SSC-ICT Haaglanden
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Federatieve authenticatie

Afstudeerscriptie

Vertrouwelijk

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

Referaat

Dijen, T. van, "Doorontwikkeling Federatieve Service", afstudeerscriptie, Technische Informatica, Haagse Hogeschool, 2016.

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 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.

Deze afstudeerscriptie vloeit voort uit een doorontwikkelingstraject van de federatieve dienst van het Ministerie van Veiligheid en Justitie, waarbij gezocht is naar oplossingen voor veel voorkomende problematiek bij federatieve diensten, zoals informatiebeveiliging en governance. Op basis van de uitkomsten is een herontwerp gemaakt en geïmplementeerd in een testomgeving.

Descriptoren:
- Federatieve dienst
- Toegangsbeheer
- Authenticatie
- Afstudeerscriptie

Documenthistorie

Versie	Status	Datum	Wijzigingen
0.1	Concept	16-11-2015	Eerste concept voor conceptbespreking
0.2	Concept	22-11-2015	Verwerking commentaar Dhr. De Vreught
0.9	Concept	30-11-2015	Conceptversie voor TTA
1.0	Definitief	7-1-2015	Vastgesteld na verwerking commentaar TTA

Voorwoord

Voor u ligt mijn afstudeerscriptie, waarin verslag wordt gedaan van de herontwikkeling van de federatieve dienst van het Ministerie van Veiligheid en Justitie. De opdracht hierbij was om de eisen/wensen van de klant en de problematiek met de huidige dienst in kaar te brengen en met een herontwerp te komen. Het herontwerp is vervolgens ook in de praktijk gebracht in een testomgeving. De opdracht is uitgevoerd bij de beheerpartij van de dienst, SSC-ICT Haaglanden te Zoetermeer.

Bij het uitvoeren van deze opdracht heb ik van verschillende personen steun, hulp en advies gekregen. Als eerste wil ik Paul van Kruistum bedanken voor het bieden van de mogelijkheid tot het uitvoeren van deze afstudeeropdracht. Daarnaast wil ik ook graag Jan Over, domeinarchitect Identity & Access Management, bedanken voor de intensieve samenwerking bij de totstandkoming van het resultaat.

Tevens gaat dank uit naar Hans de Vreught en Pieter Burghouwt, respectievelijk begeleidend en tweede examinator, die met een deskundige en kritische blik de scriptie hebben beoordeeld en tips en adviezen hebben gegeven.

Tot slot wil ik opmerken dat in een aantal gevallen wordt gerefereerd aan vertrouwelijke documenten die als input voor de afstudeeropdracht hebben gediend. Waar van toepassing is dit duidelijk kenbaar gemaakt.

Tim van Dijen
Pijnacker, januari 2016

Inhoudsopgave

1. Inleiding

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 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. Dit vertrouwen stoelt op het op orde zijn van het Identity Management van de Identity Provider en is meestal gebaseerd op contractuele afspraken tussen organisaties.

De afstudeeropdracht behelst een herontwerp op basis van een definitiestudie van de federatieve dienst van het Ministerie van Veiligheid en Justitie. De definitiestudie geeft antwoord in de (on)mogelijkheden, complicaties en consequenties van de betreffende herontwikkeling op het gebied van techniek/product/processen, tijd, geld en risico's. Het hieruit voortkomende systeemconcept is vervolgens uitgewerkt tot een technisch ontwerp en een implementatie in een testomgeving. Hierbij is ook getest op functionele en technische specificaties.

1.1 Aanleiding

Een gedeelte van de federatieve dienst van het Ministerie van Veiligheid en Justitie is in het verleden neergezet als Proof of Concept, waarbij niet of nauwelijks is gekeken naar zaken als beveiliging, schaalbaarheid, beschikbaarheid en beheerbaarheid. Doordat de live-gang van de dienst een hoge urgentie kende door politieke druk is deze PoC-omgeving vervolgens ingezet als productieomgeving, waarbij te weinig aandacht is geweest voor het beheer, de beveiliging, documentatie en de borging van kennis. Dit staat momenteel de ontwikkeling van de dienst behoorlijk in de weg omdat het aansluiten van nieuwe Justitie-onderdelen langzaam en moeizaam verloopt. Hierdoor is de directe behoefte ontstaan om de dienst door te ontwikkelen en is door het Ministerie van Veiligheid en Justitie opdracht hiertoe verleend aan SSC-ICT Haaglanden.

2. Organisatie: 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.

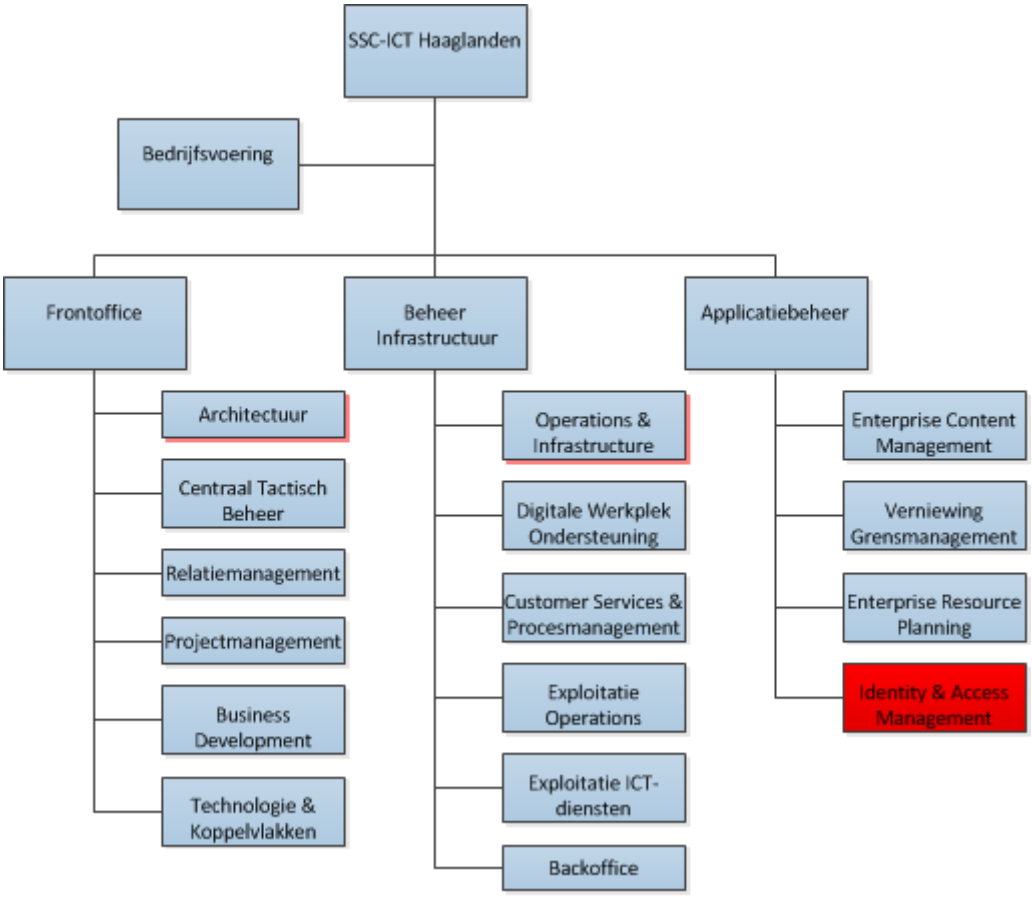
Het verzorgingsgebied is verspreid over bijna alle departementen binnen de Rijksoverheid. Naast reguliere beheertaken voor een 7x24-uurs dienstverlening is SSC-ICT Haaglanden verantwoordelijk voor projecten en programma's die een bijdrage leveren aan een compacte en duurzame overheid.

Niet onbelangrijk om te vermelden is dat de organisatie recent is gevormd door het samenvoegen van meerdere ICT-dienstverleners, te weten het Gemeenschappelijk Dienstencentrum ICT (voormalig onderdeel van Ministerie van Veiligheid en Justitie) en SSC-ICT (Ministerie van Infrastructuur en Milieu). Het samenvoegen van beide organisaties tot één SSC-ICT is nog in volle gang en dus functioneren de beide onderdelen nog veelal als zelfstandige organisaties. Zie op de volgende pagina Figuur 1: Organigram SSC-ICT Haaglanden.

2.1 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.

De afstudeeropdracht wordt uitgevoerd op de afdeling Identity & Access Management. Tijdens de definitiefase is echter nauw contact met afdeling Architectuur binnen de organisatie. Voor de realisatiefase wordt een beroep gedaan op de systeem- en netwerkbeheerders van afdeling Operations & Infrastructure.



Figuur 1: Organigram SSC-ICT Haaglanden

2.2 Ministerie van Veiligheid en Justitie

Het Ministerie van Veiligheid en Justitie is de grootste klant van SSC-ICT en tevens het grootste departement met maar liefst 60.000 FTE, verdeeld over drieëntwintig onderdelen, waarvan sommigen zelfstandig zijn (ZBO's). De laatste jaren focust het ministerie op betere samenwerking en eenvoudigere gegevensuitwisseling tussen de verschillende onderdelen, waarop ook de federatieve dienst gericht is.

2.3 Stakeholders

Samengevat zijn de volgende stakeholders te onderkennen bij de federatieve dienst:

- Ministerie van Veiligheid en Justitie – Klant / strategisch beheerder;
- Justitiële informatiedienst – Onderdeel van justitie en tactisch beheerder van de federatieve dienst. Tevens technisch beheerder van (een gedeelte van) de federatieve dienst;
- SSC-ICT – Technisch beheerder van (een gedeelte van) de federatieve dienst.

3. Opdracht

Dit hoofdstuk is een korte toelichting op de afstudeeropdracht. Voor een uitgebreide opdrachtomschrijving, zie Bijlage A - Goedgekeurd afstudeerplan.

3.1 Onderwerp

Het onderwerp van deze afstudeerscriptie betreft het doorontwikkelen van de federatieve dienst van het Ministerie van Veiligheid en Justitie. De dienst faciliteert eenvoudige samenwerking en gegevensuitwisseling tussen verschillende onderdelen van het departement.

3.2 Probleem- en doelstelling

Voor deze afstudeeropdracht is een probleemstelling geformuleerd en is een doelstelling vastgesteld.

Probleemstelling:
Als gevolg van bij de inrichting 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.

Doelstelling:
Het doel van de opdracht is om binnen een 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.

3.3 Resultaat

Het resultaat van de opdracht is een nieuw ontwerp en een nieuw te realiseren testomgeving. Het ontwerp dient hierbij te voldoen aan de eisen die gesteld worden ten aanzien van de beveiliging, schaalbaarheid, beschikbaarheid en beheerbaarheid van de dienst.

3.4 Aanpak

Voor de uitvoer van de opdracht wordt gebruik gemaakt van de watervalmethode. De watervalmethode is met name geschikt is voor systeemontwikkeling, voorziet in een duidelijke afbakening van fasen en door bij elke fase een mijlpaal te definiëren kan de voortgang van het project gemonitord worden. Hoewel Prince2 binnen SSC-ICT de standaard is voor projecten, is het gezien de omvang van het project niet reëel om hier een projectmanagementmethode bij te gebruiken.

Vanuit Bijlage A - Goedgekeurd afstudeerplan is de volgende fasering bepaald:

> Oriëntatiefase (Plan van Aanpak)
> Definitiefase (Definitiestudie)
> Ontwerpfase (Technisch Ontwerp)
> Realisatiefase (Testrapportage)

4. Theoretische achtergrond

In de klassieke vorm vindt authenticatie altijd plaats bij de aanbieder van een dienst. Op deze manier heeft vrijwel elke organisatie die diensten via het internet aanbiedt de authenticatie van zijn gebruikers geregeld.

Vanuit het perspectief van de gebruiker ziet het plaatje er echter al snel minder prettig uit. Die heeft voor elke dienst die hij wil gebruiken een separaat authenticatiemiddel, wat er toe leidt dat hij vele wachtwoorden moet onthouden en pasjes bij zich moet hebben; de digitale sleutelbos is een feit. Dit leidt ertoe dat mensen overal dezelfde wachtwoorden gaan gebruiken, of deze gaan opschrijven om te kunnen onthouden. Zie Figuur 2: Gevolgen digitale sleutelbos.

Figuur 2: Gevolgen digitale sleutelbos

De Nederlandse overheid doet voor de communicatie met burgers een poging dit terug te dringen middels het DigID-stelsel; één authenticatiemiddel voor alle digitale overheidsdiensten.

4.1 Federatieve authenticatie

Bij federatieve authenticatie, waar DigID een voorbeeld van is, zijn de applicatie en authenticatiebron van elkaar gescheiden. De applicatie (service provider) vertrouwt voor de authenticatie op een externe bron (identity provider). Zo kunnen vertrouwensrelaties opgebouwd worden tussen verschillende organisaties die applicaties en identiteiten met elkaar willen delen. Dit heeft als voordeel dat niet elke applicatie zijn eigen authenticatievoorziening hoeft te ontwikkelen (minder kans op fouten / lekken) en dat een eindgebruiker altijd kan authentiseren bij een vertrouwde authenticatievoorziening van de eigen organisatie.

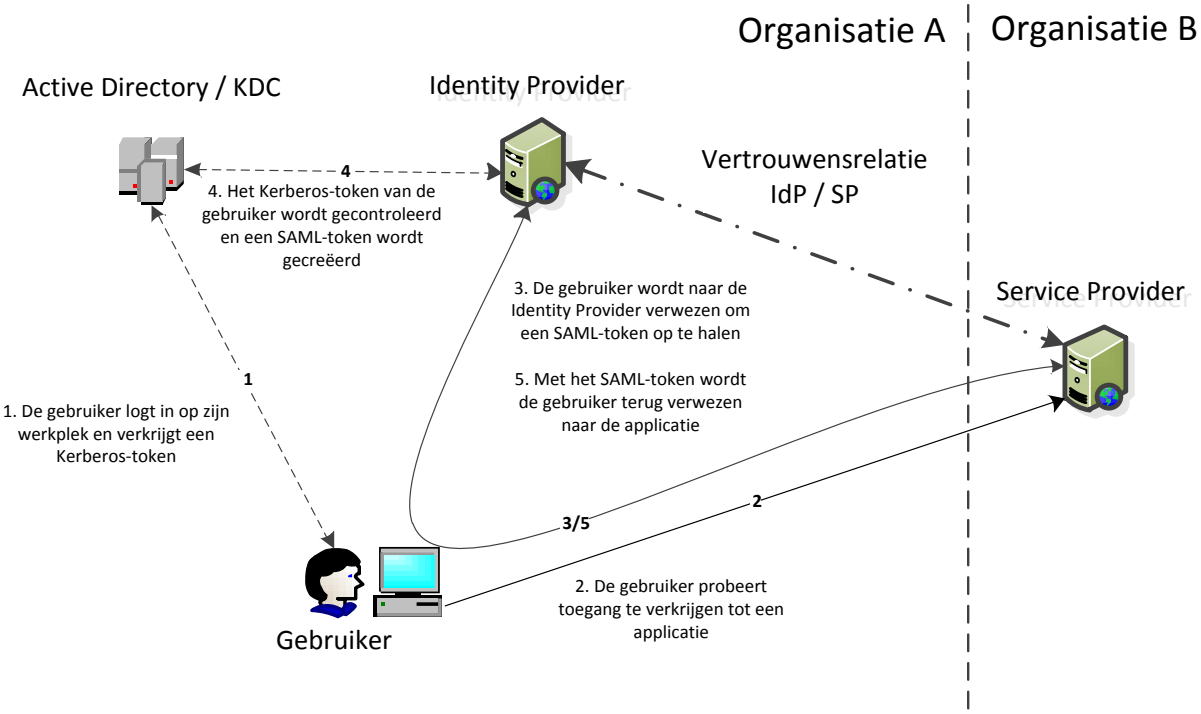
4.2 Federatief vertrouwen

Het vertrouwen wat partijen in elkaar hebben is meestal contractueel vastgelegd. Technisch gezien wordt het vertrouwen tussen een service provider en een identity provider bereikt middels PKI-certificaten, die de partijen van elkaar vertrouwen. Het onderlinge berichtenverkeer, op basis van het SAML-protocol, wordt ondertekend met deze PKI-certificaten. Desgewenst kunnen de berichten ook nog versleuteld worden.

4.3 Voorbeeld authenticatie

In Figuur 3: Voorbeeld authenticatie wordt een voorbeeld weergegeven van een standaard situatie bij federatieve authenticatie. Een gebruiker wil gebruik maken van een applicatie bij een andere organisatie. De authenticatie vindt echter plaatst bij de eigen organisatie. In stap 3 en 5 worden er SAML-berichten uitgewisseld middels http redirects, transparant voor de gebruiker. Zo wordt een Single Sign-on ervaring gecreëerd.

De gebruiker kan echter ook buiten de organisatie zitten, waardoor er geen Kerberos-token aanwezig is. In dat geval krijgt de gebruiker bij de Identity Provider een loginscherm te zien en zal hij geldige credentials moeten invoeren en wordt er in stap 4 een LDAP-authenticatie gedaan. In dit geval is er dus geen Single Sign-on ervaring voor de gebruiker.



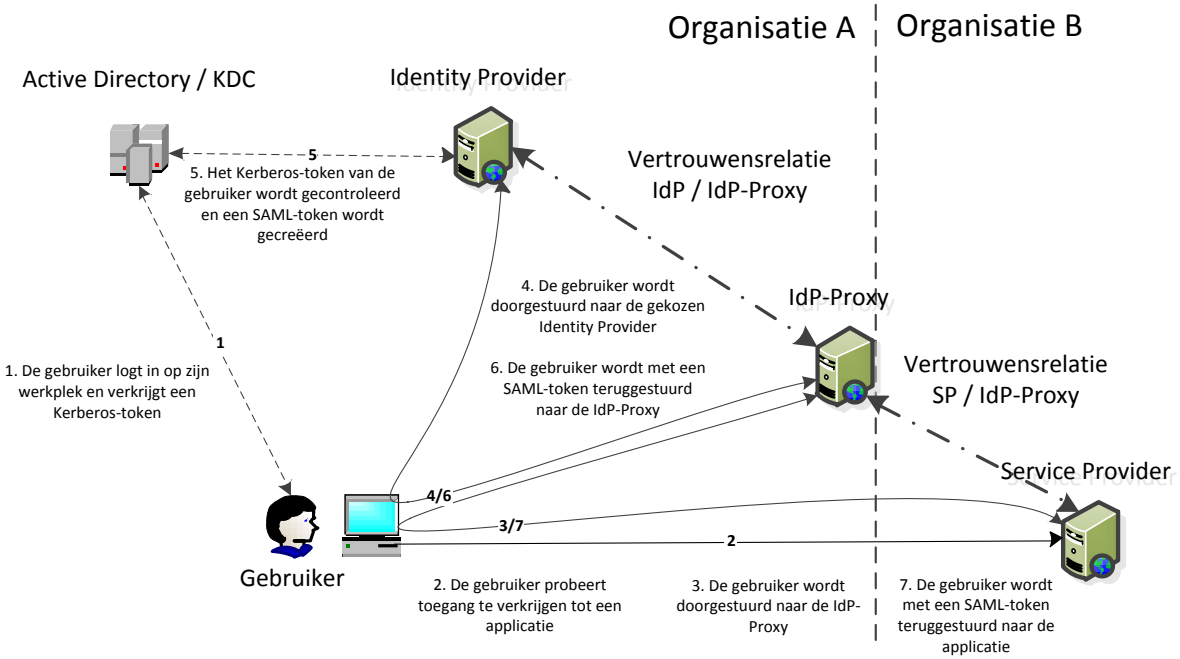
Figuur 3: Voorbeeld authenticatie

Federatieve ketens kunnen behoorlijk complex worden, bijvoorbeeld wanneer meerdere organisaties zijn aangesloten met elk een eigen Identity Provider. In zulke gevallen wordt er vaak een extra component geïntroduceerd; een IdP-Proxy. Deze term is vaak verwarrend, omdat het woordje 'proxy' associaties oproept met netwerk-proxy's. In het geval van federatieve authenticatie is het echter vooral een message broker / doorgeefluik van berichtenverkeer. Aanvullende functionaliteit is het voorzien in een WAYF[1]-pagina (Figuur 4: Voorbeeld WAYF-pagina) waarin de eindgebruiker kan kiezen waar hij zich wil authentiseren. Dit zal vrijwel altijd de eigen organisatie zijn. Ook kan een IdP-Proxy de vertaling doen tussen verschillende federatieve protocollen, zoals het oude SAML 1.0 of WS Federation.

[1] Where Are You From

Figuur 4: Voorbeeld WAYF-pagina

De gebruiker hoeft de WAYF-pagina echter niet altijd te zien. Vaak kan op basis van bijvoorbeeld het IP-adres van de gebruiker of de aanwezigheid van een cookie de keuze gemaakt worden. Op die manier blijft de Single Sign-on ervaring behouden. Zie Figuur 5: Voorbeeld authenticatie met IdP-Proxy voor een voorbeeld van een complexere keten met een IdP-Proxy.



Figuur 5: Voorbeeld authenticatie met IdP-Proxy

In Figuur 5: Voorbeeld authenticatie met IdP-Proxy is de IdP-Proxy op de stippellijn tussen Organisatie A en Organisatie B getekend. Echter is de locatie van het component niet belangrijk, zolang deze maar benaderbaar is voor alle eindgebruikers. De IdP-Proxy is feitelijk de spin in het web en vormt een koppelvlak naar één of meerdere Service Providers en naar één of meerdere Identity Providers. Bovenstaande voorbeeld kan bijvoorbeeld nog uitgebreid worden met een Identity Provider bij Organisatie B, of een Service Provider bij Organisatie A.

5. Oriëntatiefase

De voorbereiding kenmerkt zich vooral door het bekend raken met de theorie. Een andere belangrijke stap in het project is het bepalen van het Plan van Aanpak met de opdrachtgever. Hierbij is vastgesteld dat de doelstelling het volgende uitgangspunt heeft:

> *De opdrachtgever wil antwoord op de vraag of en in hoeverre het mogelijk en wenselijk is om de dienst te vereenvoudigen, goedkoper te maken en verder te professionaliseren zodat een toekomstvaste en makkelijk uitbreidbare dienst ontstaat. De opdracht is om tot een voorstel te komen, dit uit te werken en in een testomgeving te realiseren.*

Voor de oriëntatiefase zijn vooraf de volgende stappen vastgesteld:

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

Het mijlpaalproduct voor deze fase is het Plan van Aanpak. Een belangrijk deel van het Plan van Aanpak is reeds in Hoofdstuk 3 aan de orde geweest.

5.1 Opstellen Plan van Aanpak

De volgende onderdelen zijn in het Plan van Aanpak behandeld:

- Opdrachtomschrijving;
- Randvoorwaarden;
- Op te leveren resultaten;
- Risicoanalyse;
- Planning;
- Kwaliteit
- Projectorganisatie.

Het volledige Plan van Aanpak is te vinden onder Bijlage B - Plan van Aanpak.

Risicobeheersing

Voor de risicoanalyse zijn een aantal stappen doorlopen om risico's in kaart te brengen:

- Risico's identificeren;
- Risico's inschatten;
- Risico's evalueren.

Eén van de geïdentificeerde risico's bij dit project is het niet tijdig geleverd krijgen van de testomgeving. Een werkende testomgeving is het projectresultaat, dus zonder een tijdige levering van deze testomgeving komt het project ernstig in gevaar.

Bij de risico-evaluatie wordt uiteindelijk gekeken of een risico acceptabel is, en zo niet, wat er aan gedaan kan worden. Hierbij moet gedacht worden aan preventieve en repressieve maatregelen, of uitwijkmogelijkheden. In het voorbeeld van de testomgeving zijn deze als volgt:

Kansverlagende maatregel:
Aanvragen voor servers en infrastructurele zaken tijdig indienen.

Impactverlagende maatregel:
Tijdig escaleren vanuit het project bij de betreffende beheerpartij wanneer de aanvraag niet voortvarend wordt opgepakt.

Uitwijkmogelijkheid:
De omgeving lokaal in virtuele machines opbouwen. Het gevolg hiervan is wel dat niet representatief getest kan worden.

Kwaliteitbewaking

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

6. Definitiefase

Centraal in de definitiestudie staan de huidige problematiek en de veranderingsbehoefte. De belangrijkste informatiebron hiervoor zijn de Functionele Specificaties en het Pakket van Eisen welke door de klant zijn opgesteld. Deze zijn bijgevoegd onder Bijlage C – Functionele Specificaties + Pakket van Eisen.

Voor de definitiefase zijn vooraf de volgende activiteiten vastgesteld:

- Verdieping
- In kaart brengen huidige situatie
- 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

Het rapport "Definitiestudie" voortvloeiend uit de definitiefase is toegevoegd onder Bijlage D – Definitiestudie

6.1 Verdieping

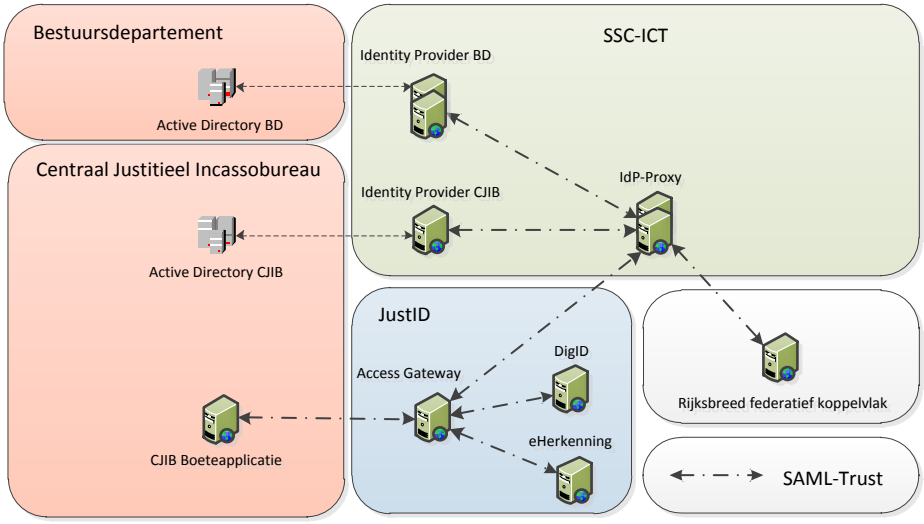
Naast de initiële input voor het project zijn ook andere relevante bronnen geraadpleegd, zoals het bestaande Functioneel Ontwerp, de aansluitvoorwaarden van de rijksbrede federatieve dienst, installatiehandleidingen en een aantal beleidsdocumenten met betrekking tot informatiebeveiliging, het gebruik van PKI en een aantal best practices op het gebied van TLS, PKI en hardening.

Hieronder een aantal voorbeelden van technische eisen die vanuit de Baseline Informatiebeveiliging Rijksdienst (BIR) zijn gesteld aan een systeem:

- "Bij voorkeur is sleutelmanagement ingericht volgens PKI-Overheid"
- "Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie van gebruikers plaats."
- "De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst."

6.2 Huidige situatie

Aan de hand van de beschikbare informatie en een analyse van de werkelijke situatie is de huidige situatie in kaart gebracht om een zo goed mogelijk overzicht te krijgen. Zie Figuur 6: Huidige situatie - functioneel op de volgende pagina.



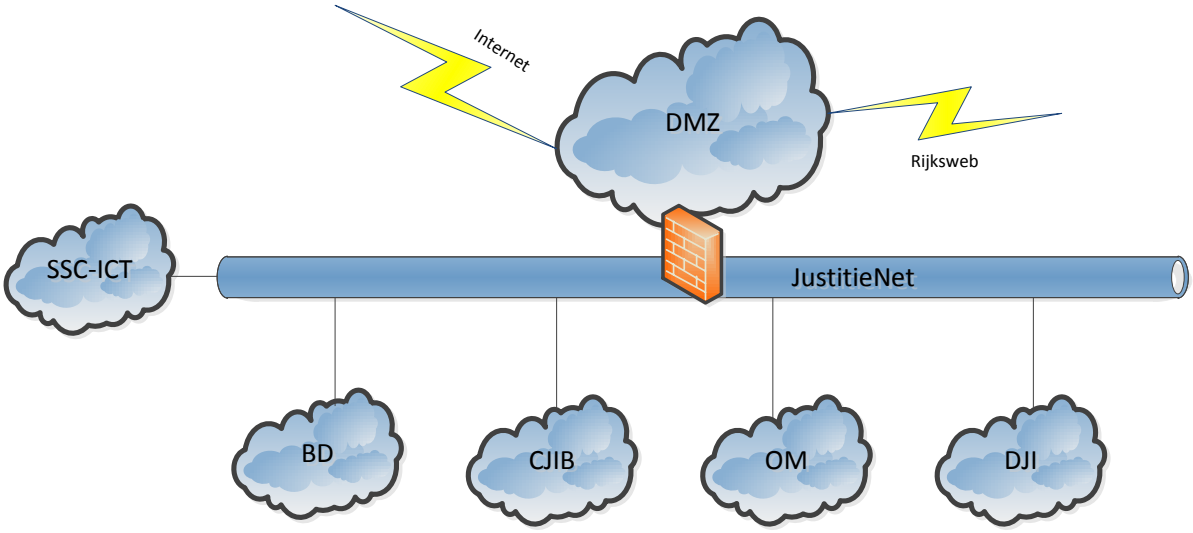
Figuur 6: Huidige situatie - functioneel

Zoals te zien in Figuur 6: Huidige situatie - functioneel zijn in de huidige situatie twee Justitie-onderdelen aangesloten op de federatieve dienst van het Ministerie van Veiligheid en Justitie, namelijk het bestuursdepartement (ministerie) zelf en het Centraal Justitieel Incassobureau. Beide onderdelen hebben hun eigen Identity Provider, gekoppeld aan een IdP-Proxy. Al deze componenten zijn in beheer van SSC-ICT. Alle applicaties (Service Providers), zoals de CJIB Boeteapplicatie, en externe Identity Providers zijn aangesloten op de Access Gateway van JustID. Deze Access Gateway kan technisch gezien worden als een IdP-Proxy en fungeert ook als spin in het web. De IdP-Proxy heeft tot slot nog een koppeling naar het rijksbrede koppelvlak, wat technisch eveneens gezien kan worden als een IdP-Proxy. Dit koppelvlak is ook in beheer bij SSC-ICT en is het aangewezen aansluitpunt voor ministeries en rijksbrede Service Providers. Het rijksbrede koppelvlak is echter niet relevant voor de opdracht en zal niet verder uitgewerkt worden.

Netwerk

Alle Justitie-onderdelen hebben hun eigen VLAN binnen het overkoepelende 'JustitieNet', welke zij over het algemeen zelf beheren. Zie Figuur 7: Huidigesituatie – Netwerk op de volgende pagina. SSC-ICT heeft als beheerpartij van JustitieNet en dienstaanbieder ook een VLAN binnen dit netwerk, waar de diensten aan de verschillende Justitie-onderdelen plaatst. Zo ook de Identity Providers die worden afgenomen door het bestuursdepartement en het CJIB.

De gemeenschappelijke DMZ wordt gebruikt voor verschillende diensten van Justitie-onderdelen aan de buitenwereld, zoals gebruikers op het internet en bij andere ministeries (Rijksweb VPN). Hier zijn o.a. de IdP-Proxy, Access Gateway en de CJIB Boeteapplicatie uit Figuur 6: Huidige situatie - functioneel te vinden. De DMZ van Justitie wordt beheerd door een marktpartij.



Figuur 7: Huidigesituatie – Netwerk

6.3 Analyse huidige situatie

Op basis van de documenten welke gelezen zijn in de verdiepingsstap (6.1) en het bekijken van de huidige situatie vallen gelijk een aantal zaken. Deze worden hieronder opgesomd.

Algemeen

1. De aanwezige documentatie is incompleet en mist basale zaken als een actueel Technisch Ontwerp en installatiehandleidingen.

2. Het aantal beleidsregels is opmerkelijk groot, zijn vaak voor meerdere interpretaties vatbaar, inconcreet en de maatregelen zijn vaak niet geconcretiseerd in technische eisen. Veel gebruikte termen in deze documenten zijn “Sterke authenticatie”, “onvertrouwde omgeving” en “Bij voorkeur”. Zie ook de voorbeelden van beleidsregels in paragraaf 6.1.
   -

Beveiliging

1. De Identity Providers zijn, in tegenstelling tot de aanbevelingen van de softwareleverancier, niet in de DMZ geplaatst maar in het interne netwerk. Met de wens uit de Functionele Specificaties (Bijlage C) om de IdP-Proxy en Identity Providers ook via internet benaderbaar te maken, ontstaat straks een situatie waarbij gebruikers van buitenaf op een webserver terecht komen in het interne netwerk. Weliswaar staan de Identity Providers in het aparte SSC-ICT gedeelte van JustitieNet, maar dit stukje netwerk is niet bedoeld als pseudo-DMZ.

2. Uit de installatiehandleidingen blijkt dat zowel de Identity Providers als de IdP-Proxy niet gehardend zijn; geen SELinux of host-firewall. Dit zou wel moeten volgens de BIR. Voor de IdP-Proxy is er wel een uitzondering gemaakt voor de toepassing van SELinux, omdat dit door het complexe software-product niet mogelijk was dit werkend te krijgen.

3. De Identity Providers van het bestuursdepartement zijn binnen het SSC-ICT gedeelte van JustitieNet niet verder gecompartimenteerd, terwijl dit wel zou moeten volgens het geldende beleid[2].

4. Er vindt geen CRL-controle op certificaten, waardoor ingetrokken certificaten ongemerkt gebruikt kunnen blijven worden. Dit is in strijd met best practices, zoals die van Geant[3].

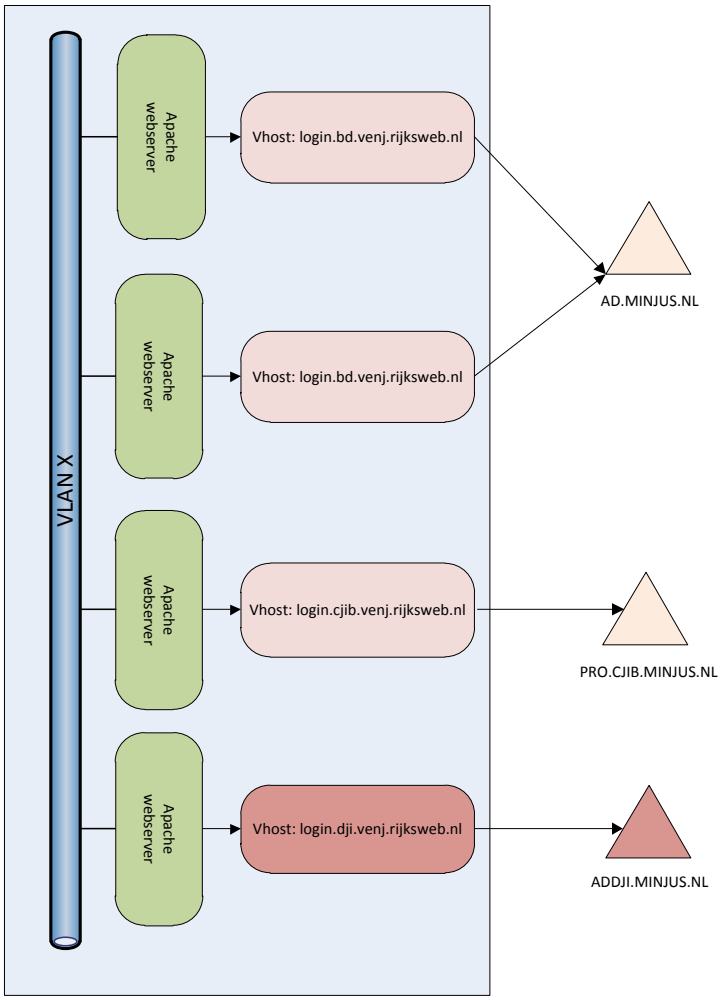
5. Uit de installatiehandleiding blijkt dat communicatie tussen de Identity Providers en de achterliggende Active Directories niet versleuteld wordt. Dit is in strijd met de BIR, welke stelt dat alle communicatie waar mogelijk versleuteld moet worden.

6. Uit de installatiehandleidingen blijkt dat er, in tegenstelling tot wat de BIR vereist (zie 6.1), op een aantal plaatsen gebruik wordt gemaakt van self-signed PKI-certificaten.

Schaalbaarheid
De Identity Providers zijn niet achter een load balancer geplaatst, waardoor het uitbreiden bij capaciteitsproblemen niet snel en makkelijk te doen is. Dit past niet in het beeld dat de dienst onder de Te Beschermen Belangen (TBB) valt, zoals te lezen valt in het oude Functioneel Ontwerp[4]. De IdP-Proxy is wél achter een load balancer geplaatst, waardoor deze wel voldoet aan de eisen voor schaalbaarheid.

Beschikbaarheid
De Identity Provider van het CJIB is uit kostenoogpunt enkelvoudig neergezet waarmee concessies gedaan zijn aan de eisen voor beschikbaarheid, zoals gesteld in het oude Functioneel Ontwerp. Voor de Identity Provider van het Bestuursdepartement is er wel een soort fail-over constructie gemaakt met twee nodes en een softwarematige truc (Zie Figuur 8: Single-tenant Identity Providers). Hiervan is echter in een eerder stadium aangegeven door systeembeheer dat deze truc niet ondersteund wordt door de leverancier van het besturingssysteem.

[2] Beleidsdocument inzake hardening – Niet openbaar
[3] Zie bronvermelding
[4] Bestaande Functioneel Ontwerp - Niet openbaar



Figuur 8: Single-tenant Identity Providers

Beheerbaarheid
Voor de IdP-Proxy en de Identity Providers zijn verschillende producten ingezet. Het product van de IdP-Proxy is bijzonder complex en eigenlijk niet bedoeld om als IdP-Proxy ingezet te worden. Dit blijkt uit correspondentie[5] tussen SSC-ICT en de leverancier. Naslag van de documentatie van de gebruikte producten wijst uit dat het product wat wordt ingezet voor de Identity Providers ook als IdP-Proxy kan worden ingezet.

6.4 Achterhalen behoeften

Aanvullend op de informatie uit de Functionele Specificaties, het Pakket van Eisen en de analyse van de bestaande situatie zijn interviews gehouden met de opdrachtgever (als zijnde proxy voor de klant), de beheerder en de domeinarchitect Identity & Access Management. Per interview zijn vooraf een aantal relevante vragen opgesteld. De interviews zijn bedoeld om een beter beeld te krijgen van de behoeften van de betrokken partijen.

[5] Correspondentie tussen SSC-ICT en softwareleverancier – Niet openbaar

Een voorbeeld van een vraag aan de opdrachtgever:

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.

Een vraag aan de beheerder legt ook gelijk een aantal pijnpunten bloot:

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 [...].
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.

Gespreksverslagen van de interviews zijn te vinden onder Bijlage E – Gespreksverslagen.

6.5 Analyse interviews

De verschillende componenten, maar ook de federatie als geheel kennen zo hun problemen. 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.

IdP-Proxy:
- Veel software-bugs die traag worden verholpen, wat de ontwikkeling van de dienst beperkt;
- Maatwerk-aanpassingen nodig om aan de wensen van de klant te voldoen, wat leidt tot hoge ontwikkelkosten;
- 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.

6.6 Ontwikkelingen rijksbreed

Doordat er ook op rijksbreed niveau de nodige ontwikkelingen zijn op het gebied van federatie, is er ook gezocht naar meer informatie hieromtrent. De verwachting vooraf was dat deze ontwikkelingen ook gevolgen zouden hebben voor de departementale federaties. Omdat ook hergebruik een belangrijke pijler is binnen de overheid, is de impactanalyse die door SSC-ICT is gedaan voor de rijksbrede federatie opgevraagd en bestudeerd.

De belangrijkste punten die uit de impactanalyse naar voren komen zijn:

- SAML wordt de "de facto" standaard en overige protocollen worden uitgefaseerd;
- Legacy-applicaties die niet SAML-aware zijn moeten achter een Access Gateway worden geplaatst;
- Er komt een koppelvlak voor externe authenticatie, waar de departementen gebruik van kunnen maken;
- Er zal gebruik gemaakt worden van open source, tenzij (comply or explain);
- Two-way trusts tussen verschillende federatieve componenten.

De gevolgen voor de VenJ federatieve dienst hiervan is dat het VenJ-koppelvlak in ieder geval met SAML overweg moet kunnen voor de aansluiting op de rijksbrede federatie en dat de implementatie van de externe Identity Providers (DigID en eHerkenning) op VenJ-niveau mogelijk overbodig is door de introductie van een rijksbreed extern koppelvlak. Op dit moment is er nog geen two-way trust met de rijksbrede federatie, maar wordt wel al gebruik gemaakt van SAML.

6.7 Bepalen gewenste situatie

Aan de hand van alle informatie die op dit punt beschikbaar is kunnen de systeemeisen bepaald worden. Functioneel moet de dienst tenminste aan de in de Functionele Specificaties (Bijlage C) gestelde authenticatiescenario's voldoen. Om deze scenario's duidelijk inzichtelijk te krijgen zijn deze in de Definitiestudie (Bijlage D) volledig functioneel uitgeschreven. Hieronder volgen een tweetal voorbeelden van authenticatiescenario's die de dienst na een doorontwikkeling moet kunnen faciliteren.

Scenario #2: 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 #10: 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.

Alle scenario's zijn vervolgens verwerkt in een tabel waarin wordt uitgezet waar de gebruiker, de client, de Identity Provider en de Service Provider zich bevinden in het gegeven scenario. Zie tabel 1 hieronder.

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

Tabel 1: Authenticatiescenario's gewenste situatie

Uit de tabel kan goed afgeleid worden dat een doorontwikkeling van de dienst in drie brokken te verdelen is, namelijk federatieve authenticatie voor:

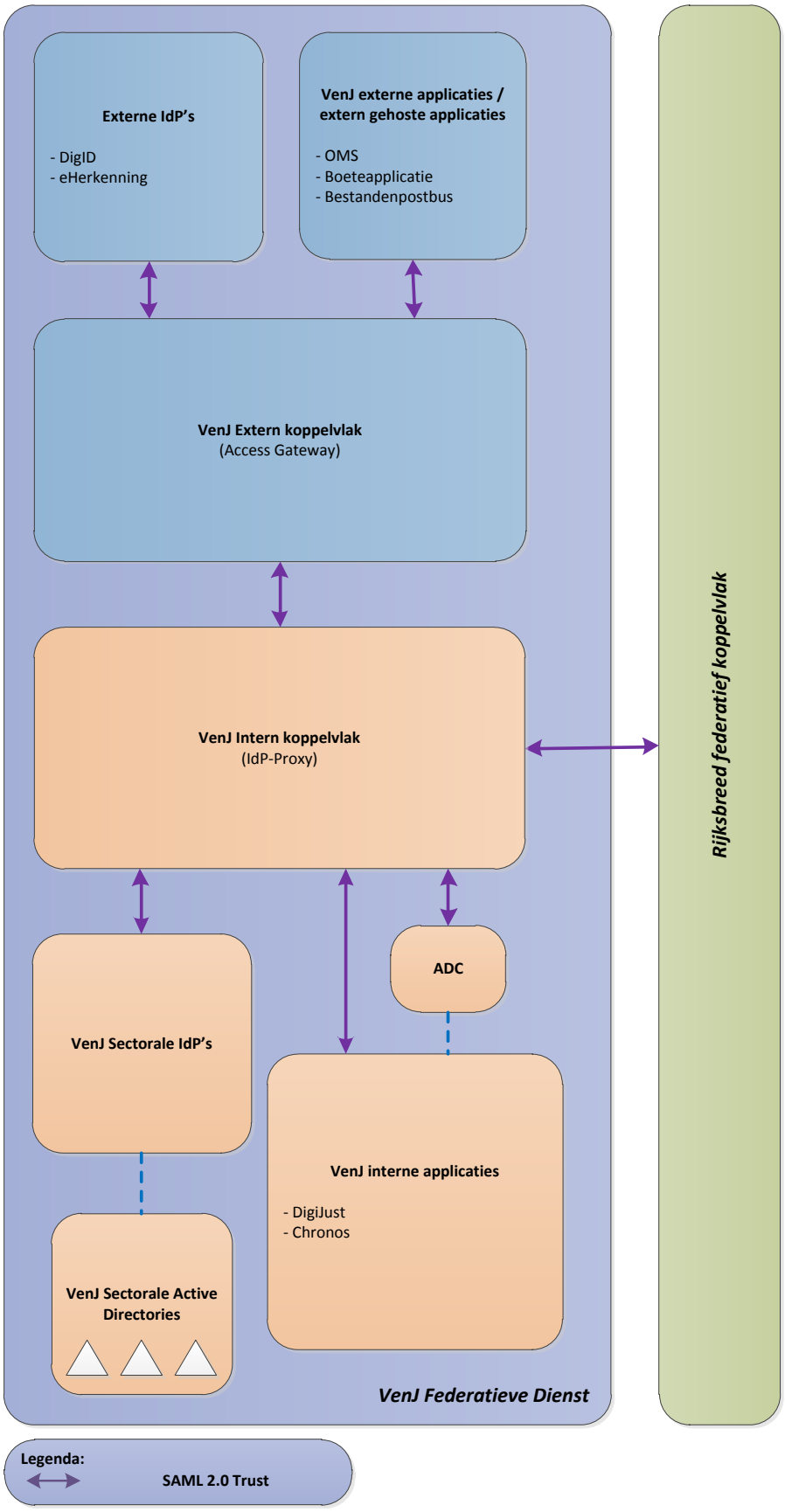
- VenJ-medewerkers (intern Justitie);
- Rijksmedewerkers (buiten Justitie, binnen de Rijksoverheid);
- Derden / Niet-Rijksoverheid.

Overige uitgangspunten
Behalve de authenticatiescenario's die ondersteund moeten worden stelt de klant in de Functionele Specificaties (Bijlage C) nog een aantal uitgangspunten waaraan de dienst moet voldoen:

- Er is slechts één trust met de Rijksbrede federatie;
- De trust met de Rijksbrede federatie is een two-way trust;
- Er is een logische scheiding tussen intern en extern verkeer;
- De oplossing is schaalbaar en hoogbeschikbaar;
- De eindgebruiker krijgt met zo min mogelijk 'hops' te maken;
- De oplossing voldoet minimaal aan de BIR en aan overig geldend beleid op het gebied van (informatie-)beveiliging.

6.8 Referentiearchitectuur

In samenwerking met de domeinarchitect is een referentiearchitectuur bedacht welke beantwoordt aan de Functionele Specificaties en het Pakket van Eisen (Bijlage C) en de aanvullende wensen vanuit applicatiebeheer. Deze referentiearchitectuur (zie Figuur 7) kenmerkt zich door een logische scheiding tussen interne (oranje) en externe (blauw) federatie. Applicaties die aan de buitenwereld beschikbaar gesteld moeten worden kunnen aan het externe koppelvlak gekoppeld worden. Interne applicaties zoals bedrijfsvoeringsapplicaties, kunnen aan het interne koppelvlak aansluiten.



Figuur 9: Referentiearchitectuur

7. Ontwerpfase

In de ontwerpfase zijn de uitgangspunten uit de definitiestudie verder geconcretiseerd tot een Technisch Ontwerp. Dit ontwerp is bijgevoegd onder is bijgevoegd onder Bijlage F - Technisch Ontwerp.

Voor de ontwerpfase zijn vooraf de volgende activiteiten vastgesteld:

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

7.1 Technische eisen

De uitgangspunten uit de definitiestudie laten zich vertalen naar technische eisen. Deze zijn per component uitgezet in een tabel en geprioriteerd (1 t/m 5, waarbij 1 het hoogst is). Deze werkwijze maakt in één oogopslag duidelijk wat er binnen het project gerealiseerd moet worden.

Voor de Identity Providers zijn bijvoorbeeld de volgende eisen vastgesteld:

#	Requirement	Prioriteit
REQ01	De Identity Provider dient hoogbeschikbaar te zijn; als de dienst niet beschikbaar is kunnen gebruikers niet authentiseren.	1
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

7.2 Logisch ontwerp

Aan het ontwerp uit Figuur 4 is nauwelijks iets veranderd. De enige wijziging hierop is dat Justitie-brede bedrijfsvoeringsapplicaties aangesloten worden op de IdP-Proxy in plaats van op de Access Gateway. Hiermee wordt de logische scheiding tussen intern en extern verkeer bewerkstelligd, zoals ook is bepaald in de referentiearchitectuur (Figuur 7). Ook blijft het aantal 'hops' zo kort mogelijk voor de eindgebruiker. Al deze zaken zijn transparant voor de eindgebruiker; de authenticatiescenario's zijn dan ook niet gewijzigd.

7.3 Fysiek ontwerp

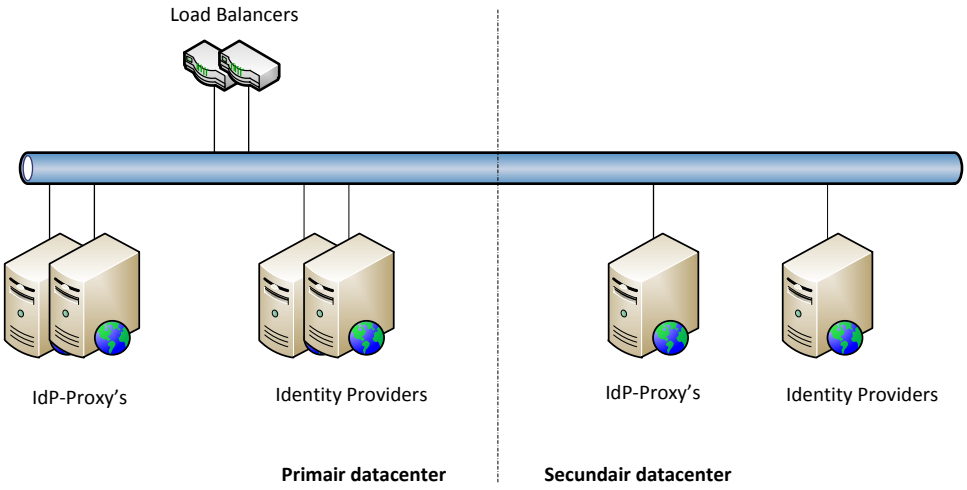
Bij het ontwerp is gebruik gemaakt van een drietal best practices[6] van Géant met betrekking tot informatiebeveiliging, PKI en hardening. Géant is een samenwerkingsverband van Europese organisaties die hoger onderwijsinstellingen met elkaar verbinden en heeft als doel om kennis en ervaring te bundelen. De best practices bieden dus handvatten en maatregelen die bijdragen aan het bereiken van de technische eisen en die breed worden gedragen door de academische wereld. Een voorbeeld van een toegepaste maatregel uit de best practice voor hardening is het gebruik van SELinux op alle machines.

De technische eisen laten zich vertalen naar een ontwerp waarin wordt voldaan aan deze eisen en aan de functionele eisen. In het voorbeeld van de bovenstaande REQ03 + REQ04 eisen betekent dit dat componenten achter een load balancer geplaatst worden.

De belangrijkste verandering ten opzichte van de bestaande situatie is dat de Identity Providers vanuit het internet netwerk naar de DMZ worden verplaatst. Met de wens om ook vanaf het internet gebruik te kunnen maken van de federatieve dienst zou hier een zeer onwenselijke situatie zijn ontstaan doordat gebruikers van buitenaf tot in het interne netwerk zouden binnenkomen. In de nieuwe situatie blijft de eindgebruiker waar deze hoort: in de DMZ, in een gescheiden VLAN. Van hieruit wordt onderwater verbinding gemaakt met de user directory in het interne netwerk. Daarmee wordt voldaan aan de eis voor compartimentering.

Met de keuze om de Identity Providers te verplaatsen is ook de mogelijkheid ontstaan om gebruik te maken van de reeds aanwezige load balancers in de DMZ. Door de Identity Providers ook samen te voegen op één cluster van webservers ontstaat een overzichtelijke en beheerbare situatie die ook voorziet in de eisen voor schaalbaarheid, fault tolerance en voor zover meetbaar ook aan de eis van beheerbaarheid door het terugdringen van het aantal te beheren servers.

De beheerder van de DMZ verdeelt cluster-nodes standaard over meerdere datacenters. Voor de Identity Providers wordt hiermee voldaan aan de eis van high availability. Zie Figuur 8 hieronder.



Figuur 10: High availability + Fault tolerance

[6] Zie bronvermelding

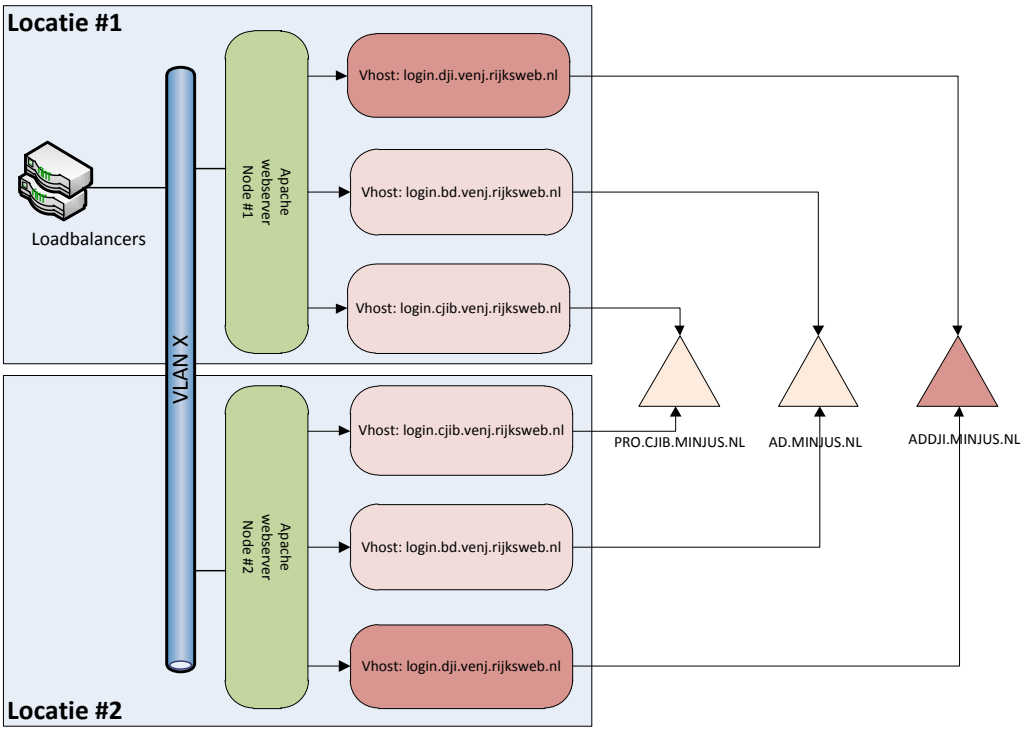
IdP-Proxy

Voor de IdP-Proxy is er voor gekozen om deze uit te voeren met een ander product, SimpleSAMLphp. Uit de definitiestudie bleek dat er al enige tijd problemen zijn met het bestaande product en dat functionaliteit ontbreekt. Navraag bij de leverancier wees uit dat het product oneigenlijk wordt gebruikt en eigenlijk niet geschikt is voor de rol van IdP-Proxy. SimpleSAMLphp daarentegen is specifiek bedoeld voor federatieve authenticatie, is beproefde technologie en wordt reeds ingezet voor de Identity Providers, waardoor de kennis over dit product al in huis is.

Deze keuze draagt bij aan een stukje minder complexiteit (betere beheerbaarheid) door het terugdringen van het aantal producten. Tevens komt het de klant tegemoet op het gebied van kosten, doordat er bespaard wordt op licentiekosten. Een extra besparen is nog het verdwijnen van de 'admin consoles' die het oude product kende. Dit scheelt over de gehele OTAP-straat vier (virtuele) machines.

Identity Providers

De Identity Providers worden in het nieuwe ontwerp samengevoegd tot één multi-tenant[7] IdP, door een cluster van webservers te configureren met meerdere 'virtual hosts'. Zie Figuur 9 voor schematische weergave.

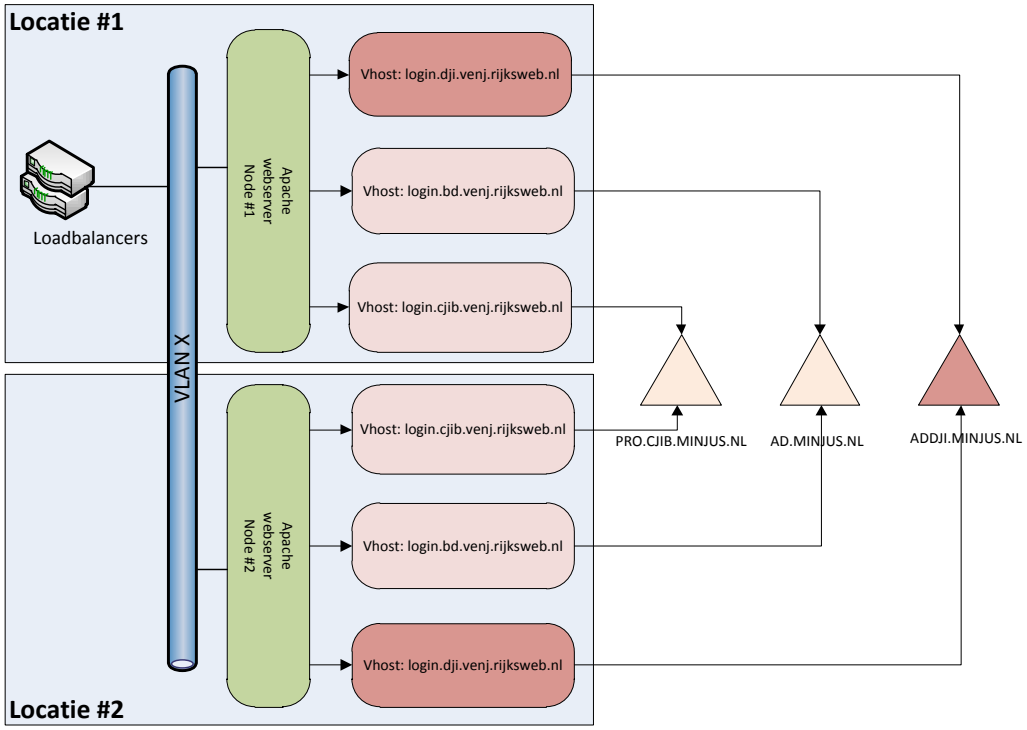


Figuur 11: Multi-tenant inrichting

[7] Multi-tenancy is een architectuur waarbij één fysieke instance meerdere klanten/groepen bedient en daarbij een logische scheiding hanteert.

Deze opstelling beantwoordt aan de gestelde eisen van high availability, fault tolerance, schaalbaarheid en compartimentering. Ook de voorheen enkel uitgevoerde IdP van het CJIB profiteert nu mee van deze functionaliteiten, doordat de nodes verdeeld zijn over meerdere locaties en er altijd één uit kan vallen zonder dat de eindgebruiker hier iets van merkt. Ook kan eenvoudig worden opgeschaald door een extra node toe te voegen aan het cluster.

Tevens komt de opstelling tegemoet aan de wensen van de klant om uitbreiding sneller te laten verlopen, door de inzet van een multi-tenancy inrichting. Uitbreiding van de omgeving met een nieuwe IdP, zoals die van DJI in



Figuur 11: Multi-tenant inrichting, kan gerealiseerd worden door een nieuwe virtual host toe te voegen op het bestaande cluster. Dit zorgt voor een kostenreductie doordat er geen nieuwe servers bijkomen, wat ook de implementatiesnelheid van nieuwe IdP's verhoogt en de beheerbaarheid ten goede komt.

8. Realisatiefase

In de realisatiefase is het ontwerp uit het vorige hoofdstuk geïmplementeerd in een testomgeving en is het geheel getest aan de hand van een testplan. Dit Testplan en de uitkomsten hiervan zijn bijgevoegd onder is bijgevoegd onder Bijlage G – Testplan + Testrapportage.

Voor de realisatiefase zijn vooraf de volgende activiteiten vastgesteld:

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

8.1 Realisatie

Voor de realisatie is een aantal infrastructurele zaken benodigd. Deze zijn in een zo vroeg mogelijk stadium aangevraagd in verband met doorlooptijden. Het gaat om de volgende zaken:

IdP-Proxy:
- Een /29 VLAN binnen de DMZ
- 2x RedHat Enterprise Linux server, geplaatst in bovengenoemde VLAN
- Een Rijksweb IP-adres + DNS (sts.tstvenj.rijksweb.nl)
- Een Load balancer IP-adres + pool met daarin beide servers
- NAT-translatie van Rijksweb-IP -> Load balancer IP
- Toegang tot het VLAN op poort 443 (HTTPS) ten behoeve van webserver en vice versa
- Toegang tot het VLAN op poort 22 (SSH) vanaf de beheeromgeving en vice versa

Identity Provider:
- Een /29 VLAN binnen de DMZ
- 2x RedHat Enterprise Linux server, geplaatst in bovengenoemde VLAN
- Een Rijksweb IP-adres + DNS (login.bd.tstvenj.rijksweb.nl en login.cjib.tstvenj.rijksweb.nl)
- Een Load balancer IP-adres + pool met daarin beide servers
- NAT-translatie van Rijksweb-IP -> Load balancer IP
- Toegang tot het VLAN op poort 443 (HTTPS) ten behoeve van de webserver en vice versa
- Toegang tot het VLAN op poort 22 (SSH) vanaf de beheeromgeving en vice versa
- Toegang tot JustitieNet op poort 636 (LDAPS) ten behoeve van authenticatie tegen AD

Service Provider:
Voor de inrichting van een service provider is gebruik gemaakt van de testapplicatie die standaard wordt meegeleverd door SimpleSAMLphp. Deze is als virtual host bijgeplaatst op het Identity Provider-cluster. Dit is een keuze die puur uit kostenoverwegingen is gemaakt en is verder niet van invloed op de werking van één van beide componenten. Op deze manier wordt een extra server uitgespaard.

Voor gebruik in de testomgeving kan worden volstaan met self-signed PKI-certificaten.

De installatie en inrichting van de verschillende componenten is vrijwel identiek en omvat o.a. de volgende stappen:

- Installatie benodigde packages (apache, php, memcached)
- Aanmaken systeemuser
- Indeling file system
- Toekennen rechten aan systeemuser en beheerders
- Configuratie webserver
- Installatie applicatie
- Hardening

File system

Het file system is zo ingedeeld dat eenvoudig een nieuwe tenant kan worden toegevoegd (Zoals DJI in Figuur 8). Door het gebruik van symbolic links kan een tenant eenvoudig opnieuw opgezet worden naast de bestaande, bijvoorbeeld wanneer er een nieuwe versie van de applicatie moet worden uitgerold. Het omzetten van de symbolic link naar de nieuwe locatie is dan genoeg voor een 'update' en een rollback is zo eenvoudig als het weer terugzetten van de symlink naar de oude locatie. Hier hoeft zelfs de webserver-configuratie niet voor aangepast te worden.

Webserver

De webserver is zo ingedeeld dat er per tenant een aparte configuratie-file bestaat met daarin de virtual host declaratie. Alle SSL/TLS-gerelateerde configuratie is in een aparte file (ssl.conf) gestopt zodat deze instellingen maar op één plek bijgehouden hoeven te worden. In het geval van de IdP-Proxy zijn er uiteraard geen tenants, maar is hetzelfde principe toegepast met een symlink.

Hardening

De hardening van de systemen is gericht op zowel hostbeveiliging als netwerkbeveiliging. Hier is invulling aan gegeven middels:

- VLAN-firewall
- Host-firewall
- Webserver / TLS-configuratie
- SELinux

De beide firewalls zijn zo geconfigureerd dat standaard alle verkeer wordt geblokkeerd, met uitzondering van het strikt noodzakelijke verkeer. Voor eindgebruikers betekent dit dat ze de machines alleen kunnen benaderen op poort 443 (HTTPS). Dit verkeer wordt door de webserver verder beperkt, door alleen veilige protocollen en algoritmen (ciphers) worden toegestaan. Voor deze configuratie is gebruik gemaakt van de best practice van Qualsys SSL Labs (zie bronvermelding). Tot slot wordt me SELinux voorkomen dat de webserver bestanden kan uitvoeren buiten bepaalde directories.

8.2 Testen nieuwe opstelling

Voor het testen van de opstelling is een testplan opgesteld. Hierin zijn o.a. een aantal entry- en exit-criteria opgesteld en zijn afspraken opgesteld over de acceptatie van de omgeving. Zie Bijlage G – Testplan + testrapportage.

Binnen SSC-ICT is het gebruikelijk om te testen middels de TMAP-methodiek. Gezien de geringe omvang van het afstudeerproject is TMAP hierbij niet gebruikt. Wel is uitgegaan van een voorbeeld-testplan wat volledig op TMAP gebaseerd is. Alle zaken die niet van toepassing zijn, zijn hierbij weggelaten.

De uitvoer van de tests is belegd bij de applicatiebeheerder, die de resultaten van de tests rapporteert aan de afstudeerder die hierop actie onderneemt om de omgeving aan te passen.

Als bijlage van het testplan is de testrapportage opgenomen. Hierin staan de scenario's die getest zijn door de applicatiebeheerder, welke de uitkomsten van de tests weer aan het project heeft gerapporteerd. De bevindingen die hierbij zijn gedaan zijn vervolgens verholpen, waarna het testtraject nogmaals is doorlopen.

De meest noemenswaardige constatering uit het testtraject was dat niet iedereen gebruik maakt van dezelfde browserversie. Waar de eindgebruikers normaliter gebruik maken van Internet Explorer 8, blijken er ook gevallen te zijn waar gebruik gemaakt wordt van Internet Explorer 11. De consequentie hiervan is dat het testtraject op de verschillende typen werkstations uitgevoerd is.

8.3 Overdracht naar beheer

Voor de overdracht naar de beheerorganisatie is een gesprek ingepland met de applicatiebeheerder. Voor de acceptatie waren vooraf door de beheerorganisatie de volgende acceptatiecriteria opgesteld:

- Testrapportage aanwezig;
- Geen blokkerende bevindingen uit het testtraject;
- Volledige documentatie en installatiehandleidingen aanwezig.

De applicatiebeheerder heeft in een eerder stadium al het Technisch Ontwerp gelezen en heeft zelf de nieuwe omgeving getest. Tijdens het gesprek zijn nog een aantal vragen beantwoord en is documentatie overgedragen, waarna de testomgeving formeel geaccepteerd is.

9. Conclusies en aanbevelingen

Op basis van de testresultaten kan de conclusie worden getrokken dat met relatief weinig inspanning een aantal (voornamelijk technische) wijzigingen kunnen worden doorgevoerd om de dienst te verbeteren. Deze verbeteringen omvatten:

- High availability / schaalbaarheid over de gehele omgeving, door alle componenten redundant, achter een load balancer te plaatsen en te verdelen over meerdere datacenters;
- Betere beveiliging conform de BIR, door het verplaatsen van de Identity Providers naar de DMZ en het hardenen van het platform;
- Logische scheiding tussen interne en externe verkeersstromen, door het koppelen van bedrijfsvoeringsapplicaties aan het interne koppelvlak (IdP-Proxy);
- Lagere beheerinspanning door standaardisatie en het terugdringen van het aantal servers;
- Het terugdringen van de kosten op licenties door het schrappen van één van de gebruikte producten;
- Het verkorten van implementatietijden bij het aansluiten van nieuwe Identity Providers, door deze op een multi-tentant omgeving te plaatsen waardoor niet voor elke nieuwe aansluiting ook nieuwe servers benodigd zijn.

De eerste aanbeveling luidt dan ook om eerst orde op zaken te stellen en deze wijzigingen door te voeren op de bestaande acceptatie- en productieomgeving, voordat verder gegaan wordt met het uitbouwen van de dienst met nieuwe Identity Providers en Service Providers. Hiermee kan op een gedegen manier invulling worden gegeven aan het faciliteren van de authenticatiescenario's 1 tot en met 5 (zie Tabel 1).

Vervolgens kunnen de authenticatiescenario's 6 tot en met 9 worden gerealiseerd door een two-way trust met de rijksbrede federatie. Hiermee worden ambtenaren van andere ministeries in staat gesteld gebruik te maken van de applicaties van Justitie.

Een laatste stap kan dan zijn om authenticatiescenario's 10 en 11 te realiseren door het verder concretiseren van het externe koppelvlak, wat momenteel nog een proof of concept is. Het is echter maar de vraag of dit nog nodig en economisch rendabel is, gezien de ontwikkeling van een extern koppelvlak op rijksbreed niveau. Gebruik van een rijksbreed extern koppelvlak is vele malen goedkoper dan wanneer elk ministerie haar eigen koppelvlak ontwikkelt. Potentieel kan dit Justitie een besparing opleveren van 10/11^{e} deel (De kosten van 1 koppelvlak verdeeld over 11 ministeries)

Huis op orde

Ondanks de talloze mogelijkheden tot doorontwikkeling strekt het de aanbeveling om de dienst eerst in de basis uit te breiden door eerst heel justitie (drieëntwintig onderdelen) aan te sluiten middels een Identity Provider en meer Justitie-applicaties aan te sluiten als Service Provider, zodat de dienst een breder draagvlak krijgt binnen Justitie. Dit rechtvaardigt dan ook beter de kosten van dienst.

Tot slot kan op basis van interviews en eigen ervaring worden geconcludeerd dat documentatie en beheerafspraken niet op orde zijn. De logische aanbeveling die hieruit volgt is dan ook om deze zaken op orde te brengen door de documentatie op orde te brengen, beheerafspraken te maken met alle betrokken partijen en door een vorm van ketenregie in het leven te roepen.

10. Evaluatie

In dit hoofdstuk wordt teruggeblikt op de afstudeertraject. Hoe is het proces verlopen en hoe staat dat tot verhouding met de planning die bij aanvang was opgesteld.

Proces

Voor de afstudeeropdracht is gebruik gemaakt van de watervalmethode. Deze methode is prima geschikt gebleken voor de afstudeeropdracht, dankzij de gefaseerde benadering. Iedere fase gaf een goed en duidelijk beeld van de voortgang van het project. Wel is er een risico in het gebruik van de methode: een ernstige bevinding tijdens het testen zou potentieel kunnen leiden tot een aanpassing van het Technisch Ontwerp, terwijl de watervalmethode niet bedoeld is voor het terugspringen naar een vorige fase.

Wat planning betreft zijn er een aantal uitdagingen geweest gedurende het project. Zo is begonnen met een kleine vertraging doordat het opstarten van het project wat moeizaam verliep en is de definitiefase ook met zo'n twee weken uitgelopen. Doordat de implementatie zeer voorspoedig verlopen is, is de oplevering van het geheel op tijd geweest.

Oriëntatiefase

Tijdens de oriëntatiefase lag de nadruk vooral op het bekend raken met het begrip "federatieve authenticatie" en de daar bijbehorende technieken. In dit stadium werd al gelijk duidelijk dat het een concept, wat op zichzelf niet heel ingewikkeld is, gebruik maakt van een groot aantal technieken en dat het een behoorlijk complex geheel is. Begrippen als PKI en TLS waren mij vanuit opleiding en werkervaring al wel bekend, maar met name het SAML-protocol bleek een behoorlijk complex verhaal waar ik veel van geleerd heb.

Het opstellen van het Plan van Aanpak is verder niet al te moeilijk bevonden. Dit document kon voor een belangrijk deel al worden gevuld met gegevens uit het eerder opgestelde afstudeerplan.

Definitiefase

In de definitiefase is er verder verdiept in de situatie bij Justitie en is deze verder geanalyseerd. Dit is als een behoorlijk lastige klus ervaren, doordat er niet veel documentatie voor handen was. Uiteindelijk is dit probleem omzeild door meer 'hands-on' de configuraties te bestuderen.

De Definitiestudie is uiteindelijk een behoorlijk groot document geworden. Doordat hier van begin af aan verschillende relevante personen (beheerder, opdrachtgever) bij betrokken zijn en het document aan een peer-review onderworpen is, is het een degelijk stuk is geworden waarin alle aspecten aan bod komen die relevant zijn geweest voor dit project.

Ontwerpfase

Tijdens de ontwerpfase is onderzocht welke mogelijkheden er momenteel zijn om te voldoen aan de opgestelde wensen en eisen. Al snel kon de conclusie getrokken worden dat de behoeften vooral op een snellere en efficiëntere inzet van bestaande componenten betrekking hadden.

Binnen de omgeving wordt gebruik gemaakt van verschillende producten, terwijl één van de producten ook prima ingezet kan worden als Identity Provider én als IdP-Proxy. Door ook gelijke componenten samen te voegen is een aanzienlijke besparing op de beheerlast en kosten van de omgeving gerealiseerd.

Het Technisch Ontwerp wat voorkomt uit de ontwerpfase is dankzij de ruime voorbereiding in de definitiefase een degelijk document geworden, wat gedragen wordt door relevante stakeholder zoals de beheerder en de domeinarchitect.

Realisatiefase

In de ontwerpfase is het technisch ontwerp in de praktijk gebracht en onderworpen aan een aantal relevante tests. De implementatie is vrijwel vlekkeloos verlopen, wat de kwaliteit van het Technisch Ontwerp verder onderschrijft.

Bronvermelding

Standaarden:
Koppelvlakstandaard ebMS voor Digikoppeling, versie 3.0
[https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/documentatie_23-09/Digikoppeling_3.0_Koppelvlakstandaard_ebMS_v3.0.pdf]

Idensys afsprakenstelsel, versie 1.0
[http://www.idensys.nl/fileadmin/eid/documenten/4._Interface_specifications_v1.0.pdf]

Voorschrift Informatiebeveiliging Rijksdienst
[https://nl.wikipedia.org/wiki/Voorschrift_Informatiebeveiliging_Rijksdienst]

Best Practices:
Géant - Securing Linux Servers – Best Practice Document
[http://services.geant.net/cbp/Knowledge_Base/Security/Documents/CBP-10_securing-linux-servers.pdf]

Géant - Securing Service Access With Digital Certificates – Best Practice Document
[http://services.geant.net/cbp/Knowledge_Base/Security/Documents/cbp-20_securing-server-access-with-digital-certificates.pdf]

Géant - Information Security Policy – Best Practice Document
[http://services.geant.net/cbp/Knowledge_Base/Security/Documents/gn3-na3-t4-ufs126.pdf]

Qualsys SSL Labs – SSL/TLS Deployment Best Practices
[https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf]

Overige:
SSLlabs Server Test
[https://www.ssllabs.com/ssltest]

Beleidsdocumenten:
Aansluitvoorwaarden Rijks-SSOn, versie 1.3, departementaal vertrouwelijk
Doelarchitectuur domein Toegang 2015, versie 0.8, departementaal vertrouwelijk

BIR 2012, versie 1.0
[http://www.earonline.nl/images/ear/6/6f/BIR_TNK_1_0_definitief.pdf]

Documentatie:
Functioneel ontwerp Federatieve Service VenJ, versie v1.1, departementaal vertrouwelijk
Technisch ontwerp Federatieve Service VenJ, d.d. 18-10-2012 (geen versienummer), departementaal vertrouwelijk
Business Impact Analyse – Doorontwikkeling SSOn Rijk, v0.2.1 concept, departementaal vertrouwelijk

Lijst van gebruikte afkortingen

ADC	Application Delivery Controller
BD	Bestuursdepartement
BIR	Baseline Informatiebeveiliging Rijksdienst
CJIB	Centraal Justitieel Incassobureau
DA	Doelarchitectuur
DAP	Dossier Afspraken en Procedures
DEP-V	Departementaal Vertrouwelijk
DI&I	Directie Informatisering en Inkoop
DNO	Dienst-Niveau Overeenkomst
DJI	Dienst Justitiële Inrichtingen
DWR	Digitale Werkplek Rijksdienst
HRD	Home-Realm Discovery
IdP	Identity Provider
JustID	Justitiële Informatiedienst
MFA	Multi-Factor Authentication
NBV	Nationaal Bureau Verbindingsbeveiliging
PDC	Producten- en Dienstencatalogus
PIA	Privacy Impact Assessment
RIdM	Rijks Identity Management
RIN	Rijks Identificerend Nummer
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SOC	Security Operations Center
SP	Service Provider
SSC-ICT	Shared-Service Center ICT
SSOn	Single Sign-on
TBB	Te Beschermen Belangen
VIR-BI	Voorschrift Informatiebeveiliging – Bijzondere Informatie
WAYF	Where Are You From
WBP	Wet Bescherming Persoonsgegevens
ZBO	Zelfstandig Bestuursorgaan