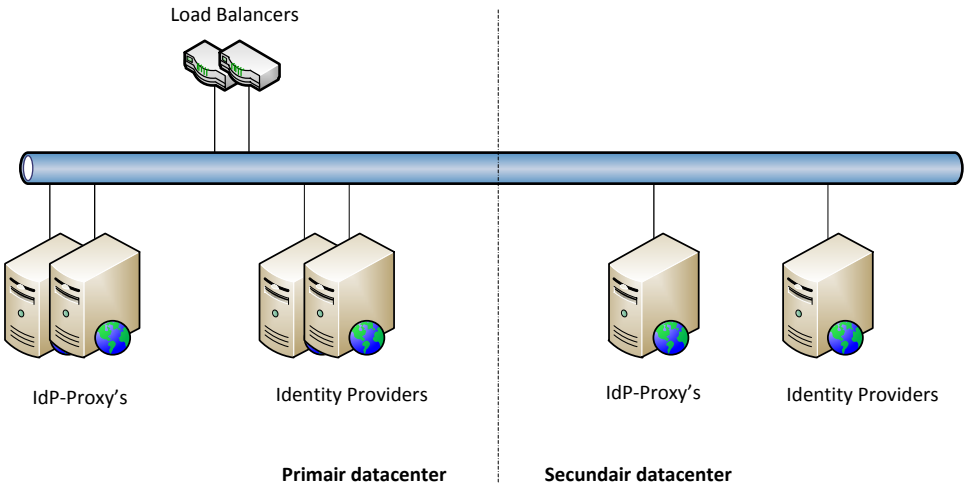
High Availability

De IdP-Proxy en de Identity Providers dienen de authenticatie van tal van applicaties. Uitval van dergelijke systemen zal impact hebben op een gedeelte van of zelfs de gehele gebruikersgroep. Daarnaast speelt dat behalve de VenJ-medewerkers ook medewerkers van ketenpartners van de systemen gebruik maken.

Om die redenen zou de opzet voor de IdP-Proxy als volgt kunnen zijn:

Drie IdP-Proxy's achter minimaal 2 loadbalancers, verdeeld over twee datacenters. De IdP-Proxy's fungeren hierbij als een enkele dienst en nemen het van elkaar over als er een uitvalt. Dit betekent dus ook dat sessie-data gedeeld moet worden over de verschillende nodes.

Voor de Identity Providers kan eenzelfde opzet gebruikt worden.



Figuur 3: High Availability

Bovenstaand figuur is een voorbeeld hoe HA/FT te bereiken zijn met load balancers. Het figuur geeft een voorbeeld weer met 3 nodes. Dit maakt het een high-end voorziening, gezien het belang van de federatieve voorziening. Het aantal nodes van de IdP-Proxy is gelijk aan de huidige situatie, omdat dit volstaat voor het huidige gebruik. Voor de Identity Provider dient het de aanbeveling om minstens een gelijk aantal nodes als de IdP-Proxy te houden, aangezien deze minimaal eenzelfde hoeveelheid verkeer te verwerken krijgt. Het aantal nodes kan eenvoudig uitgebreid worden als de noodzaak daartoe zich aandient.

5.3 IdP-Proxy

De IdP-Proxy zal worden ingericht op basis van SimpleSAMLphp, een webapplicatie. Dit product bevat een aantal functies die technisch ingeregeld moeten worden:

- Theming; De WAYF-pagina kan aangepast worden naar de wensen van de organisatie. Deze pagina zal moeten worden aangepast naar de Rijks-huisstijl.
- Trusts; De trusts met de verschillende federatieve componenten moeten elk afzonderlijk worden ingeregeld.
- Scoping; Per Service Provider kan desgewenst ingesteld worden bij welke Identity Provider er kan worden geauthentiseerd.
- SAML-signing; Met behulp van een PKIoverheid-certificaat kunnen SAML-berichten worden ondertekend om de integriteit van het bericht te kunnen waarborgen.

- Profiling; Per Service Provider kan worden geconfigureerd welke attributen IdP-Proxy mag doorlaten.

Tevens moet op het niveau van het operating system het volgende aangepast worden:

- Een veilige TLS-configuratie in de webserver, conform de geldende richtlijnen van het Nationaal Cyber Security Centrum (NCSC).
- Hardening van de webservers en PHP, conform de geldende richtlijnen.

Home Realm Discovery

Voor veel applicaties zal de zogenaamde Service Provider Initiated Sign-on toegepast worden. Dat betekent dat een gebruiker als eerste stap de applicatie probeert te benaderen. De applicatie signaleert dat de gebruiker nog geen valide SAML token heeft en stuurt de gebruiker naar de IdP-Proxy. Op de IdP-Proxy zal vervolgens bepaald moeten worden naar welke Identity Provider de gebruiker gestuurd moet worden voor authenticatie en het verkrijgen van een SAML token. Deze stap wordt ook wel Home Realm Discovery genoemd.

De eis (REQ13) is dat de keuze van de Identity Provider indien mogelijk geautomatiseerd wordt gemaakt op basis van de beschikbare informatie.
Alleen indien er op basis van deze informatie geen keuze gemaakt kan worden, zal de gebruiker gevraagd worden om een keuze te maken.

De selectieschermen zullen drie methodieken ondersteunen voor de Home Realm Discovery:

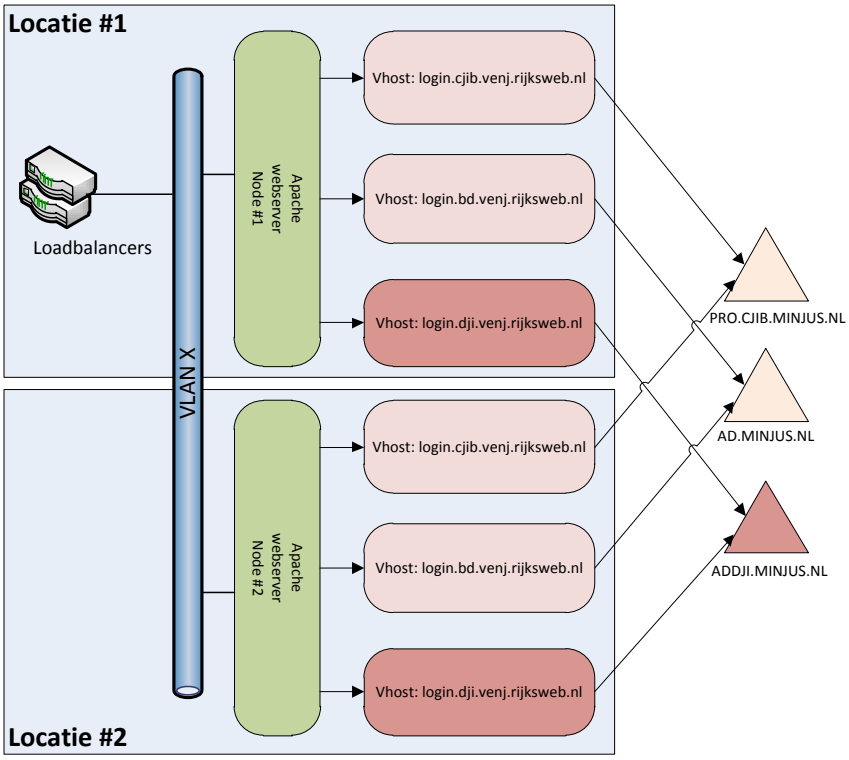
- Handmatige keuze; hierbij selecteert de gebruiker naar welke Identity Provider hij wordt geleid.
- Cookie; na één keer handmatig te hebben geselecteerd wordt de cookie gezet en bij een volgende keer gebruikt om de selectie automatisch te krijgen. Dit kan bijvoorbeeld door een "Onthoud mijn keuze" optie.
- Automatisch; De selectie dient automatich plaats te kunnen vinden op basis van vooraf ingegeven informatie zoals bv een emailadres

Indien een gebruiker een eenmaal opgeslagen keuze voor de Identity Provider ongedaan wil maken kan dit door het verwijderen van de Home Realm cookie. Omdat niet alle gebruikers in de browser interface de autorisatie hebben om cookies weg te gooien, zal er ook een webpagina op de IdP-Proxy worden aangeboden die

het weggooien van de Home Realm cookie voor de gebruiker uitvoert (na bevestiging gevraagd te hebben). Een link naar deze applicatie zal op een centraal punt (bijv. het Rijksweb portaal) worden aangeboden.

5.4 Identity Providers

De Identity Providers worden ingericht op basis van SimpleSAMLphp, een webapplicatie. Dit is in lijn met de huidige situatie. Het verschil met de oude situatie is dat de verschillende losse machines 'gestapeld' worden tot één multi-tenant Identity Provider (cluster) wat conform een eenduidige standaard wordt ingericht. Dit komt tegemoet aan de wens om het beheer eenvoudiger en eenduidiger te maken en realiseert eveneens een kostenbesparing. Ook kunnen de Identity Providers die in de huidige situatie enkelvoudig zijn uitgevoerd in de nieuwe situatie profiteren van failover clustering en loadbalancing. Zie onderstaande afbeelding.



Figuur 4: Multi-tenant inrichting

De technische functionaliteiten die ingericht moeten worden op de Identity Providers zijn:

- -Theming; De login-pagina kan aangepast worden naar de wensen van de organisatie. Deze pagina zal moeten worden aangepast naar de huisstijl van het betreffende VenJ-onderdeel.
- - Trusts; De trusts met de IdP-Proxy moet worden ingeregeld. Ook wordt hier de opbouw van de SAML-tokens gedefinieerd.

- SAML-signing; Met behulp van een PKIoverheid-certificaat kunnen SAML-berichten worden ondertekend om de integriteit van het bericht te kunnen waarborgen.
- Profiling; Per Identity Provider kan worden geconfigureerd welke attributen er uit de achterliggende user directory worden opgehaald.

Tevens moet op het niveau van het operating system het volgende aangepast worden:

- Een veilige TLS-configuratie in de webserver, conform de geldende richtlijnen van het Nationaal Cyber Security Centrum (NCSC).
- Hardening van de webservers en PHP, conform de geldende richtlijnen.

5.5 Access Gateway

De Access Gateway is alleen van belang voor Fase 3 van het doorontwikkelingsproject en valt vooralsnog buiten scope. De bestaande omgeving zal in stand gehouden worden zolang hier geen besluit over genomen wordt.

De IDP Proxy en de centrale Access Management Gateway dienen beide van buiten het justitienetwerk en van binnenuit beschikbaar te zijn.
Binnen justitie is echter een split DNS actief. Om de resolving goed te laten werken worden beide machines opgenomen in het rijksweb.nl domein. Binnen JuBIT worden ze zodanig opgesteld dat ze onderdeel uitmaken van de haagse ring.
Dit geldt echter ook voor de sector gebaseerde IDP. Deze wordt als publieke resources achter de centrale AG geplaatst.

5.6 SAML 2.0

SAML is vastgesteld als rijksbrede standaard welke voorziet in een generiek mechanisme voor authenticatie en autorisatie. Hierbij wordt gebruik gemaakt van SAML-profielen voor het standaardiseren van het berichtenverkeer.

Voor een profiel zijn de volgende zaken verder vorm te geven:

- Een keuze voor initiatie aan de zijde van de vragende partij (SP initiated) of leverancier (IdP initiated);
- De binding voor transport van berichten;
- De wijze waarmee een sessie gestalte krijgt en weer beëindigd wordt: inloggen, single sign on en het uitloggen;
- De character-set en encoding;
- De attributen;

Een SAML-token kent een bepaalde levensduur. Een nadere vaststelling hiervan is nodig. Single Sign-on bewerkstelligt een levensduur die meerdere sessies overstijgt. Voor strikte beveiliging is een levensduur per sessie of per activiteit noodzakelijk. Vaststelling en versiebeheer van het profiel is nader vorm te geven.

Om het federeren vorm te geven zal in de voorbereiding van realisatie ook afspraken moeten worden gemaakt over de te gebruiken SAML-attributen.
Op rijksbreed niveau is vastgesteld welke attributen een gebruiker uniek kunnen identificeren.

Metadata

De metadata van een federatieve koppeling bevat alle relevante gegevens om de koppeling (trust) tot stand te kunnen brengen. Per protocol (SAML, Liberty) worden hier de gegevens opgenomen voor bijvoorbeeld:

- Gebruikte certificaten
- URL voor Single Logout
- URL voor Single Sign-On
- Trusted relation
- Redirect URL's
- URL voor artifact resolution

Op basis van deze metadata weten de IdP en SP onderling aan welke URL's zij hun verzoek tot authenticatie, federatie, etc. moeten richten.

5.7 X509-certificaten

Voor zowel het transport (HTTPS), SAML-signing (en wellicht toekomstig SAML-encryption) is het gebruik van PKIoverheid-certificaten een vereiste, zoals vastgesteld in de BIR-2012. Deze certificaten dienen een private key van tenminste 2048 bits te hebben.

Voor de verbindingen naar achterliggende user directories (intern VenJ) volstaat het gebruik van interne PKI-certificaten. Het gebruik van self-signed certificaten is niet toegestaan.

6. Ontwerpbeslissingen

Voor het invullen van de techniek kiest VenJ er voor om een centrale faciliteit te realiseren bestaande uit een intern en extern koppelvlak, om de volgende redenen:

1. Past het beste bij de structuur en opzet van JustitieNet en voorkomt daarmee potentiële problemen / risico's die zouden ontstaan als alle sectoren zelf aan de slag zouden moeten gaan;
2. Draagt zorg voor gecontroleerde benadering en beveiliging;
3. De rijksbrede federatieve dienst eist in de aansluitvoorwaarden dat een departement zich representeert als één stelsel en met één gezicht;
4. Presentatie van de VenJ federatieve dienst met één gezicht richting externe partijen.

Daarnaast kan een centrale voorziening diensten bieden als:

1. Een controlepunt voor autorisatie en toegang(regels) (Policy decision en Policy Enforcement);
2. Het toevoegen van benodigde attributen;
3. Een filter ter voorkoming van het versturen autorisatiegegevens exclusief voor intern gebruik;
4. Protocolconversie.

De te implementeren oplossing zal de in de vorige hoofdstukken en in het document "Functionele Specificaties" v1.0 beschreven requirements en functionaliteiten moeten bieden. Tevens dient verder uitgewerkt te worden in het architectuurforum met welk SAML-profiel er wordt gewerkt. Technisch zijn de mogelijkheden vrijwel onbeperkt, maar uit oogpunt van beheerbaarheid is het wenselijk om te kijken of er op één "Rijksoverheids-profiel" gestandaardiseerd kan worden.

Bijlagen

De volgende bijlagen maken deel uit van technisch ontwerp - Doorontwikkeling Federatieve Service:

- Bijlage 1: Installatiehandleiding: IdP-Proxy op basis van SimpleSAMLphp
- Bijlage 2: Installatiehandleiding: Multi-tenant Identity Provider op basis van SimpleSAMLphp

Bijlage 1 – Installatiehandleiding – Multi-tenant inrichting Identity Provider

SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Installatiehandleiding

Multi-tentant inrichting Identity Provider o.b.v. SimpleSAMLphp

Versie 1.0

Datum	29 november 2015
Status	Definitief

Colofon

Afzendgegevens	**DG Organisatie Bedrijfsvoering Rijk** SSC-ICT Haaglanden Pijler 2 SSC-ICT/BH/IAM Luxemburglaan 2 2711 BC Zoetermeer Postbus 7385 2701 AJ Zoetermeer
Contactpersoon	Dijen, T. van *Applicatiebeheerder* T 079 330 22 00 F 079 330 22 22
Projectnaam	VenJ Federatieve Service
Ons kenmerk	SSC-ICT/BH/IAM
Auteurs	T. van Dijen
Reviewers	G. Grabner

Inhoudsopgave

1. Inleiding

Dit document is bedoeld als technische blauwdruk voor het inrichten van een multi-tenant IdP op basis van het open-source pakket SimpleSAMLphp. De scope van dit document is uitdrukkelijk beperkt tot klaarmaken van een omgeving voor het gebruik van meerdere Identity Providers op één HA-cluster. Overige zaken zoals projectaanpak e.d. vallen buiten de scope van dit document.

Voor het inrichtingen van een nieuwe multi-tenant IdP doorloopt u het hele document. Voor het toevoegen van een nieuwe IdP aan een bestaande multi-tenant IdP begint u bij hoofdstuk 3.

Alle handelingen beschreven in dit document dienen op alle nodes van het HA-cluster te worden uitgevoerd, zodat alle nodes identiek zijn.

Bij het schrijven van dit document is uitgegaan van de volgende software:

- Red Hat Enterprise Linux 6.6
- SimpleSAMLphp 1.13.2
- Apache 2.2.15
- PHP 5.3.3
- PHP Kerberos-module 1.0.0
- Kerberos 5
- Active Directory als authenticatiebron

2. Multi-tenant inrichting

Dit hoofdstuk beschrijft de voorbereidende handelingen die noodzakelijk zijn voor het opzetten van een multi-tenant IdP. De inrichting van een nieuwe IdP (tenant) wordt beschreven in het volgende hoofdstuk.

2.1 Voorbereidingen

Voordat begonnen kan worden met de installatie is het noodzakelijk dat SSC-ICT Haaglanden / IAM een aantal voorbereidende handelingen verricht. Deze handelingen worden hieronder beschreven.

Leonardo-code

Aangenomen dat er een getekende offerte is, dient er ook een Leonardo-code te zijn waarop gemaakte uren en server(s) kunnen worden geboekt.

Server(s)

Afhankelijk van de grootte van de omgeving dient er een aanvraag te worden gedaan voor een aantal 'Linux Virtueel Middel' servers. Uitgegaan wordt van een omgeving met tenminste twee servers. De servers dienen samen in een apart VLAN geplaatst te worden.

De aanvraag kan worden gedaan via het Topdesk Selfservice Portaal o.v.v. de in paragraaf 2.1.1 verkregen Leonardo-code. Zodra er gegevens bekend zijn van de servers dienen deze vastgelegd te worden in het document 'FS – Overzicht servers + connecties.xlsx'.

Load Balancer

De servers moeten als één systeem naar de buitenwereld reageren. Hiervoor dient een Load Balancer pool te worden aangemaakt. Dien hiertoe een aanvraag in middels het het Topdesk Selfservice Portaal, voorzien van de in paragraaf 2.1.2 verkregen IP-adressen van de afzonderlijke machines.

Uit de aanvraag komt een Load Balancer IP terug welke vastgelegd dient te worden in het document 'FS – Overzicht servers + connecties.xlsx'.

Firewall-changes

Voor een juiste werking van de IdP is het noodzakelijk dat deze conform het Technisch Ontwerp benaderbaar is op poort 443 en verbinding naar buiten kan maken op poort 636.

Dien hiertoe een aanvraag in middels het Topdesk Selfservice Portaal, waarin je vermeld dat het VLAN (verkregen in paragraaf 2.1.2) naar binnen toe opengesteld dient te worden voor poort 443 vanaf JustitieNet + Rijksweb en naar buiten toe op poort 636 naar JustitieNet.

Tevens is het noodzakelijk om een firewall-change uit te laten voeren in de DMZ zodat de Centrale JuBit Proxy verbinding kan maken met de betreffende IdP.

Van Bluecoat proxies naar <Load Balancer IP> HTTPS port TCP 443

Van Bluecoat proxies naar <Load Balancer IP> HTTPS port TCP 443

Ook hiervoor dient een aanvraag te worden ingediend middels het het Topdesk Selfservice Portaal, voorzien van de bovenstaande rules en aangevuld met het Load Balancer IP uit de vorige paragraaf.

2.2 OS & Packages

Voordat de installatie kan beginnen is het van belang dat enkele zaken op het gebied van het Operating System worden geregeld. Deze punten worden hieronder beschreven.

Systeemuser

Er dient een nieuwe systeemuser met de naam 'saml' gemaakt te worden:

```
adduser --system –no-create-home -u 6261 -c "IAM applicatie gebruiker"
usermod –m –d /apps saml
```

Red Hat packages

De volgende packages moeten worden geïnstalleerd:

```
yum install httpd mod_ssl php php-ldap php-mcrypt php-xml php-devel krb5-
devel.x86_64 nano openldap-clients php-pecl-memcache memcached
```

File System

De volgende mappen moeten worden aangemaakt:

```
mkdir /apps
mkdir /apps/sources
mkdir /apps/log
mkdir /apps/log/httpd
mkdir /apps/log/simplesamlphp
chmod –R 755 /apps
chown -R saml:saml /apps
chown saml:apache /apps/log/simplesamlphp
```

Automatisch opstarten services

```
chkconfig httpd on
chkconfig memcached on
```

Kerberos configuratie

Edit /etc/krb5.ini en voeg onder `[libdefaults]` toe:
`rdns = false`

Maak een melding aan in Topdesk voor O&I/Linux met het verzoek deze file te beschermen tegen automatisch overschrijven door RedHat Satellite Server.

Klaarzetten sources

Download de laatste versie van de volgende software:

- https://simplesamlphp.org/download
- https://pecl.php.net/package/krb5

Zet de gedownloade bestanden klaar in `/apps/sources`.
Kopieer tevens de huisstijl en certificaten `/apps/sources`.

Uitpakken SimpleSAMLphp

NB.: De commando's uit deze paragraaf dienen te worden uitgevoerd onder de saml-user!

Pak het eerder gedownloade pakket uit naar de installatiedirectory:

```
cd /apps/sources
tar -xzf /apps/sources/simplesamlphp-1.13.2.tar.gz
```

Taalgebruik

SimpleSAMLphp is een applicatie welke zijn oorsprong vindt in het Hoger Onderwijs. Dit klinkt door in het taalgebruik binnen de applicatie, wat niet door alle eindgebruikers gewaardeerd kan worden. Een voorbeeld hiervan is de melding "Vette pech" wanneer een verkeerd wachtwoord wordt ingevoerd. Het strekt dan ook de aanbeveling om deze krachtterm te verwijderen en ook de rest van het taalbestanden na te lopen op ongewenst taalgebruik. Deze taalbestanden kunnen gevonden worden in: `/apps/simplesamlphp/dictionaries`

Compileren Kerberos-module voor PHP

Compileer de Kerberos-module:

```
tar xvfz /apps/sources/krb5-1.0.0.tgz -C /apps/sources
cd /apps/sources/krb5-1.0.0
phpize
./configure
make && make install
mv /apps/sources/krb5-1.0.0/modules/krb5.so /usr/lib64/php/modules
rm -rf /apps/sources/krb5-1.0.0
```

Maak de file /etc/php.d/krb5.ini aan en vul deze met:

```
; Enable krb5 extension module
extension=krb5.so
```

SELinux

SELinux hoort standaard aan te staan op machines in de JuBit DMZ. Indien dit toch niet het geval is dient dit ingeschakeld te worden:

```
setenforce 1

semanage fcontext –f –l -a -t http_sys_content_t "/apps/simplesamlphp(/.*)?"
semanage fcontext -a -t httpd_log_t "/apps/logs(/.*)?".
semanage fcontext -a -t httpd_cache_t "/var/cache(/.*)?"

restorecon -Rv /apps/simplesamlphp
restorecon -Rv /apps/logs
restorecon -Rv /var/cache
```

OpenLDAP configuratie

Edit /etc/openldap/ldap.conf en maak de volgende wijzigingen:

```
TLS_CACERTDIR /etc/openldap/certs
TLS_REQCERT     allow
```

2.3 Configuratie Apache & PHP

Voordat de installatie kan beginnen is noodzakelijk dat een aantal zaken rondom de webserver worden geregeld. Deze punten worden hieronder beschreven.

Apache algemene configuratie

De volgende settings dienen te worden aangepast in `/etc/httpd/conf/httpd.conf` . De instellingen zijn bedoeld voor een juiste werking ofwel in het kader van hardening. De wijzigingen ten opzichte van de standaardinstellingen zijn onderstreept.

```
#LoadModule include_module modules/mod_include.so
#LoadModule env_module modules/mod_env.so
#LoadModule ext_filter_module modules/mod_ext_filter.so
#LoadModule status_module modules/mod_status.so
#LoadModule actions_module modules/mod_actions.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule cgi_module modules/mod_cgi.so
#LoadModule version_module modules/mod_version.so

#Listen 80

ServerTokens Prod
ServerSignature Off
TraceEnable Off

LimitRequestFieldSize 16380
```

Opmerking [TvD1]: Organisaties die veel geneste groepen hebben in AD krijgen hele lange Kerberos-tokens, wat resulteert in een HTTP/400 Bad Request. De default-waarde voor dit veld is 8190

Vervangen standaard SSL-configuratie

Archiveer de volgende file:

```
mv /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf.bak
```

Maak een nieuwe file aan voor de SSL-configuratie:

```
/etc/httpd/conf.d/ssl.conf
```

Vul de file met de volgende inhoud:

```
# This is the Apache server configuration file providing SSL support.
# It contains the configuration directives to instruct the server how to
# serve pages over an https connection. For detailing information about these
# directives see <URL:http://httpd.apache.org/docs/2.2/mod/mod_ssl.html>
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#

LoadModule ssl_module modules/mod_ssl.so
#
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
```

```
Listen 443
SSLEngine On

##
##  SSL Global Context
##
##  All SSL configuration in this context applies both to
##  the main server and all SSL-enabled virtual hosts.
##

#   Pass Phrase Dialog:
#   Configure the pass phrase gathering process.
#   The filtering dialog program (`builtin' is a internal
#   terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog  builtin

#   Inter-Process Session Cache:
#   Configure the SSL Session Cache: First the mechanism
#   to use and second the expiring timeout (in seconds).
SSLSessionCache         shmcb:/var/cache/mod_ssl/scache(512000)
SSLSessionCacheTimeout  300

#   Semaphore:
#   Configure the path to the mutual exclusion semaphore the
#   SSL engine uses internally for inter-process synchronization.
SSLMutex default

#   Pseudo Random Number Generator (PRNG):
#   Configure one or more sources to seed the PRNG of the
#   SSL library. The seed data should be of good random quality.
#   WARNING! On some platforms /dev/random blocks if not enough entropy
#   is available. This means you then cannot use the /dev/random device
#   because it would lead to very long connection times (as long as
#   it requires to make more entropy available). But usually those
#   platforms additionally provide a /dev/urandom device which doesn't
#   block. So, if available, use this one instead. Read the mod_ssl User
#   Manual for more details.
SSLRandomSeed startup file:/dev/urandom  256
SSLRandomSeed connect builtin
#SSLRandomSeed startup file:/dev/random  512
#SSLRandomSeed connect file:/dev/random  512
#SSLRandomSeed connect file:/dev/urandom 512

#
# Use "SSLCryptoDevice" to enable any supported hardware
# accelerators. Use "openssl engine -v" to list supported
# engine names.  NOTE: If you enable an accelerator and the
# server does not start, consult the error logs and ensure
# your accelerator is functioning properly.
#
SSLCryptoDevice builtin
#SSLCryptoDevice ubsec

SSLProtocol all -SSLv2 -SSLv3
```

```
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:kEDH+AESGCM:
ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-
SHA:!aNULL:!eNULL:!DHE:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

SSLHonorCipherOrder On
SSLCompression Off
```

PHP-configuratie

De volgende settings dienen te worden aangepast in `/etc/php.ini` voor een juiste werking ofwel in het kader van hardening. De wijzigingen ten opzichte van de standaardinstellingen zijn onderstreept.

```
expose_php = Off
display_errors = Off
html_errors = Off
allow_url_fopen = Off
session.cookie_secure = 1
session.cookie_httponly = 1
date.timezone = Europe/Amsterdam
```

Herstarten Apache

Herstart Apache om de wijzigingen uit deze paragraaf te activeren:
`service httpd restart`

3. Toevoegen Identity Provider

In het vorige hoofdstuk is het systeem voorbereid op een multi-tenant inrichting. Het nu volgende hoofdstuk beschrijft het toevoegen van een nieuwe Identity Provider (tenant).

3.1 Voorbereidingen door SSC-ICT Haaglanden

Voordat begonnen kan worden met de installatie is het noodzakelijk dat SSC-ICT Haaglanden een aantal voorbereidende handelingen verricht. Deze handelingen worden hieronder beschreven. Parallel aan deze handelingen kunnen de handelingen uit paragraaf 3.2 worden uitgevoerd.

Leonardo-code

Aangenomen dat er een getekende offerte is, dient er ook een Leonardo-code te zijn waarop gemaakte uren kunnen worden geboekt.

Rijksweb-IP + DNS

Middels het Topdesk Selfservice Portaal kan een aanvraag worden ingediend voor een Rijksweb-IP en bijbehorende DNS-record. De DNS-naam dient conform het Technisch Ontwerp in het volgende formaat te worden gedefinieerd:
`login.<VenJ-onderdeel>.<tstvenj | accvenj | venj>.rijksweb.nl`

Voorbeeld:
`login.cjib.accvenj.rijksweb.nl`

Deze DNS-naam moet voor JustitieNet-gebruikers benaderbaar zijn op het interne IP-adres. Vermeld dit duidelijk in de aanvraag en vernoem ook het in paragraaf 2.1 vergaarde Load Balancer IP!

Neem de gegevens wederom op in het document '*FS - Overzicht servers + connecties.xlsx*'.

PKIoverheid-certificaat + Self-signed certificaat

Voor zowel de HTTPS-verbinding als voor SAML-signing moet, conform BIR en Technisch Ontwerp, een PKIoverheid-certificaat gebruikt worden volgens het SHA256 algoritme en met een private key van tenminste 2048 bits.

Beide certificaten kunnen worden aangevraagd/gegenereerd middels het document *Werkinstructie FS - Aanmaken (PKIo-)certificaten.docx*.

NB.: De certificaten zijn per omgeving gelijk. Dit betekent dat de certificaten op één van de nodes gegenereerd worden en daarna gekopieerd naar de overige nodes.

3.2 Voorbereidingen door VenJ-onderdeel

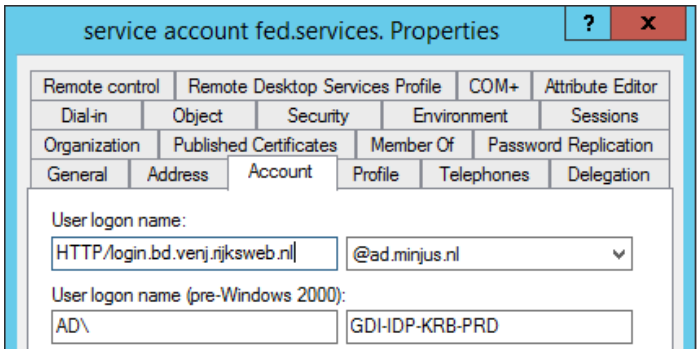
Voordat begonnen kan worden met de installatie is het van belang dat het aan te sluiten VenJ-onderdeel een aantal handelingen uitvoert. Deze handelingen worden hieronder beschreven.

Systeemusers

Er dienen een drietal systeemusers aangemaakt te worden binnen het domein van het aan te sluiten VenJ-onderdeel. Het betreft een user-account ten behoeve van LDAPS-authenticatie, een account ten behoeve van Kerberos-authenticatie en een account waarmee de beheerders van de VenJ Federatieve Service de werking van de Federatieve keten kunnen testen.

Het Kerberos-account moet een ServicePrincipalName hebben in het formaat:
`HTTP/<DNS-NAME>`

Voorbeeld:



Genereren keytab-file

Er dient een keytab-file gegenereerd te worden op een willekeurige Windows-server binnen het domein van het aan te sluiten VenJ-onderdeel. Het juiste commando hiervoor is als volgt:

```
ktpass /out c:\<DNS-NAME>.keytab /princ <SPN-van-Kerberos-user>@<Kerberos-realm> /mapuser <DOMEIN\sAMAccountName-van-Kerberos-user> /mapop set /pass * /crypto ALL /ptype KRB5_NT_PRINCIPAL /kvno 0
```

Voorbeeld:

```
ktpass /out c:\login.bd.venj.rijksweb.nl.keytab /princ HTTP/login.bd.venj.rijksweb.nl@AD.MINJUS.NL /mapuser AD\BD-IDP-KRB-PRD /mapop set /pass * /crypto ALL /ptype KRB5_NT_PRINCIPAL /kvno 0
```

Browser-settings

Voor de Single Sign-On-functionaliteit is het noodzakelijk om de DNS-naam uit paragraaf 2.1 toe te voegen aan de 'Vertrouwde websites' van de webbrowser. De browser zal dan een Kerberos-token meesturen om de authenticatie mee uit te voeren. Als deze stap niet wordt uitgevoerd zal de gebruiker elke keer een username + wachtwoord moeten invoeren wanneer gebruik gemaakt wordt van de IdP.

Firewall-change

Voor een juiste werking is het noodzakelijk dat de IdP de Active Directory van het VenJ-onderdeel kan benaderen. Hiervoor dient het VenJ-onderdeel poort 636 (LDAPS) open te stellen voor de/het IP-adres(sen) uit paragraaf 2.1.

Huisstijl

Standaard wordt een IdP voorzien van de algemene Justitie-huisstijl. Het is echter wenselijk om de IdP herkenbaar te maken als IdP voor het specifieke VenJ-onderdeel.

Dit kan door een kopie te maken van de huisstijl-module en hierin het logo van het VenJ-onderdeel toe te voegen aan de `www` directory en de padverwijzing in het bestand `themes/justitie/default/includes/header.php` aan te passen:

```
cp –R /apps/simplesamlphp/modules/themejustitie
/apps/simplesamlphp/modules/theme-<VenJ-onderdeel>
```

3.3 Operating System

Voordat de installatie kan beginnen is het van belang dat enkele zaken op het gebied van het Operating System worden geregeld. Deze punten worden hieronder beschreven.

File System

Maak een kopie van de SimpleSAMLphp-source:

```
cp –R /apps/sources/simplesamlphp-1.13.2 /apps/tenants/simplesamlphp-1.13.2-
<VenJ-onderdeel>
```

De volgende mappen moeten worden aangemaakt:

```
mkdir /etc/openldap/certs/<VenJ-onderdeel>
mkdir /apps/simplesamlphp-<VenJ-onderdeel>/cert
```

Ga naar de `/apps` directory en maak de volgende symlink aan:

```
cd /apps
ln –s /apps/tenants/simplesamlphp-1.13.2-<VenJ-onderdeel> simplesamlphp-
<VenJ-onderdeel>
```

Maak een kopie van de volgende mappen:

```
cp –R config-templates config
cp –R metadata-templates metadata
```

Kerberos configuratie

Edit /etc/krb5.ini:

```
rdns = false
```

Opmerking [TvD2]: Mogelijk is dit overbodig als de /etc/hosts file correct wordt aangepast. Zie paragraaf 2.3.10

Voeg onder `[realms]` een nieuwe Kerberos-realm toe voor het domein waar de IdP voor gaat authentiseren:

```
<DOMEINNAAM-IN-HOOFDLETTERS> = {
  kdc = <hostnaam-van-domeincontroller>
}
```

Voeg ook twee entries toe onder `[domain_realm]` volgens het stramien van de reeds gedefinieerde AD.MINJUS.NL realm.

Voorbeeld:

```
[realms]
 PRO.CJIB.MINJUS.NL = {
  kdc = cjibka0003.pro.cjib.minjus.nl
 }

[domain_realm]
 pro.cjib.minjus.nl = PRO.CJIB.MINJUS.NL
 .pro.cjib.minjus.nl = PRO.CJIB.MINJUS.NL
```

Klaarzetten certificaten, private keys en keytab

De in hoofdstuk 2 verkregen certificaten, keys en keytab moeten op de juiste locatie worden neergezet. Het PKIoverheid-certificaat en de bijbehorende private key worden in de volgende twee directories gezet:
`/etc/httpd/ssl`
`/apps/simplesamlphp-<VenJ-onderdeel>/cert`

Stel de rechten in op de private key in `/etc/httpd/ssl` en verwijder het wachtwoord:

```
cd /etc/httpd/ssl
chmod 400 <DNS-naam>.key
openssl rsa –in <DNS-naam>.key –out <DNS-naam>.key

cd /apps/simplesamlphp-<VenJ-onderdeel>/cert
chmod 400 <DNS-NAAM>.key
```

Kopieer het bestand rijksweb-chain.crt naar /apps/simplesamlphp/cert:
`cp /apps/sources/rijksweb-chain.crt /apps/simplesamlphp-<VenJ-onderdeel>/cert`

Kopieer het bestand met de certificate-chain van de domain controller naar /etc/openldap/certs:
`cp /apps/sources/dc-chain.crt /etc/openldap/certs`

Zet tot slot het signing-certificaat, de bijbehorende private key en de keytab in de directory `/apps/simplesamlphp-<VenJ-onderdeel>/cert`

Enablen Negotiate-module

Schakel de Negotiate-module in middels het volgende commando:
`touch /apps/simplesamlphp-<VenJ-onderdeel>/modules/negotiate/enable`

OpenLDAP configuratie

`Lees de geplaatste certificaten in de certificatentabel in:`
`/usr/sbin/cacertdir_rehash /etc/openldap/certs`

/etc/hosts file

Pas de file `/etc/hosts` aan zodat er een verwijzing op hostnaam naar de nieuwe IdP in staat. Dit is noodzakelijk voor de juiste werking van Kerberos-module.

Voorbeeld:
`10.42.101.35  login.bd.accvenj.rijksweb.nl`

3.4 Configuratie Apache

In paragraaf 2.3 is de webserver al voorbereid op een multi-tenant structuur. In deze paragraaf wordt de configuratie van de nieuwe tenant (IdP) uitgevoerd.

VirtualHost-configuratie

Maak een nieuwe file aan voor de HTTP-verbindingen:
`/etc/httpd/conf.d/<VenJ-onderdeel>.conf`

Vul de file met de volgende inhoud van de volgende pagina:

```
<VirtualHost *:443>
    ServerName <RIJKSWEB-DNS-NAME>

    ServerAdmin <ADMIN-EMAIL>
    DocumentRoot /apps/simplesamlphp-<VenJ-onderdeel>/www

    SSLCertificateFile /etc/httpd/ssl/<RIJKSWEB-DNS-NAME>.crt
    SSLCertificateKeyFile /etc/httpd/ssl/<RIJKSWEB-DNS-NAME>.key
    SSLCertificateChainFile /etc/httpd/ssl/rijksweb-chain.crt

    ErrorLog /apps/log/httpd/<VenJ-onderdeel>-error.log
    CustomLog /apps/log/httpd/<VenJ-onderdeel>-access.log common

    RewriteEngine on

    RewriteCond %{THE_REQUEST} !HTTP/1.1$
    RewriteRule .* - [F]

    RewriteCond %{HTTP:Authorization}  !^$
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization},L]

    <Location />
       Order deny,allow
       Deny from all
       Allow from 127.0.0.0/8
       Allow from ::1/128
       Allow from <ADMIN-NETWORK>
    </Location>

    <Location /login.php>
       Allow from all
    </Location>

    <Location /resources>
       Allow from all
    </Location>

    <Location /saml2>
       Allow from all
    </Location>

    <Location /module.php/core/loginuserpass.php>
       Allow from all
    </Location>

    <Location /module.php/core/idp>
       Allow from all
    </Location>

    <Location /module.php/negotiate/backend.php>
       Allow from all
    </Location>
</VirtualHost>
```

Herstarten Apache

Herstart Apache om de wijzigingen uit deze paragraaf te activeren:
`service httpd restart`

3.5 Configuratie SimpleSAMLphp

Deze paragraaf beschrijft de configuratie van SimpleSAMLphp. De verschillende componenten die aangepast dienen te worden, worden hieronder beschreven.

SimpleSAMLphp algemene configuratie

Genereer alvast een password-hash d.m.v. het volgende commando:
`/apps/simplesamlphp/bin/pwgen.php`

Kies een wachtwoord voor de beheerinterface van SimpleSAMLphp, gebruik een sterk hashing algoritme [sha256] en gebruik een salt [yes].

Genereer ook alvast een secret salt:
`tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo`

Open nu de file `/apps/simplesamlphp-<VenJ-onderdeel>/config/config.php` en pas de volgende settings aan voor een juiste werking dan wel in het kader van hardening. De wijzigingen ten opzichte van de standaardinstellingen zijn onderstreept.

```
'loggingdir' => '/apps/log/simplesamlphp/',
'auth.adminpassword' => '<PASSWORD-HASH>',
'admin.protectindexpage' => true,
'secretsalt' => '<SECRET-SALT>',
'technicalcontact_name' => '<ADMIN-NAME>',
'technicalcontact_email' => '<ADMIN-EMAIL>',
'timezone' => 'Europe/Amsterdam',
'logging.handler' => 'file',
'enable.saml20-idp' => true,
'session.cookie.secure' => true,
'session.phpsession.httponly' => true,
'language.available' => array('en', 'nl'),
'language.rtl' => array(),
'language.default' => 'nl',
'theme.use' => 'themejustitie:justitie'
'store.type' => 'memcache',
'memcache_store.servers' => array(
    array(
        array('hostname' => '<NODE-1-FQDN>'),
    ),
    array(
        array('hostname' => '<NODE-2-FQDN>'),
    ),
    array(
        array('hostname' => '<NODE-3-FQDN>'),
    ),
),
```

Opmerking [TVD3]: Wanneer in paragraaf 3.2 een nieuwe thema-module gemaakt is, dan dient die hier ingevuld te worden i.p.v. de default Justitie-theme

Configureren authenticatiebronnen

Archiveer de file /apps/simplesamlphp/config/authsources.php:

```
mv /apps/simplesamlphp-<VenJ-onderdeel>/config/authsources.php
/apps/simplesamlphp-<VenJ-onderdeel>/config/authsources.php.bak
```

Maak vervolgens een nieuwe file aan met de volgende inhoud:

NB.: De onderstreepte delen vereisen aanpassing.

```
<?php

$config = array(

        // This is a authentication source which handles admin
authentication.
        'admin' => array(
                // The default is to use core:AdminPassword, but it can be
replaced with
                // any authentication source.

                'core:AdminPassword',
        ),

        'AD-KERBEROS' => array(
             'negotiate:Negotiate',
             'keytab' => '/apps/simplesamlphp-<VenJ-onderdeel>/cert/<DNS-
NAAM>.keytab',
             'fallback' => 'AD-LDAP',
             'hostname' => 'ldaps://<FQDN-AD-DOMAIN-CONTROLLER-1>
ldaps://<FQDN-AD-DOMAIN-CONTROLLER-2>',
             'enable_tls' => TRUE,
             'port' => 636,
             'referrals' => FALSE,
             'debugLDAP' => FALSE,
             'timeout' => 3,

             'base' => '<DISTINGUISHED-NAME-ORGANISATIONAL-UNIT>',
             'attr' => 'sAMAccountName',

             'adminUser' => '<DISTINGUISHED-NAME-KERBEROS-USER>',
             'adminPassword' => '<PASSWORD-KERBEROS-USER>',

             'attributes' => array('mail'),
        ),
```

Opmerking [TvD4]: Zal pas daadwerkelijk werken vanaf SSP 1.14

Opmerking [TvD5]: Vanaf SSP 1.14 kan dit een array zijn.

```
'AD-LDAP' => array(
                'ldap:LDAP',

                // Give the user an option to save their username for future
login attempts
                // And when enabled, what should the default be, to save the
username or not
                //'remember.username.enabled' => FALSE,
                //'remember.username.checked' => FALSE,

                // The hostname of the LDAP server.
                'hostname' => 'ldaps://<FQDN-AD-DOMAIN-CONTROLLER-1>
ldaps://<FQDN-AD-DOMAIN-CONTROLLER-2>',

                // The port used when accessing the LDAP server.
                // The default is 389.
                'port' => 636,

                // Whether SSL/TLS should be used when contacting the LDAP
server.
                'enable_tls' => TRUE,

                // Whether debug output from the LDAP library should be
enabled.
                // Default is FALSE.
                'debug' => FALSE,

                // The timeout for accessing the LDAP server, in seconds.
                // The default is 0, which means no timeout.
                'timeout' => 3,

                // Set whether to follow referrals. AD Controllers may
require FALSE to function.
                'referrals' => FALSE,

                // Which attributes should be retrieved from the LDAP server.
                // This can be an array of attribute names, or NULL, in which
case
                // all attributes are fetched.
                'attributes' => array('mail'),

                // The pattern which should be used to create the users DN
given the username.
                // %username% in this pattern will be replaced with the users
username.
                //
                // This option is not used if the search.enable option is set
to TRUE.
                //'dnpattern' =>
'uid=%username%,ou=people,dc=example,dc=org',

                // As an alternative to specifying a pattern for the users
DN, it is possible to
                // search for the username in a set of attributes. This is
enabled by this option.
```

```
                'search.enable' => TRUE,

                // The DN which will be used as a base for the search.
                // This can be a single string, in which case only that DN is
searched, or an
                // array of strings, in which case they will be searched in
the order given.
                'search.base' => array('<DISTINGUISED-NAME-SEARCH-
ORGANISATIONAL-UNIT>'),

                // The attribute(s) the username should match against.
                //
                // This is an array with one or more attribute names. Any of
the attributes in
                // the array may match the value the username.
                'search.attributes' => array('sAMAccountName'),

                // The username & password the simpleSAMLphp should bind to
before searching. If
                // this is left as NULL, no bind will be performed before
searching.
                'search.username' => '<DISTINGUISHED-NAME-LDAPS-USER>',
                'search.password' => '<PASSWORD-LDAPS-USER>',

                // If the directory uses privilege separation,
                // the authenticated user may not be able to retrieve
                // all required attributes, a privileged entity is required
                // to get them. This is enabled with this option.
                'priv.read' => FALSE,

                // The DN & password the simpleSAMLphp should bind to before
                // retrieving attributes. These options are required if
                // 'priv.read' is set to TRUE.
                'priv.username' => NULL,
                'priv.password' => NULL,
        ),

);
```

Metadata configureren

Pas de file `/apps/simplesamlphp-<VenJ-onderdeel>/metadata/saml20-idp-hosted.php` aan met de volgende inhoud:

NB.: De onderstreepte delen vereisen aanpassing.

```
<?php

/**
 * SAML 2.0 IdP configuration for simpleSAMLphp.
 *
 * See: https://rnd.feide.no/content/idp-hosted-metadata-reference
 */
```

```
$metadata['__DYNAMIC:1__'] = array(
        /*
         * The hostname of the server (VHOST) that will use this SAML entity.
         *
         * Can be '__DEFAULT__', to use this entry by default.
         */
        'host' => '__DEFAULT__',

        /* X.509 key and certificate. Relative to the cert directory. */
        'privatekey'    => '<DNS-NAME>_SIGNING.key',
        'certificate'   => '<DNS-NAME>_SIGNING.crt',
        'privatekey_pass' => '<SIGNING-CERTIFICATE-PASSWORD>',

        /*
         * Authentication source to use. Must be one that is configured in
         * 'config/authsources.php'.
         */
        'auth' => 'AD-KERBEROS',
        'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-
format:basic',

        'authproc' => array(
            1 => array(
                'class' => 'saml:TransientNameID',
            ),
            2 => array(
                'class' => 'saml:PersistentNameID',
                'attribute' => 'mail',
            ),
            3 => array(
                'class' => 'saml:AttributeNameID',
                'attribute' => 'mail',
                'Format' => 'urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress',
            ),
            4 => array(
                'class' => 'core:AttributeMap',
                'mail' =>
'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress',
            ),
            5 => array(
                'class' => 'saml:AuthnContextClassRef',
                'AuthnContextClassRef' =>
'urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport',
            ),
        ),

        'signature.algorithm' => 'http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256',
);
```

Koppeling met IdP-Proxy als Service Provider

Vervang de file /apps/simplesamlphp-<VenJ-onderdeel>/metadata/saml20-sp-remote.php met de meegeleverde variant.

4. Verificatie en afronding

De IdP is nu volledig geïnstalleerd en geconfigureerd. De volgende paragraaf beschrijft methoden om de verschillende aspecten van de IdP te testen en de juiste werking te verifiëren.

Beheerinterface

Controleer of de beheerinterface te benaderen is. Open een browser en vul de Rijksweb DNS-naam in. Wanneer http:// gebruikt wordt zou er automatisch omgeschakeld moeten worden naar https://.
De beheerpagina zou er als volgt uit moeten zien:

Als de pagina niet benaderbaar is, controleer dan allereerst of de httpd service gestart is. Wanneer er een '403 Forbidden' foutmelding gegeven wordt, controleer dan of de IP-reeks van het werkstation is opgenomen als *<ADMIN-NETWORK>* in de Apache-configuratie (zie paragraaf 3.4).

Wordt de pagina wél getoond, log dan in met het admin-wachtwoord uit paragraaf 3.5. Ga naar het tabblad configuratie en controleer of alle vinkjes groen zijn, met uitzondering van Shib 1.3 IdP en MySQL-support.

Klik op 'Beschikbare modules' en verifieer dat de 'Negotiate' module is ingeschakeld.

Ga naar het tabblad 'Authenticatie' en test of er ingelogd kan worden met het eigen AD-account voor zowel AD-LDAP als voor AD-KERBEROS. Indien het inloggen niet lukt is er een probleem met de koppeling tussen IdP en de achterliggende Active Directory. Raadpleeg het meegeleverde troubleshooting-document.

Koppeling met IdP-Proxy als Service Provider

Voor een koppeling met de IdP-Proxy is er aan die kant ook de metadata van de IdP nodig. Deze metadata kan worden opgevraagd middels de volgende URL: https://<DNS-naam>/saml2/idp/metadata.php

Ketentest

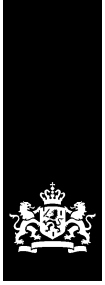
Wanneer de koppeling met de IdP-Proxy is afgerond, moet het mogelijk zijn om volledig gebruik te maken van de VenJ federatie. De keten kan getest worden vanuit twee oogpunten: Vanuit SSOn Rijk (Rijksbrede applicaties zoals P-direkt, Samenwerkruimte) en vanuit de JustID Access Gateway (VenJ-brede applicaties).

SSOn Rijk:
- SSOn-Test Acceptatie
- SSOn-Test Productie

Bij een juiste werking van de keten wordt het volgende scherm getoond:

Het bovenste nummer representeert het SAP-personeelsnummer, wat noodzakelijk is voor Single Sign-on naar P-direkt. LET OP: Dit is **niet** het RIN!

Bijlage 2 – Installatiehandleiding – IdP-Proxy op basis van SimpleSAMLphp



SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Installatiehandleiding SimpleSAMLphp

IdP-Proxy

Versie 1.0

Datum	20 november 2015
Status	Definitief

Colofon

Afzendgegevens	**DG Organisatie Bedrijfsvoering Rijk** SSC-ICT Haaglanden Pijler 2 SSC-ICT/BH/IAM Luxemburglaan 2 2711 BC Zoetermeer Postbus 7385 2701 AJ Zoetermeer
Contactpersoon	Dijen, T. van *Applicatiebeheerder* T 079 330 22 00 F 079 330 22 22
Projectnaam	VenJ Federatieve Service
Ons kenmerk	SSC-ICT/BH/IAM
Auteurs	T. van Dijen
Reviewers	G. Grabner

Inhoudsopgave

1. Inleiding

Dit document is bedoeld als technische blauwdruk voor het inrichten van een IdP-Proxy op basis van het open-source pakket SimpleSAMLphp. De scope van dit document is uitdrukkelijk beperkt tot technische aspecten van de inrichting. Overige zaken zoals projectaanpak e.d. vallen buiten de scope van dit document.

2. Voorbereiding

Dit hoofdstuk beschrijft de voorbereidende handelingen voorafgaande aan de installatie en configuratie van SimpleSAMLphp.

Bij het schrijven van dit document is uitgegaan van de volgende software:
- Red Hat Enterprise Linux 6.6
- SimpleSAMLphp 1.13.2
- Apache 2.2.15
- PHP 5.3.3

Bijlagen bij deze handleiding zijn:
- SimpleSAMLphp Justitie-theme (`themejustitie` directory)
- Access Gateway metadata (`saml20-sp-remote.php` file)
- Rijksweb certificate chain (`rijksweb-chain.crt` file)

Leonardo-code

Aangenomen dat er een getekende offerte is, dient er ook een Leonardo-code te zijn waarop gemaakte uren en server(s) kunnen worden geboekt.

Server(s)

Afhankelijk van of er de IdP-Proxy een enkele of een geclusterde opzet krijgt, dient er een aanvraag gedaan te worden voor een aantal 'Linux Virtueel Middel' servers. De machine(s) dient/dienen in een eigen VLAN geplaatst te worden binnen de JuBit DMZ.

Voor de geclusterde variant dient een extra load balancer IP gereserveerd te worden. Laat hiervoor een extra activiteit aan de wijziging toevoegen voor O&I/Netwerken (IP-adres reserveren).

De aanvraag kan worden gedaan via het Topdesk Selfservice Portaal o.v.v. de in paragraaf 2.1.1 vergaarde Leonardo-code. Zodra er gegevens bekend zijn van de machine(s) dienen deze vastgelegd te worden in het document 'FS – Overzicht servers + connecties.xlsx'.

Rijksweb-IP + DNS

Middels het Topdesk Selfservice Portaal kan een aanvraag worden ingediend voor een Rijksweb-IP en bijbehorende DNS-record. De DNS-naam dient conform het Technisch Ontwerp in het volgende formaat te worden gedefinieerd:
`sts.<tstvenj | accvenj | venj>.rijksweb.nl`

Voorbeeld:
`sts.accvenj.rijksweb.nl`

Deze DNS-naam moet voor JustitieNet-gebruikers benaderbaar zijn op het interne IP-adres (In het geval van een cluster dient hier het load balancer VIP gebruikt te worden). Vermeld dit duidelijk in de aanvraag en vernoem ook het in paragraaf 2.1.2 verkregen interne (V)IP-adres!

Neem de gegevens wederom op in het document 'FS - Overzicht servers + connecties.xlsx'.

Firewall-change

Voor een juiste werking van de IdP-Proxy is het noodzakelijk dat deze conform het Technisch Ontwerp benaderbaar is op poort 443. Dien hiertoe een aanvraag in middels het Topdesk Selfservice Portaal, waarin je vermeld dat het VLAN (verkregen in paragraaf 2.1.2) opengesteld dient te worden op de genoemde poort voor JustitieNet + Rijksweb.

Tevens is het noodzakelijk om een firewall-change uit te laten voeren door ASP4ALL zodat de Centrale JuBit Proxy verbinding kan maken met de IdP-Proxy.

Van Bluecoat proxies naar sts. <tstvenj | accvenj | venj>.rijksweb.nl (Intern (V)IP) HTTPS port TCP 443

Van Bluecoat proxies naar sts. <tstvenj | accvenj | venj>.rijksweb.nl (Intern (V)IP) HTTPS port TCP 443

Ook hiervoor dient een aanvraag te worden ingediend middels het het Topdesk Selfservice Portaal, voorzien van de bovenstaande rules en aangevuld met het interne (cluster-)IP.

PKIoverheid-certificaten

Voor zowel de HTTPS-verbinding als voor SAML-signing moet, conform BIR-2012 en Technisch Ontwerp, een PKIoverheid-certificaat gebruikt worden op basis van het SHA256 algoritme en met een private key van tenminste 2048 bits.

Beide certificaten kunnen worden aangevraagd/gegenereerd middels het document Werkinstructie FS - Aanmaken (PKIo-)certificaten.docx.

NB.: De certificaten zijn per omgeving gelijk. In een cluster-opstelling betekent dit dat de certificaten op één van de nodes gegenereerd worden en daarna gekopieerd naar de overige nodes.

3. Installatie en configuratie

Voor het gebruik van SimpleSAMLphp is het noodzakelijk om bepaalde packages te installeren en instellingen aan te passen. De noodzakelijke handelingen worden in dit hoofdstuk beschreven.

3.1 OS & packages

Voordat de installatie kan beginnen is het van belang dat enkele zaken op het gebied van het Operating System worden geregeld. Deze punten worden hieronder beschreven.

Systeemuser

Er dient een nieuwe systeemuser met de naam 'saml' gemaakt te worden:

```
adduser --system –no-create-home -u 6261 -c "IAM applicatie gebruiker"
usermod –m –d /apps saml
```

Red Hat packages

De volgende packages moeten worden geïnstalleerd:

```
yum install httpd mod_ssl php php-mcrypt php-xml nano
```

File System

De volgende mappen moeten worden aangemaakt:

```
mkdir /apps
mkdir /apps/sources
mkdir /apps/log
mkdir /apps/log/httpd
mkdir /apps/log/simplesamlphp
chmod –R 755 /apps
chown -R saml:saml /apps
chown saml:apache /apps/log/simplesamlphp
```

Automatisch opstarten services

```
chkconfig httpd on
```

Klaarzetten sources

Download de laatste versie van de volgende software:

- https://simplesamlphp.org/download

Zet de gedownloade bestanden klaar in `/apps/sources`.
Kopieer tevens de huisstijl en certificaten `/apps/sources`.

Uitpakken SimpleSAMLphp

NB.: De commando's uit deze paragraaf dienen te worden uitgevoerd onder de saml-user!

Pak het eerder gedownloade pakket uit naar de installatiedirectory:

```
cd /apps
tar -xzf /apps/sources/simplesamlphp-1.13.2.tar.gz
```

Maak een symbolic link aan:

```
ln -s /apps/simplesamlphp-1.13.2 simplesamlphp
```

Maak de cert-directory aan binnen de SimpleSamlPHP-directory:

```
mkdir /apps/simplesamlphp/cert
```

Kopieer de theme-directory:

```
cp -R /apps/sources/themejustitie /apps/simplesamlphp/modules
```

Klaarzetten certificaten, private keys en keytab

De in hoofdstuk 2 gegenereerde certificaten, keys en keytab moeten op de juiste locatie worden neergezet. Het transport-certificaat en de bijbehorende private key worden in de volgende twee directories gezet:

```
/etc/httpd/ssl
/apps/simplesaml/cert
```

Stel de rechten in op de private key in `/etc/httpd/ssl` en verwijder het wachtwoord:

```
cd /etc/httpd/ssl
chmod 400 <DNS-naam>.key
openssl rsa –in <DNS-naam>.key –out <DNS-naam>.key

cd /apps/simplesamlphp/cert
chmod 400 <DNS-NAAM>.key
```

Kopieer het bestand rijksweb-chain.crt naar /apps/simplesamlphp/cert:

```
cp /apps/sources/rijksweb-chain.crt /apps/simplesamlphp/cert
```

Zet tot slot het signing-certificaat, de bijbehorende private key in de directory `/apps/simplesamlphp/cert`

Host Firewall

Vul de file `/etc/sysconfig/iptables` met de volgende inhoud:

```
# Generated by iptables-save v1.4.7 on Thu Oct 15 13:40:29 2015
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:LOGDROP - [0:0]
# Algemeen input
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -s 127.0.0.0/8 -d 127.0.0.0/8 -i lo -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
# Memcached in
-A INPUT -i eth0 -p tcp -m tcp –dport 11211 –s <SUBNET> -m state --state NEW
-j ACCEPT
# Verbindingen vanaf de browser naar de Identity Provider / IdP-Proxy
-A INPUT -i eth0 -p tcp -m tcp --dport 443 -m state --state NEW -j ACCEPT
-A INPUT -j LOGDROP
# Algemeen output
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m udp --dport 443 -m state --state NEW -j ACCEPT
-A OUTPUT -p udp -m udp --dport 123 -m state --state NEW -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -m state --state NEW -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 25 -m state --state NEW -j ACCEPT
-A OUTPUT -p tcp -m tcp –d <SUBNET> --dport 11211 -m state --state NEW -j
ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
-A OUTPUT -j LOGDROP
-A LOGDROP -m limit --limit 6/min -j LOG --log-prefix "LOGDROP "
-A LOGDROP -j DROP
COMMIT
# Completed on Thu Oct 15 13:40:29 2015
```

Herstart iptables

```
service iptables restart
```

SELinux

SELinux hoort standaard aan te staan op machines in de JuBit DMZ. Indien dit toch niet het geval is dient dit ingeschakeld te worden:

```
setenforce 1

semanage fcontext -a -t http_sys_content_t "/apps/simplesamlphp(/.*)?"
semanage fcontext -a -t httpd_log_t "/apps/logs(/.*)?".
semanage fcontext -a -t httpd_cache_t "/var/cache(/.*)?"
```

```
restorecon -Rv /apps/simplesamlphp
restorecon -Rv /apps/logs
restorecon -Rv /var/cache
```

Cluster-configuratie (Optioneel)

Indien de server onderdeel wordt van een cluster dienen een aantal extra handelingen te worden gedaan ter voorbereiding.

Extra packages moeten worden geïnstalleerd:
```
yum install php-pecl-memcache memcached
```

Memcached moet automatisch gestart worden:
```
chkconfig memcached on
```

3.2 Configuratie Apache & PHP

Voordat de installatie kan beginnen is noodzakelijk dat een aantal zaken rondom de webserver worden geregeld. Deze punten worden hieronder beschreven.

Apache algemene configuratie

De volgende settings dienen te worden aangepast in `/etc/httpd/conf/httpd.conf` . De instellingen zijn bedoeld voor een juiste werking ofwel in het kader van hardening. De wijzigingen ten opzichte van de standaardinstellingen zijn onderstreept.

```
#LoadModule include_module modules/mod_include.so
#LoadModule env_module modules/mod_env.so
#LoadModule ext_filter_module modules/mod_ext_filter.so
#LoadModule status_module modules/mod_status.so
#LoadModule actions_module modules/mod_actions.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule cgi_module modules/mod_cgi.so
#LoadModule version_module modules/mod_version.so

#Listen 80

ServerTokens Prod
ServerSignature Off
TraceEnable Off
```

Vervangen standaard SSL-configuratie

Archiveer de volgende file:
`mv /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf.bak`

Maak een nieuwe file aan voor de SSL-configuratie:
`/etc/httpd/conf.d/ssl.conf`

Vul de file met de volgende inhoud:

```
# This is the Apache server configuration file providing SSL support.
# It contains the configuration directives to instruct the server how to
# serve pages over an https connection. For detailing information about these
# directives see <URL:http://httpd.apache.org/docs/2.2/mod/mod_ssl.html>
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#

LoadModule ssl_module modules/mod_ssl.so
#
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
Listen 443
```

```
##
##  SSL Global Context
##
##  All SSL configuration in this context applies both to
##  the main server and all SSL-enabled virtual hosts.
##

#   Pass Phrase Dialog:
#   Configure the pass phrase gathering process.
#   The filtering dialog program (`builtin' is a internal
#   terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog  builtin

#   Inter-Process Session Cache:
#   Configure the SSL Session Cache: First the mechanism
#   to use and second the expiring timeout (in seconds).
SSLSessionCache         shmcb:/var/cache/mod_ssl/scache(512000)
SSLSessionCacheTimeout  300

#   Semaphore:
#   Configure the path to the mutual exclusion semaphore the
#   SSL engine uses internally for inter-process synchronization.
SSLMutex default

#   Pseudo Random Number Generator (PRNG):
#   Configure one or more sources to seed the PRNG of the
#   SSL library. The seed data should be of good random quality.
#   WARNING! On some platforms /dev/random blocks if not enough entropy
#   is available. This means you then cannot use the /dev/random device
#   because it would lead to very long connection times (as long as
#   it requires to make more entropy available). But usually those
#   platforms additionally provide a /dev/urandom device which doesn't
#   block. So, if available, use this one instead. Read the mod_ssl User
#   Manual for more details.
SSLRandomSeed startup file:/dev/urandom  256
SSLRandomSeed connect builtin
#SSLRandomSeed startup file:/dev/random  512
#SSLRandomSeed connect file:/dev/random  512
#SSLRandomSeed connect file:/dev/urandom 512

#
# Use "SSLCryptoDevice" to enable any supported hardware
# accelerators. Use "openssl engine -v" to list supported
# engine names.  NOTE: If you enable an accelerator and the
# server does not start, consult the error logs and ensure
# your accelerator is functioning properly.
#
SSLCryptoDevice builtin
#SSLCryptoDevice ubsec

SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:kEDH+AESGCM:
ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:
```

```
ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-
SHA:!aNULL:!eNULL:!DHE:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

SSLHonorCipherOrder On
SSLCompression Off
```

VirtualHost-configuratie

Maak een nieuwe file aan voor de HTTP-verbindingen:
`/etc/httpd/conf.d/idpproxy.conf`

Vul de file met de volgende inhoud:

```
<VirtualHost *:443>
    ServerName <RIJKSWEB-DNS-NAME>
    ServerAlias <NODE-FQDN>
    ServerAlias <NODE-HOSTNAME>

    ServerAdmin <ADMIN-EMAIL>
    DocumentRoot /apps/simplesamlphp/www

    SSLEngine on
    SSLCertificateFile /etc/httpd/ssl/<RIJKSWEB-DNS-NAME>.crt
    SSLCertificateKeyFile /etc/httpd/ssl/<RIJKSWEB-DNS-NAME>.key
    SSLCertificateChainFile /etc/httpd/ssl/rijksweb-chain.crt

    ErrorLog /apps/log/httpd/idp-ssl-error.log
    CustomLog /apps/log/httpd/idp-ssl-access.log common

    RewriteEngine on

    RewriteCond %{THE_REQUEST} !HTTP/1.1$
    RewriteRule .* - [F]

    RewriteCond %{HTTP:Authorization}  !^$
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization},L]

    <Location />
       Order deny,allow
       Deny from all
       Allow from 127.0.0.0/8
       Allow from ::1/128
       Allow from <ADMIN-NETWORK>
    </Location>

    <Location /login.php>
       Allow from all
    </Location>

    <Location /resources>
       Allow from all
    </Location>

    <Location /saml2>
```

```
      Allow from all
   </Location>

   <Location /module.php/core/loginuserpass.php>
      Allow from all
   </Location>

   <Location /module.php/core/idp>
      Allow from all
   </Location>

   <Location /module.php/negotiate/backend.php>
      Allow from all
   </Location>
</VirtualHost>
```

PHP-configuratie

De volgende settings dienen te worden aangepast in `/etc/php.ini` voor een juiste werking ofwel in het kader van hardening. De wijzigingen ten opzichte van de standaardinstellingen zijn onderstreept.

```
expose_php = Off
display_errors = Off
html_errors = Off
allow_url_fopen = Off
session.cookie_secure = 1
session.cookie_httponly = 1
date.timezone = Europe/Amsterdam
```

Herstarten Apache

Herstart Apache om de wijzigingen uit deze paragraaf te activeren:
`service httpd restart`

3.3 Configuratie SimpleSAMLphp

Deze paragraaf beschrijft de configuratie van SimpleSAMLphp. De verschillende componenten die aangepast dienen te worden, worden hieronder beschreven.

SimpleSAMLphp algemene configuratie

Genereer alvast een password-hash d.m.v. het volgende commando:
`/apps/simplesamlphp/bin/pwgen.php`

Kies een wachtwoord voor de beheerinterface van SimpleSAMLphp, gebruik een sterk hashing algoritme `[sha256]` en gebruik een salt `[yes]`.

Genereer ook alvast een secret salt:
`tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo`

Open nu de file `/apps/simplesamlphp/config/config.php` en pas de volgende settings aan voor een juiste werking dan wel in het kader van hardening. De wijzigingen ten opzichte van de standaardinstellingen zijn onderstreept.

```
'loggingdir' => '/apps/log/simplesamlphp/',
'auth.adminpassword' => '<PASSWORD-HASH>',
'admin.protectindexpage' => true,
'secretsalt' => '<SECRET-SALT>',
'technicalcontact_name' => '<ADMIN-NAME>',
'technicalcontact_email' => '<ADMIN-EMAIL>',
'timezone' => 'Europe/Amsterdam',
'logging.handler' => 'file',
'enable.saml20-idp' => true,
'session.cookie.secure' => true,
'session.phpsession.httponly' => true,
'language.available' => array('en', ‘nl’),
'language.rtl' => array(),
'language.default' => 'nl',
'theme.use' => 'themejustitie:justitie'
'memcache_store.servers' => array(
    array(
        array('hostname' => '<NODE-1-FQDN>'),
    ),
),
```

Configureren authenticatiebronnen

Archiveer de file /apps/simplesamlphp/config/authsources.php:
`mv /apps/simplesamlphp/config/authsources.php /apps/simplesamlphp/config/authsources.php.bak`

Maak vervolgens een nieuwe file aan met de volgende inhoud:

```
<?php

$config = array(

     // This is a authentication source which handles admin authentication.
     'admin' => array(
         // The default is to use core:AdminPassword, but it can be replaced
with
         // any authentication source.

         'core:AdminPassword',
     ),


     'default-sp' => array(
         'saml:SP',
     ),

);
```

Metadata-file Remote Service Providers

Pas de file `/apps/simplesamlphp/metadata/saml20-idp-remote.php` aan met de volgende inhoud:

```
<?php
/**
  * SAML 2.0 remote SP metadata for simpleSAMLphp.
  *
  * See:
https://simplesamlphp.org/docs/stable/simplesamlphp-reference-sp-remote
  */
```

Deze file wordt in een later stadium aangevuld met trusts naar remote SP's.

Metadata-file Remote Identity Providers

Pas de file `/apps/simplesamlphp/metadata/saml20-idp-remote.php` aan met de volgende inhoud:

```
<?php
/**
  * SAML 2.0 remote IdP metadata for simpleSAMLphp.
  *
  * Remember to remove the IdPs you don't use from this file.
  *
  * See:
https://simplesamlphp.org/docs/stable/simplesamlphp-reference-idp-
remote
  */
```

Deze file wordt in een later stadium aangevuld met trusts naar remote IdP's.

Metadata-file IdP-Proxy

Pas de file `/apps/simplesamlphp/metadata/saml20-idp-hosted.php` aan met de volgende inhoud:

```
<?php
/**
  * SAML 2.0 IdP configuration for simpleSAMLphp.
  *
  * See:
https://simplesamlphp.org/docs/stable/simplesamlphp-reference-idp-hosted
  */

$metadata['__DYNAMIC:1__'] = array(
         /*
          * The hostname of the server (VHOST) that will use this SAML
entity.
          *
          * Can be '__DEFAULT__', to use this entry by default.
          */
         'host' => '__DEFAULT__',

         /* X.509 key and certificate. Relative to the cert directory. */
         'privatekey' => '<DNS-naam>.key',
         'certificate' => '<DNS-naam>.crt',

         /*
          * Authentication source to use. Must be one that is configured in
          * 'config/authsources.php'.
          */
         'auth' => 'default-sp',

         /*
          * WARNING: SHA-1 is disallowed starting January the 1st, 2014.
          *
          * Uncomment the following option to start using SHA-256 for your
signatures.
          * Currently, simpleSAMLphp defaults to SHA-1, which has been
deprecated since
          * 2011, and will be disallowed by NIST as of 2014. Please refer to
the following
          * document for more information:
          *
          *
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
          *
          * If you are uncertain about service providers supporting
SHA-256 or other
          * algorithms of the SHA-2 family, you can configure it individually
in the
          * SP-remote metadata set for those that support it. Once you are
certain that
          * all your configured SPs support SHA-2, you can safely remove the
configuration
          * options in the SP-remote metadata set and uncomment the following
option.
          *
          * Please refer to the IdP hosted reference for more information.
```

```
          */
         'signature.algorithm' =>
'http://www.w3.org/2001/04/xmldsig-more#rsa-sha256',

);
```

Cluster-configuratie (optioneel)

Open nogmaals de file `/apps/simplesamlphp/config/config.php` en voeg een tweede memcache-server toe. De wijzigingen ten opzichte van de huidige stand zijn weer onderstreept:

```
'store.type' => 'memcache',

'memcache_store.servers' => array(
    array(
        array('hostname' => '<NODE-1-FQDN>'),
    ),
     array(
       array('hostname' => '<NODE-2-FQDN>'),
     ),
),
```

3.4 Verificatie en afronding

De IdP-Proxy is nu volledig geïnstalleerd en geconfigureerd. De volgende paragraaf beschrijft methoden om de verschillende aspecten van de IdP-Proxy te testen en de juiste werking te verifiëren.

Beheerinterface

Controleer of de beheerinterface te benaderen is. Open een browser en vul de Rijksweb DNS-naam in. Wanneer http:// gebruikt wordt zou er automatisch omgeschakeld moeten worden naar https://.
De beheerpagina zou er als volgt uit moeten zien:

Als de pagina niet benaderbaar is, controleer dan allereerst of de httpd service gestart is. Wanneer er een '403 Forbidden' foutmelding gegeven wordt, controleer dan of de IP-reeks van het werkstation is opgenomen als *<ADMIN-NETWORK>* in de Apache-configuratie (zie paragraaf 3.2.3).

Wordt de pagina wél getoond, log dan in met het admin-wachtwoord uit paragraaf 3.3.1. Ga naar het tabblad configuratie en controleer of alle vinkjes groen zijn, met uitzondering van Shib 1.3 IdP en MySQL-support.

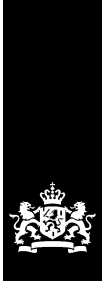
Koppeling met Service Providers en Identity Providers

Voor een koppeling met een SP of IdP is metadata van de tegenpartij benodigd. Deze metadata wordt aangeboden als XML-file. Ga naar het tabblad 'Federatie' en kies voor 'XML naar SimpleSAMLphp metadata vertaling'. Voer hier nu de geleverde XML-code in, **zonder** de XML declaratie: `<?xml version="1.0"?>`

De uitvoer is een stuk PHP-code wat aan de juiste file toegevoegd moet worden. Voor Service Providers is dit:
`/apps/simplesamlphp/metadata/saml20-sp-remote.php`

Voor Identity Providers is dit:
`/apps/simplesamlphp/metadata/saml20-idp-remote.php`

Om de koppeling volledig werkend te krijgen moet de tegenpartij de metadata van de IdP-Proxy inlezen. Deze metadata is beschikbaar op de volgende url:
https://<DNS-naam>/saml2/idp/metadata.php



SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Doorontwikkeling Federatieve Service

Testplan

Auteur: Tim van Dijen - studentnummer 00008055

Opdrachtgever: Dhr. R. P. van Kruistum

Datum: dinsdag 1 december 2015
Versie: 1.0
Status: Concept

Colofon

Afzendgegevens	**DG Organisatie Bedrijfsvoering Rijk** SSC-ICT Haaglanden Pijler 2 Luxemburglaan 2 2711 BC Zoetermeer Postbus 7385 2701 AJ Zoetermeer
Contactpersoon	T. van Dijen T 079 330 22 00 F 079 330 22 22
Projectnaam	Doorontwikkeling VenJ Federatieve Dienst
Auteurs	T. van Dijen

Documenthistorie

Versie	Status	Datum	Wijzigingen
0.1	Concept	24-11-2015	Eerste versie
0.2	Concept	30-11-2015	Verwerking commentaar M. Heeren
1.0	Definitief	1-12-2015	Vastgesteld

Inhoudsopgave

1. Inleiding

In 2015 is in het project 'Doorontwikkeling Federatieve Service' gerealiseerd als vervanging van de oude VenJ Federatieve Service. Het management van SSC-ICT heeft op basis van de ervaringen met de diens t en met goedkeuring van de klant opdracht gegeven voor het project 'Doorontwikkeling Federatieve Service'. Aanleiding voor het project was de wens om een dienst neer te zetten die goedkoper en flexibeler is, beter te beheren valt en tevens voldoet aan nieuwe wensen en eisen zoals externe federatie. De Federatieve Service ondersteunt hiermee het plaats en tijd onafhankelijk kunnen werken. De architectuur van de nieuwe Federatieve Service garandeert tevens uniformiteit, eenvoud en stabiliteit in beheer.

Het geschetste toekomstbeeld van de Dienst Informatisering en Inkoop is dat er totaal drieëntwintig VenJ-onderdelen aangesloten gaan worden op de Federatieve Service. Tevens ligt er een sterke wens om de federatie geschikt te maken voor authenticatie van buitenaf.

Het doel van dit Testplan is om een ieder die betrokken is bij Project Doorontwikkeling Federatieve Service te informeren over de aanpak, de activiteiten en de op te leveren producten met betrekking tot de Federatieve Service die ter vervanging dient van de huidige versie. Dit Testplan geeft voor de Federatieve Service een concreet en gedetailleerd beeld van

- de componenten die onderdeel zijn van de te testen project producten
- de wijze waarop we gaan aantonen dat de opgeleverde project producten zijn opgeleverd conform de technische ontwerpen
- de stabiliteit en technische werking van de componenten en het project product als geheel
- De marges waarbinnen de verschillende componenten kunnen functioneren

1.1 Opdrachtformulering

Opdrachtgever
Paul van Kruistum, Manager IAM, gedelegeerd opdrachtgever in naam van de klant, DI&I.

Opdrachtnemer
IAM, in de persoon van Tim van Dijen, afstudeerder

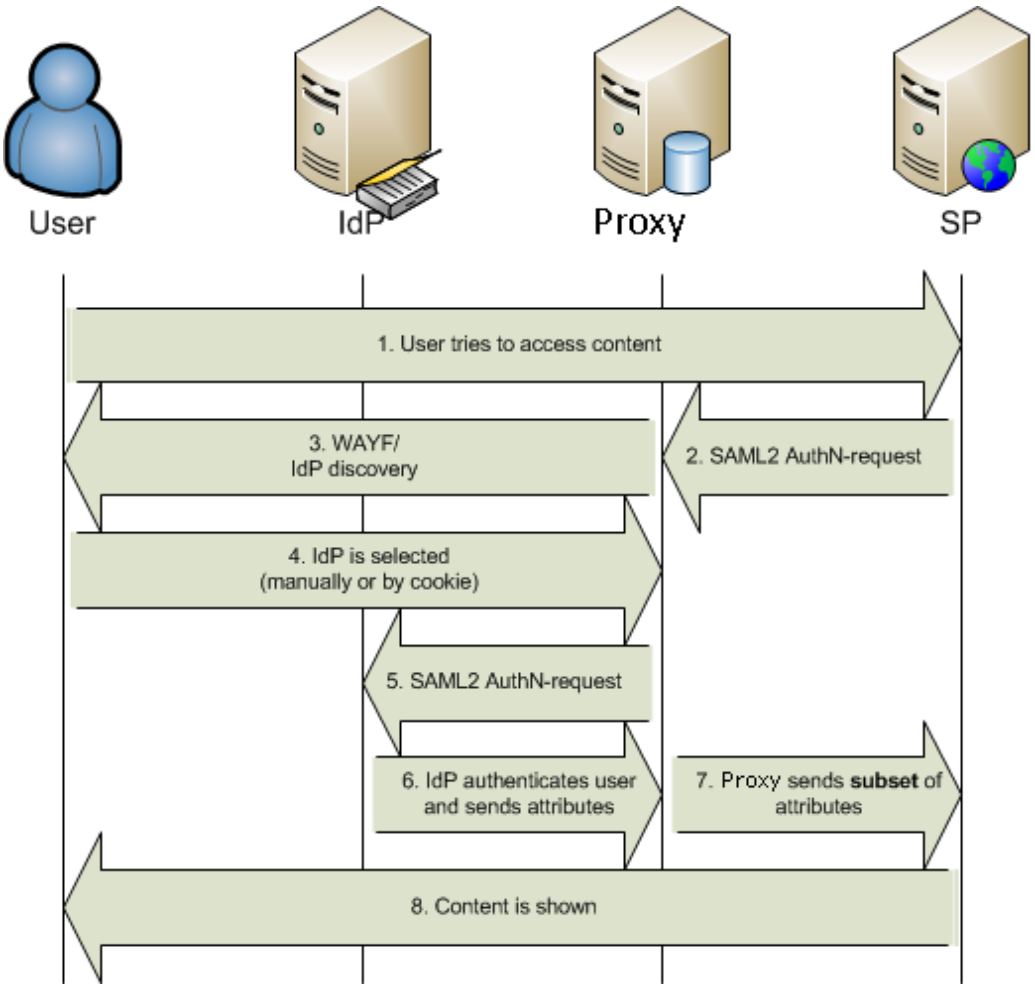
Opdracht
IAM heeft de opdracht voor het opstellen van een testplan en het uitwerken van testscenario's en eventuele testscripts om de componenten die onderdeel zijn van het op te leveren project "Doorontwikkeling Federatieve Service" conform de TMAP-methodiek methodisch te testen. Hierbij is het uitgangspunt om in eerste instantie een systeemtest uit te voeren. De regieorganisatie van het bestuursdepartement zal verantwoordelijk zijn voor de gebruikersacceptatietest (GAT). Indien de regieorganisatie er voor kiest om dit uit te besteden aan SSC-ICT, dan zal dit als een nieuwe opdracht aan project "Doorontwikkeling Federatieve Service" worden beschouwd.

Omschrijving VenJ Federatieve Service

Een federatie in zijn meest simpele vorm bestaat uit een Identity Provider (IdP) en een Service Provider (SP). Door middel van een Identity Provider Proxy (IdP-Proxy, ook wel broker of bridge genoemd) kunnen ook complexe federatieve ketens gemaakt worden. De SP is een webapplicatie, welke zelf geen eigen identity store heeft. Een gebruiker die naar de webapplicatie gaat, en nog geen geldige security token heeft, zal worden doorverwezen naar de IdP. Hier moet worden ingelogd, waarna de gebruiker met een security token weer wordt teruggestuurd naar de webapplicatie. Door de onderlinge vertrouwensrelatie tussen de SP en de IdP, zal de gebruiker worden toegelaten tot de applicatie. Deze vertrouwensrelatie is gebaseerd op PKI (Public Key Infrastructure). Het onderlinge berichtenverkeer verloopt middels het SAML protocol. Zie Figuur 1 op de volgende pagina voor een voorbeeld van federatieve authenticatie.

Een voorbeeld van een dergelijke omgeving binnen de publieke sector is DigID. Diverse overheidssites (SP's) vereisen dat een bezoeker zich authentiseert bij DigID (IdP). De SP's vertrouwen hierbij op de authenticatie van deze IdP. Op deze manier hoeft niet elke website een eigen identity store te hebben.

Aanvullend op het concept van de federatieve dienst kan voor eindgebruikers een Single Sign-On (SSO) ervaring worden gecreëerd, zodat zij niet bij elke federatief ontsloten applicatie apart moeten inloggen. De authenticatie vindt dan plaats bij het inloggen op het werkstation, waarbij een Kerberos-token wordt verkregen. Wanneer de gebruiker via een Service Provider naar een Identity Provider wordt gestuurd (1), zal de browser het Kerberos-token meesturen. De Identity Provider kan deze tegen de achterliggende identity store verifiëren (2, 3, 4, 5), waarna de gebruiker automatisch en volledig transparant voorzien wordt van een SAML-token en weer wordt teruggestuurd naar de Service Provider (6, 7).



Figuur 1: Voorbeeld federatieve authenticatie

1.2 Normen en standaarden

Er is voor de volgende methodieken gekozen bij het samenstellen van dit testplan:

- TMAP Next;
- Prince 2.

1.3 Scope van de opdracht

Het testen van het project "Doorontwikkkeling Federatieve Service" beperkt zich tot de componenten welke door SSC-ICT worden beheerd. In hoofdstuk 2.1 staat beschreven welke componenten er binnen dit testplan worden getest. Een volledig overzicht in hoofdlijnen van de uiteindelijk op te leveren telewerk omgeving staat hieronder beschreven:

Componenten tbv de telewerk omgeving	Toelichting	Domein A (beheerfacing)	Domein B (infrastructuur facing)	Domein C (userfacing)
Red Hat Enterprise Linux 6.6	Een 64-bit operating system van Red Hat		X	
DWR-werkplek	De standaard werkplek voor de eindgebruikers			X
IdP-Proxy	Het interne koppelvlak van de federatie, met koppelingen naar de verschillende Identity Providers en de rijksbrede federatie	X		X
Identity Providers	Het component waar de authenticatie van de eindgebruikers plaatsvindt tegen de achterliggende Active Directories.	X		X

1.4 Testorganisatie

Het testproject wordt uitgevoerd onder verantwoordelijkheid van Tim van Dijen, welke wekelijks rapporteert aan de opdrachtgever, Paul van Kruistum.

Binnen het testproject worden de volgende testfuncties onderscheiden:

Testcoördinator
De testcoördinator is verantwoordelijk voor de voortgang van de werkzaamheden, de bewaking, beheersing en uitvoering van het testproces. Tevens is de testcoördinator het aanspreekpunt voor derden. De testcoördinator valideert de probleemrapporten van de testers en verzorgt de communicatie met de opdrachtgever. Ook is de testcoördinator verantwoordelijk voor de inhoudelijke bepaling van situaties die getest moet worden. De testcoördinator zorgt ervoor dat zoveel mogelijk inhoudelijk rendement uit de testuitvoering wordt gehaald door het leveren van goede testscripts en de testgegevens.

Tester
De tester voert de tests uit die door de testcoördinator worden aangeleverd. Tevens levert de tester indien nodig probleemrapporten aan de testcoördinator. Onder testers valt in de regel ook de uiteindelijke beheerder / gebruiker van de omgeving, maar ook specialisten die mede adviseren over de verwachte uitkomst van een test activiteit.

Rol / functie	Naam	Cluster / team
Testcoördinator	Tim van Dijen	IAM

De volgende rollen mogen in het geheel niet gecombineerd worden met andere rollen. Dit om belangenverstrengeling uit te sluiten.

Testers	Georg Grabner	IAM

Acceptanten	n.n.t.b.	DI&I

Benodigdheden
Hier wordt kort aangegeven welke zaken de testers nodig hebben voor het naar behoren uitvoeren van hun taken.

Per Tester:	Standaard werkplek
	Verbinding met front-end omgeving
	Omgevingskennis (voor gebruikerstester)
	Systeemkennis (voor ontwikkeltester)
(Beheerder)	Standaardwerkplek met beheertools
	Netwerktoegang naar backend en front-end
	Beheer rechten op de te testen omgeving
	Technisch inhoudelijke kennis over het te testen product
Aanbevolen:	Kennis van TMap
	Ervaring met TMap testtechnieken
	Omgevingskennis (conceptueel)

Vrijgavemoment
De acceptatie (vrijgave voor volgende testfase) vindt plaats na een Go / No Go overleg dat door de testcoördinator met de opdrachtgever wordt belegd. Basis bij dit overleg is het testrapport uit de test.

Vrijgave van een component vindt plaats nadat geverifieerd is dat aan de exit- of acceptatiecriteria is voldaan. Hierover wordt in het testrapport uitsluitsel gegeven. De vrijgavebeslissing wordt genomen door Paul van Kruistum, manager IAM, die zich daarbij (mede) baseert op het testrapport.

1.5 Documentatie

In deze paragraaf wordt de gebruikte documentatie beschreven welke relaties hebben met het systeemtesten, veelal gelijk aan de ontwikkelbasis.

Basis voor het testplan

De volgende documenten zijn gebruikt als basis voor dit testplan:

Documentnaam	Versie	Datum	Auteur
Plan van Aanpak - Doorontwikkeling Federatieve Service	1.2	21-9-2015	Tim van Dijen
TMAP Next			

Testbasis

De testbasis bestaat uit die documenten en omgevingen waaruit de testgevallen worden afgeleid. De testbasis bevat de documentatie die als basis dient voor de uit te voeren tests. Onderstaand overzicht geeft de documentatie die als uitgangspunt dient bij de systeem- en acceptatietesten.

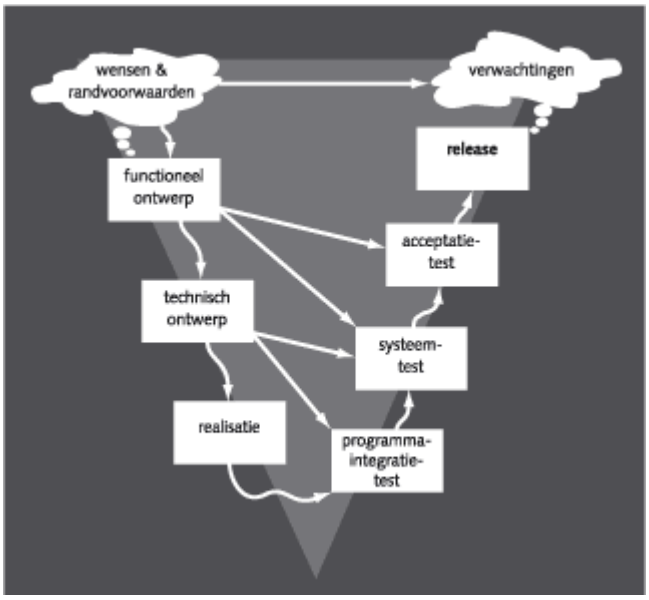
Documentnaam	Versie	Datum	Auteur
Definitiestudie	1.1	2-11-2015	Tim van Dijen
Technisch Ontwerp	1.0	16-11-2015	Tim van Dijen

2. Teststrategie

De beschikbare tijd om te testen is beperkt; niet alles kan even zwaar worden getest. Dus moesten er keuzes worden gemaakt. Daarbij is ernaar gestreefd om de testcapaciteit zo effectief en efficiënt mogelijk over het totale testtraject te verdelen.

De teststrategie legt vast wat er met welke zwaarte wanneer (in welke testsoort) getest gaat worden en is er op gericht om zo vroeg mogelijk de belangrijkste fouten te vinden tegen de minste kosten, dus met optimaal gebruik van de beschikbare capaciteit en tijd.

In dit testplan is de teststrategie verder uitgewerkt voor de Federatieve Service. Dit is weergegeven in paragraaf 2.1. In bijlage I wordt de uit deze teststrategie resulterende concrete testaanpak, het hoe, beschreven.



Figuur 2: V-model fasering testtraject

2.1 Teststrategie Federatieve Service

De volgende componenten worden onderworpen aan een systeemtest:

- Red Hat Enterprise Linux 6.6; korte toets bij alle producten die op dit platform draaien.
- IdP-Proxy; Test op TO, beheerbaarheid, bruikbaarheid, functionaliteit, beveiliging, connectiviteit.
- Identity Provider(s); Test op TO, beheerbaarheid, bruikbaarheid, functionaliteit, beveiliging, connectiviteit.

Hieruit valt af te leiden dat het eerste product gecontroleerd worden op juistheid en volledigheid bij oplevering. Het project richt deze producten niet in, maar neemt ze af van de beheerorganisatie SSC-ICT.

De Identity Provider(s) en IdP-Proxy moeten afdoende getest worden, omdat deze in de basisfunctionaliteit van de federatieve dienst voorzien. Bruikbaarheid en continuïteit staan hierbij centraal. Ook de inpasbaarheid binnen de huidige organisatie moet goed zijn uitgewerkt; Het gaat hier om een organisatie-overstijgend systeem, hetgeen afstemming behoeft over de taken, bevoegdheden en verantwoordelijkheden voor elk VenJ-onderdeel wat acteert binnen deze omgeving.

Wanneer het eerste component een succesvolle systeemtest heeft ondergaan, kan begonnen worden met de Systeem Integratie Test (SIT). De technische basis is dan klaar.

De IdP-Proxy en Identity Provider(S) worden inhoudelijk getest op configuratie (TO-check). Daarnaast wordt er een nulmeting verricht voor de performance indicatoren geheugen, processor, disk en netwerk. Vervolgens wordt de redundantie en continuïteit getest; wat gebeurd er als een machine uitvalt. Wat betekent uitval of voor de continuïteit van de dienstverlening.

2.2 Beschrijving testaanpak

Het testen start met het uitvoeren van een intake op het testobject om te verifiëren dat aan de entry-criteria is voldaan. Deze intake bestaat uit een volledigheidscheck en een pre-test.

Volledigheidscheck
Aan de hand van een checklist wordt vastgesteld of het testobject en alle bijbehorende documentatie volledig zijn opgeleverd.

Pre-test
De pre-test dient om voorafgaand aan de werkelijke testuitvoering vast te stellen of het mogelijk en zinvol is om met de testuitvoering te starten. De pre-test wordt als volgt uitgevoerd:
1. checklist met alle functies; deze moeten allemaal benaderbaar zijn;
2. voor een aantal representatieve functies wordt een eenvoudig testgeval met valide invoer ("goed"-geval) gespecificeerd en uitgevoerd;
3. enkele op integratie gerichte testgevallen worden gespecificeerd en uitgevoerd om te controleren dat de verschillende onderdelen van het systeem met elkaar kunnen communiceren.

2.3 Entry- en exit-criteria

Systeemtest
Entry criteria voor fase Specificatie:

- Er is een definitief technisch ontwerp die als basis dient voor de technische inrichting van het component
- De infrastructuur is bekend en beschreven

Entry criteria voor fase Uitvoering:

- De ontwerpers / bouwers geven aan dat de te testen omgeving is ingericht conform het technisch ontwerp
- Er is een implementatie handleiding opgeleverd, waarin eventuele verschillen t.o.v. het oorspronkelijke ontwerp zijn opgenomen
- Er zijn geen blokkerende issues bekend tijdens de bouw van het component
- Toegang en autorisatie is geregeld voor de testers en de ondersteuners
- De juiste versie van het testscript is voorhanden
- Resources zijn geclaimd en toegekend
- Er zijn geen verstoringen binnen de infrastructuur die de tests kunnen beïnvloeden

Exit criteria voor fase afronding:

- Er zijn geen open bevindingen van het kaliber A of B
- Bevindingen van het kaliber C zijn óf opgelost, óf geaccepteerd door de opdrachtgever
- De test procedure en uitvoering is geëvalueerd. Aanpassingen voor toekomstige tests zijn beschreven (lessons learned)
- De documentatie is waar nodig bijgewerkt
- De testscripts zijn aangepast voor hergebruik

Systeem Integratie Test
Entry criteria voor fase Specificatie:

- Voor alle componenten die deelnemen aan de SIT geldt dat er een definitief technisch ontwerp is.
- De beoogde techniek en/of functionaliteit die de gezamenlijke componenten moeten vormgeven, is afdoende beschreven (wat is het beoogde resultaat)
- De marges waarin de omgeving mag acteren zijn bekend.

Entry criteria voor fase Uitvoering:

- Alle componenten die deelnemen aan de SIT (systeem Integratie Test) hebben een afgerond ST (systeem Test) doorlopen
- Er zijn geen blokkerende issues bekend tijdens de bouw het component
- Toegang en autorisatie is geregeld voor de testers en de ondersteuners
- De juiste versie van het testscript is voorhanden
- Resources zijn geclaimd en toegekend
- Er zijn geen verstoringen binnen de infrastructuur die de tests kunnen beïnvloeden

Exit criteria voor fase afronding:

- Er zijn geen open bevindingen van het kaliber A of B
- Bevindingen van het kaliber C zijn óf opgelost, óf geaccepteerd door de opdrachtgever
- De test procedure en uitvoering is geëvalueerd. Aanpassingen voor toekomstige tests zijn beschreven (lessons learned)
- De documentatie is waar nodig bijgewerkt
- De testscripts zijn aangepast voor hergebruik

Functioneel Acceptatie Test

Entry criteria voor fase Specificatie:

- Alle componenten die als basis dienen voor de beoogde functionaliteit hebben de SIT succesvol afgerond
- Voor alle componenten die deelnemen aan de FAT (Functionele Acceptatie Test) geldt dat er een definitief functioneel ontwerp is

Entry criteria voor fase Uitvoering:

- De ontwerpers / bouwers geven aan dat de te testen omgeving is ingericht conform het functioneel ontwerp
- Het is duidelijk welke functionaliteit geëist wordt, belangrijk of gewenst is
- Er is een implementatie handleiding opgeleverd, waarin eventuele verschillen t.o.v. het oorspronkelijke ontwerp zijn opgenomen
- Er zijn geen blokkerende issues bekend tijdens de bouw van de omgeving
- Toegang en autorisatie is geregeld voor de testers en de ondersteuners
- De juiste versie van het testscript is voorhanden
- Resources zijn geclaimd en toegekend
- Er zijn geen verstoringen binnen de infrastructuur die de tests kunnen beïnvloeden

Exit criteria voor fase afronding:

- Er zijn geen open bevindingen van het kaliber A of B
- Bevindingen van het kaliber C zijn óf opgelost, óf geaccepteerd door de opdrachtgever
- De test procedure en uitvoering is geëvalueerd. Aanpassingen voor toekomstige tests zijn beschreven (lessons learned)
- De documentatie is waar nodig bijgewerkt
- De testscripts zijn aangepast voor hergebruik

3. Infrastructuur

De volgende componenten worden ingericht ten behoeve van de Federatieve Service:

Leverancier	Product	Versie	Hostnaam	Functie
Red Hat	Red Hat Enterprise Linux	6.6	GDISX0061	IdP-Proxy
	Red Hat Enterprise Linux	6.6	GDISX0062	IdP-Proxy
	Red Hat Enterprise Linux	6.6	GDISX0063	Identity Provider
	Red Hat Enterprise Linux	6.6	GDISX0064	Identity Provider

3.1 Testomgeving

Per testscript en testfase zal worden beschreven welke componenten deelnemen aan de test. Voorbeelden hiervan staan hieronder beschreven:

Systeemtesten
Benodigde testomgeving(en):
- Hardware;
- Systeemsoftware;
- Communicatiemiddelen;
- Faciliteiten voor opbouw en gebruik van bestanden;
- Procedures en Afspraken.

Acceptatietesten
Benodigde testomgeving(en):
- Hardware;
- Systeemsoftware;
- Communicatiemiddelen;
- Faciliteiten voor opbouw en gebruik van bestanden;
- Procedures en Afspraken.

4. Beheer

Testprocesbeheer
Voortgang en kwaliteit van testwerkzaamheden wordt bewaakt door de testcoördinator.

Wekelijks wordt het voortgangsrapport testen gemaild aan de opdrachtgever. Het voortgangsrapport geeft inzicht in status van de testwerkzaamheden en de tot dusver geconstateerde kwaliteit van het systeem onder test.

Bevindingenprocedure
Het bevindingenbeheer is ingericht conform de in TMap NEXT beschreven bevindingenprocedure of de bij de klantorganisatie vigerende bevindingenprocedure.

De verantwoordelijkheid voor de naleving van deze bevingenprocedure ligt bij de testcoördinator.

Planning

De planning met betrekking tot het testen van de omgeving moet overeenstemmen met de projectplanning. Daar waar sprake is van afwijkingen moeten deze zijn afgestemd met de opdrachtgever en moet een motivering van de afwijkingen gegeven worden, in termen van Resultaat, Risico, Tijd en Geld.

Bijlage 1 - Testrapportage

Teststap	Tester	Datum	Bevinding	Priorisering	Status	Mogelijke oplossing	Status
1: Internet Explorer start op	TVD/GGR	30-nov		1	OK		OK
2: Versie Internet Explorer is 8	TVD/GGR	30-nov	Sommige clients draaien IE11	3	NOK	Tests ook uitvoeren onder IE11	OK
3: Op Rijksweb-url is het component niet direct benaderbaar (HTTP/403)	TVD/GGR	30-nov		2	OK		OK
4: Op hostnaam is het component niet direct benaderbaar (HTTP/403)	TVD/GGR	30-nov		2	Ok		OK
5: Op hostnaam is het component wél benaderbaar vanaf de beheerserver	TVD/GGR	30-nov		2	OK		OK
6: De interface is in het Nederlands	TVD/GGR	30-nov		1	OK		OK
7: De interface is in de VenJ huisstijl	TVD/GGR	30-nov		1	OK		OK
8: Op het configuratiescherm zijn alle vinkjes groen, m.u.v. Mysql Support en Shib 1.3	TVD/GGR	30-nov		2	OK		OK
9: De Sanity check wordt succesvol doorlopen	TVD/GGR	30-nov		2	OK		OK
10: Authenticatie middels LDAP gaat goed	TVD/GGR	30-nov		1	Ok		OK
11: Authenticatie middels Kerberos gaat goed	TVD/GGR	30-nov		2	OK		OK
12: De keten vanaf SSOn-Rijk kan succesvol doorlopen worden	TVD/GGR	30-nov		1	OK		OK
13: De keten vanaf de Access Gateway kan succesvol doorlopen worden	TVD/GGR	30-nov		1	OK		OK
14: Tijdens beide ketentesten worden geen certificaatfouten getoond	TVD/GGR	30-nov		3	OK		OK
15: Cluster Failover-test	TVD/GGR	30-nov		2	OK		OK
16: SELinux staat op 'Enforced'	TVD/GGR	30-nov	SELinux staat op 'Permissive'	4	NOK	SELinux moet ingeschakeld worden door de systeembeheerders.	OK
						Niet blokkerend	
17: De Iptables service draait	TVD/GGR	30-nov		4	OK		OK
18: Een Webserver-configuratietest via ssllabs.com resulteert in een A+ rating	TVD/GGR	30-nov		4	OK		OK

Dijen, T. van - GDI/BH/IAM

Van: Tim van Dijen <tvdijen@gmail.com>
Verzonden: woensdag 11 november 2015 14:02
Aan: Hans de Vreught
CC: Dijen, T. van - GDI/BH/IAM; Heeren, M.R. - GDI/BH/IAM
Onderwerp: Voortgang afstudeerstage

Beste meneer de Vreught,

Bij deze, conform afspraak, een kort voortgangsverslag met betrekking tot mijn afstudeerstage.
We zijn inmiddels ruim over de helft van de periode en de opdracht verloopt tot op heden redelijk goed! De verwachting die we vooraf hadden was dat de definitiefase misschien wel iets uit zou gaan lopen. Deze verwachting is waar gebleken, waardoor ik iets uitloop op de planning. Ook ben ik een aantal dagen ziek geweest begin november.

Naar verwachting kan deze week het Technisch Ontwerp worden vastgesteld en kan vanaf komende week aan de realisatie worden begonnen. De opleverdatum van de benodigde servers staat op vrijdag aanstaande. Ondanks de achterstand verwacht ik deze ruimschoots goed te kunnen maken dankzij de grondige voorbereiding in de definitie- en ontwerpfase.

Dat gezegd hebbende zou ik graag met u afspraken maken voor een conceptbespreking en het tussentijds assessment. Mijn voorstel daarbij is om de conceptbespreking eind november te plannen en het TTA begin december. Voor het TTA gaat de voorkeur uit naar een maandag, dinsdag of woensdag in verband met de beschikbaarheid van mijn bedrijfsmentor.

Met vriendelijke groet,

Tim van Dijen

Bespreking concept	Tussentijds assessment	Eerste beoordeling

Formulier bespreking concept afstudeerdossier

Student: Tim van Dijen **Studentnummer:** 8055

Datum: 17-11-2015

Tijdens de bespreking is het volgende geconstateerd:		**ja**	**nee**
a	*Het voortgangsverslag is ontvangen*	v	
b	*Het afstudeerdossier is digitaal beschikbaar*	v	
c	*Het afstudeerdossier is opgebouwd conform de richtlijnen*	v	
d	*Het goedgekeurde afstudeerplan is aanwezig*	v	
e	*Het plan van aanpak is aanwezig*	v	
f	*Reeds geleverd commentaar is aanwezig*	n.v.t.	
g	*Het afstudeerdossier geeft voldoende inzicht in de stand van zaken*		x
h	*De afstudeeropdracht is tot nu toe naar behoren uitgevoerd*	v	

Verbeterpunten:

Laat meer van je (deel-) producten zien in het verslag. Je moet dit gebruiken als kapstok om uit te leggen hoe je van deelproduct A naar deelproduct B komt. Zo geef je inzicht in de gevolgde procesgang.

Opmerkingen:

De bijlagen zien er kwalitatief in orde uit, het probleem zit in de verslaglegging van afstudeerdossier naar ons toe. Bij de bespreking hebben we ook even naar wat voorbeeld afstudeerverslagen.

Naam begeleidend examinator: **Hans de Vreught**

Datum: **17-11-2015**

Dit formulier wordt door de begeleidend examinator digitaal ingevuld en per email naar de student verstuurd met een cc naar de coördinator van At Work faculteit ITD (A.M.Schipper@hhs.nl). Het formulier dient door de student te worden opgenomen in het afstudeerdossier.

Bespreking concept	**Tussentijds assessment**	Eerste beoordeling

Formulier tussentijds assessment

Student: Tim van Dijen **Studentnummer:** 00008055

Datum: 1-12-2015 **eerste / tweede TTA:** eerste

Tijdens het tussentijds assessment is het volgende geconstateerd:		**ja**	**nee**
a	*Het voortgangsverslag is ontvangen*	x	
b	*Het afstudeerdossier is digitaal beschikbaar*	x	
c	*Het afstudeerdossier is opgebouwd conform de richtlijnen*	x	
d	*Het goedgekeurde afstudeerplan is aanwezig*	x	
e	*Het plan van aanpak is aanwezig*	x	
f	*Reeds geleverd commentaar is aanwezig*	x	
g	*Het afstudeerdossier geeft voldoende inzicht in de stand van zaken*	x	
h	*De afstudeeropdracht is tot nu toe naar behoren uitgevoerd*	x	

Aanpak	**O**	**T**	**V**	**G**
Passend		x	x	
Theoretisch verantwoord		x		
Samenhang uitvoering beroepstaken			x	

Beroepstaken op afgesproken niveau uitgevoerd?		**O**	**T**	**V**	**G**
1	G1 Praktische aspecten hanteren in (internationale) projecten		x		
2	A1 Analyseren van het probleemdomein		x	x	
3	C9 Ontwerpen van een infrastructuur		x	x	
4	D18 Testen van een infrastructuur		x		
5					
6					

Producten	**O**	**T**	**V**	**G**
Tussenproducten			x	
Eindproducten				

Effectief communiceren	**O**	**T**	**V**	**G**
Binnen afstudeerbedrijf			x	
Afstudeerdossier		x		

Reflectie	**O**	**T**	**V**	**G**
Inzicht in eigen functioneren			x	
Inzicht in eigen leerproces			x	

<u>Toelichting per beoordelingscriterium</u>

Aanpak
- Eigen bijdrage onduidelijk. Moeilijk voor de lezer om inzichten overzicht van de aanpak te krijgen op basis van de scriptie. - Theoretisch niet verantwoord: geen referenties aan de lijst en te weinig motivatie in de scriptie - Passend met beroepstaken

Beroepstaken op afgesproken niveau uitgevoerd?
G1: Beheersaspecteen in PMW niet goed toegepast. Verwarrende risicoanalyse. Overige beheersaspecten ontbreken mogelijk. A1: Bijlagen ok maar te weinig in de hoofdtekst (Idaardoor lastig leesbaar) C9: Bijlagen ok maar te weinig in de hoofdtekst (Idaardoor lastig leesbaar) D18: Testen nog onder de maat (door onduidelijkheid eisen) Testomgeving te summier beschreven

Producten
Te veel in de bijlagen en te weinig in de hoofdtekst

Verder onduidelijk wat het eigen werk is en wat van anderen is.

Effectief communiceren
Te veel in de bijlagen en te weinig in de hoofdtekst Verder onduidelijk wat het eigen werk is en wat van anderen is.

Reflectie
Te algemeen evaluatiehoofdstuk. Inzicht eigen leervermogen nog niet duidelijk.

Advies

x	**Inleveren** (bindend advies)
	Verlengen (vrijblijvend advies)
	Stoppen (vrijblijvend advies)

Besluit student

Aankruisen welke beslissing de student heeft genomen (alleen na vrijblijvend advies)

x	**Afstudeerdossier wordt op afgesproken datum ingeleverd** Inleverdatum: 8 januari 2016
	Afstudeerperiode wordt verlengd
	Student stopt met afstudeeropdracht

Naam begeleidend examinator: Hans de Vreught

Naam tweede examinator: Pieter Burghouwt

Datum: 1-12-2015

Dit formulier wordt door de tweede examinator digitaal ingevuld, waarna de begeleidend examinator het per email verstuurt naar de student met een cc naar de coördinator van ICT & Media @ Work (A.M.Schipper@hhs.nl). Het formulier dient door de student te worden opgenomen in het afstudeerdossier.

DE HAAGSE HOGESCHOOL

Faculteit IT & Design

Delft
Den Haag
Zoetermeer

Evaluatieformulier afstuderen

In te vullen door opdrachtgever c.q. bedrijfsmentor(en)

Student: Tim van Dijen - 00008055

Periode: 2015-2.1

Bedrijf c.q. instelling: SSC-ICT

Bedrijfsmentor: Dhr. R. P. van Kruistum

Plaats: Zoetermeer

Datum: 5 januari 2016

1. Heeft de student zich zelf snel en goed ingewerkt in het bedrijf en de uit te voeren afstudeeropdracht?

Tim heeft zich in zeer korte tijd de benodigde materie eigen gemaakt. Daarbij gaat Tim zelfstandig te werk en stelt indien nodig de vragen die hij nodig heeft om een antwoord te krijgen. Daarbij stelt Tim zich positief kritisch op en vraagt door wanneer zaken voor hem onduidelijk blijven.

2. Hoe beoordeelt u de communicatieve vaardigheden van de student (in de samenwerking met collega's, in contacten met de opdrachtgever, bij mondelinge presentaties, schriftelijke rapportages)?

Tim communiceert helder en zakelijk. Levert de gevraagde informatie tijdig op en stelt duidelijke kaders tav de wijze waarop hij zijn werk oplevert. Daarnaast staat Tim open voor feedback vanuit de opdrachtgever en gaat hier direct mee aan de slag.

3. Hoe heeft de student tijdens het uitvoeren van de opdracht gefunctioneerd?

- **Qua verantwoordelijkheid** goed
- **Qua zelfstandigheid** goed
- **Qua planmatig werken** goed
- **Qua creativiteit** goed
- **Qua productiviteit** goed
- **Qua samenwerken met collega's** goed
- **Qua draagvlakontwikkeling** voldoende
- **Qua inspelen op bedrijfscultuur** goed
- **Qua rekening houden met de specifieke context van het bedrijf** goed
- **Qua het op gang brengen van de nodige veranderingen** voldoende

4. Hoe beoordeelt u de kennis en kunde van de student in verhouding tot wat u verwacht van een bijna afgestudeerde?

Tim neemt het initiatief en verdiept zich in de materie. Hiermee laat Tim zien dat hij concepten die hem nog niet eigen zijn wel zeer snel eigen maakt. Het enthousiasme werkt aanstekelijk en Tim laat zien dat hij eveneens buiten zijn reguliere werktijd beschikbaar is voor het oppakken van bepaalde zaken in relatie tot het project.

5. Hoe beoordeelt u de kwaliteit van de opgeleverde (tussen)producten?

De producten zijn gedegen en voldoen ruimschoots aan de kaders die de organisatie stelt. Tim vraagt eveneens pro actief om feedback en input van zowel zijn directe collega's als de opdrachtgever.

6. Bent u tevreden over het opgeleverde (eind)product?

Hetgeen wat is opgeleverd voldoet ruimschoots aan de verwachting. Tim toont aan dat hij zich als een volwaardige technisch informatica professional functioneert.

- **In hoeverre heeft u gekregen wat is afgesproken?**

  Alles is conform de opdracht opgeleverd. Daarnaast heeft dit traject aanvullende aanbevelingen opgeleverd die eveneens geïmplementeerd worden in de nieuwe omgeving van de federatieve service.

- **In hoeverre voldoet het (eind)product aan uw verwachtingen?**

  Zie eerdere bullet

- **Wat is de bruikbaarheid en onderhoudbaarheid hiervan?**

  Idem

- **Wat gebeurt er met het opgeleverde (eind)product?**

  Alle zaken zullen conform het aangegeven advies worden geïmplememteerd

- **Kunt u direct met het opgeleverde product aan de slag?**

  Absoluut

7. Zijn er nog aspecten voor u van belang die nog niet aan de orde zijn geweest?

Neen, zoals eerder aangegeven laat Tim zien dat hij zowel op inhoudelijk vlak namelijk het realiseren van een technische oplossing en afstemming met de belangrijkste stake holders beheerst. Daarnaast kan Tim zijn advies en zienswijze duidelijk verwoorden naar de opdrachtgever en is in staat dit traject geheel zelfstandig te doorlopen.

8. Bent u bereid een volgende keer weer uw medewerking te verlenen aan het beschikbaar stellen van een afstudeerplaats (graag met toelichting)**?**

Absoluut! Het niveau van HHS studenten richting technische informatie vormen een welkome aanwinst voor de organisatie. Er zijn verschillende opdrachten beschikbaar om uit te voeren binnen de SSC-ICT organisatie.