# Scriptie Single Sign-on

Afstudeerder: Stefan Breukelman

Studentnummer: 1575398

Bedrijfsbegeleider: Gerton Krol

Docentbegeleider: Alphons Moes

# VOORWOORD

Deze scriptie is geschreven in het kader van mijn afstudeeropdracht voor de opleiding System and Network Engineering Duaal aan de Hogeschool van Utrecht.

De afstudeeropdracht is uitgevoerd bij de Bestuursdienst Ommen-Hardenberg in de periode van april tot en met oktober 2014.

Graag wil ik een aantal mensen bedanken voor hun medewerking en ondersteuning tijdens het uitvoeren van mijn afstudeeropdracht. Bij deze wil ik Gerton Krol, die tijdens deze periode mijn bedrijfsbegeleider is geweest, bedanken voor het meedenken, formuleren en aanleveren van de afstudeeropdracht.
De keuze voor het onderwerp Single Sign-on heeft er aan bijgedragen dat o.a. mijn kennis op het gebied van authenticatie en autorisatie naar een hoger niveau is getild.

Tevens wil ik mijn collega's van het team ICT bedanken voor de ondersteuning en behulpzaamheid tijdens het uitvoeren van de afstudeeropdracht.

Daarnaast wil ik mijn afstudeerbegeleider Alphons Moens bedanken voor zijn begeleiding tijdens het afstuderen. De gesprekken die in het begin gevoerd zijn, en de feedback die ik ontvangen heb tijdens deze periode, heb ik als zeer bruikbaar ervaren.

13 oktober 2014

Stefan Breukelman

# MANAGEMENT SAMENVATTING

In deze scriptie is de uitwerking van het onderzoek naar een Single Sign-on oplossing voor de Bestuursdienst Ommen-Hardenberg terug te vinden.

Medewerkers moeten tegenwoordig steeds vaker gebruik maken van applicaties om diverse werkzaamheden uit te kunnen voeren. Hiervoor moet de gebruiker enkele handelingen uitvoeren om toegang tot deze applicatie te krijgen.
In het bijzonder het invoeren en onthouden van meerdere inlognamen en wachtwoorden. Dit wordt door de gebruiker als storend ervaren.
Om gebruik te kunnen maken van applicaties binnen de Bestuursdienst Ommen-Hardenberg is dit echter wel noodzakelijk, er moet immers sprake zijn van een goede informatiebeveiliging.

Maar wanneer een gebruiker deze gegevens noteert op papier of in een tekstdocument dan heeft dit invloed op de veiligheid van het systeem. Een onbevoegde kan met deze inloggegevens informatie verkrijgen die niet voor hem of haar is bedoeld. Tevens vergeten gebruikers de wachtwoorden omdat het er soms simpelweg te veel zijn om te onthouden.
Er moet dan vanuit ICT aan deze gebruikers support verleend worden om te zorgen dat zij weer in kunnen loggen. Het invoeren van Single Sign-on in de organisatie kan bijdragen aan het verhelpen van dit probleem.
Gebruikers loggen éénmalig aan op het systeem en kunnen vervolgens meerdere applicaties starten zonder telkens opnieuw aan te loggen.

Tijdens deze afstudeeropdracht heb ik informatie over diverse technieken waar Single Sign-on gebruik van kan maken, onderzocht. Door gebruik te maken van verschillende onderzoeksmethodes ben ik tot een advies voor de organisatie gekomen.

Om ervoor te zorgen dat zoveel mogelijk applicaties van Single Sign-on gebruik kunnen maken, kan de organisatie het beste kiezen voor een Enterprise Single Sign-on oplossing omdat deze de mogelijkheid heeft om meerdere applicaties van diverse platformen te voorzien van Single Sign-on in samenwerking met een sterke authenticatie.

# INHOUDSOPGAVE:

# INLEIDING

De Bestuursdienst Ommen-Hardenberg is voortgekomen uit een samenwerkingsverband tussen de gemeente Hardenberg en de gemeente Ommen. Er wordt nog wel gebruik gemaakt van beide gemeentehuizen en er zijn een aantal buitenlocaties waaronder enkele zwembaden, een lokaal opleidingscentrum en het theater.

Bij de Bestuursdienst Ommen-Hardenberg zijn 550 werkplekken aanwezig, waar 650 gebruikers zich op kunnen aanmelden. De werkplek bestaat hoofdzakelijk uit een virtuele machine die met behulp van een Virtuele Desktop Image (VDI) gekoppeld wordt aan een thin-client en vervolgens aan de gebruikers wordt aangeboden.

Daarnaast zijn er enkele werkplekken voorzien van een vaste PC in verband met diverse randapparatuur. Op deze pc's is een VMWare view client geïnstalleerd die het ook mogelijk maakt om een virtuele desktop te kunnen starten.

Deze afstudeeropdracht bestaat uit een onderzoek naar de mogelijkheden van een Single Sign-on oplossing voor de Bestuursdienst Ommen-Hardenberg.

# 1 CONTEXT

Binnen de Bestuursdienst Ommen-Hardenberg is er behoefte aan de implementatie van een Single Sign-On oplossing. Single Sign-on is een gebruikersauthenticatieproces welke ervoor zorgt dat de gebruiker “slecht” één keer zijn inloggegevens hoeft in te voeren om vervolgens toegang te krijgen tot meerdere systemen en applicaties. Het is dan voor de gebruiker niet meer nodig om verschillende inloggegevens te onthouden. De medewerkers maken gebruik van meerdere inloggegevens om diverse systemen te kunnen starten. Om de medewerkers te ontlasten is mij gevraagd om een project te starten waarin de mogelijkheden worden onderzocht om over te gaan naar een systeem dat kan voorzien in het éénmalig inloggen voor de gebruiker.

Met deze afstudeeropdracht is het de bedoeling dat er gekeken wordt naar de mogelijkheid om de omgeving uit te breiden met een Single Sign-on oplossing, hier moet uiteindelijk een advies uitkomen voor de Bestuursdienst Ommen-Hardenberg.

## 1.1 BETROKKENEN BIJ HET PROJECT

De projectorganisatie bestaat uit de volgende deelnemers:

| | | |
|---|---|---|
| Gerton Krol | Vakspecialist A ICT | Bedrijfsbegeleider |
| Alphons Moens | Docent Hogeschool Utrecht | Docentbegeleider |
| Stefan Breukelman | Netwerk/Systeembeheerder | Afstudeerder |

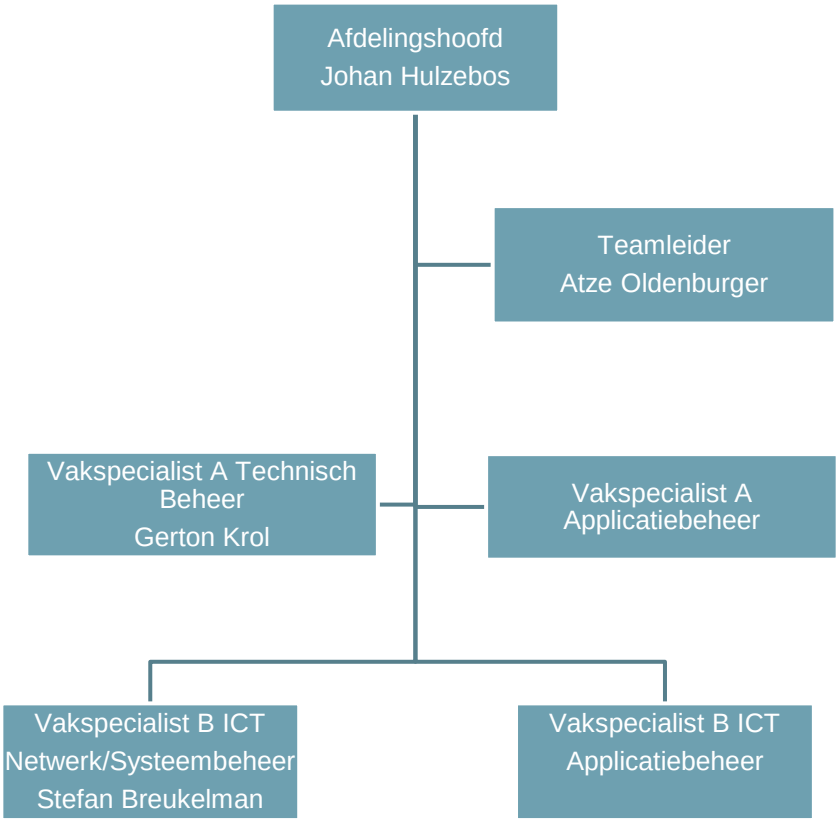
## 1.2 BEDRIJFSSITUATIE

De ICT afdeling bestaat uit 18 medewerkers die de organisatie adviseert bij ICT vraagstukken en dienstverlenend is in geval van calamiteiten. Daarnaast wordt er constant gekeken naar vernieuwingen en verbeteringen in de huidige ICT-omgeving.

De ICT afdeling bestaat uit de volgende functiegroepen:

- Vakspecialisten A
- Vakspecialisten B Applicatiebeheer
- Vakspecialisten B Netwerk/Systeembeheer

Organigram bedrijfspositie:




## 1.3 POSITIE STUDENT

In 2006 ben ik als netwerk/systeembeheerder gestart bij de gemeente Hardenberg, en in 2012 vervolgens overgegaan in de nieuwe organisatie de Bestuursdienst Ommen-Hardenberg. Mijn dagelijkse werkzaamheden bestaan uit het beheren van diverse servers, virtuele desktops, databases van meerdere platforms en diverse netwerkapparatuur. Daarnaast zorg ik voor de controle op back-ups en biedt ondersteuning aan gebruikers.

Deze werkzaamheden voer ik uit met meerdere collega's van het team netwerk/systeembeheer, in totaal zijn we binnen dit team met 6 medewerkers. Er is een onderverdeling qua expertise en vakgebieden die voornamelijk door de jaren heen zo gegroeid is.

Het bijhouden van kennis wordt als een belangrijk aandachtpunt gezien binnen ons team, er zijn daarom ook voldoende mogelijkheden in de vorm van cursussen en opleidingen om ervoor te zorgen dat het kennisniveau op peil blijft.

# 2 DOELSTELLING EN PROBLEEMSTELLING

## 2.1 DOELSTELLING

Het doel van mijn onderzoek is om te komen tot een goede keuze voor een Single Sign-on functionaliteit die binnen de organisatie geïmplementeerd gaat worden.
De aangeboden oplossing moet de mogelijkheid hebben om de belangrijkste applicaties in de virtuele omgeving van de Bestuursdienst Ommen-Hardenberg te benaderen via een enkele inlogprocedure.

Na het inloggen, moet het mogelijk zijn om de belangrijkste applicaties welke binnen de virtuele desktop omgeving worden aangeboden zeer snel via een Single Sign-on procedure te openen.
Het wachtwoord beheer moet gemakkelijk en overzichtelijk toegepast kunnen worden door meerdere collega's van technisch beheer.

## 2.2 PROBLEEMSTELLING

Binnen onze organisatie zijn er meerdere applicaties waarvoor de gebruiker een inlognaam en een wachtwoord nodig heeft om in te kunnen loggen.

Hier wordt vanuit dagelijks beheer veel tijd ingestoken. Gebruikers vergeten hun inloggegevens of voeren meerdere keren onjuiste informatie in. Om ervoor te zorgen dat deze problemen structureel opgelost worden, is er gevraagd om de mogelijkheden van een Single Sign-on oplossing te onderzoeken.

De Bestuursdienst Ommen-Hardenberg heeft 650 actieve gebruikersaccounts binnen de Active Directory, deze is ook leidend binnen de organisatie op gebied van naamgeving. Wanneer er op andere plekken een account wordt gecreëerd dan moet de naamgeving uit De Active Directory gehanteerd worden.

Er zijn dus applicaties die een eigen database met inloggegevens hanteren, voor de gebruiker is het daarom ook noodzakelijk deze accounts mee te nemen. Voor het onderzoek heb ik de Prio 1 applicaties (belangrijkste applicaties in de organisatie) als uitgangspunt genomen.

## 2.3 ONDERZOEKSVRAGEN

Om de vragen die ontstaan tijdens de probleemomschrijving te kunnen beantwoorden heb ik onderstaande onderzoeksvraag opgesteld:

Op welke wijze kan het selecteren en implementeren van een Single Sign-on oplossing plaatsvinden, waarbij er ook rekening wordt gehouden met het bestaande ICT-beleid en de aanwezige ICT-architectuur?

### 2.3.1 DEELVRAGEN

De onderstaande deelvragen moeten bijdragen aan het beantwoorden van de onderzoeksvraag, De vragen worden in verschillende hoofdstukken van de scriptie beantwoord.

1. Aan welke eisen moet het nieuwe systeem voldoen?
2. Wat is de haalbaarheid van een Single Sign-on oplossing?
3. Hoe kan de Single Sign-on oplossing in de bestaande ICT-infrastructuur geïmplementeerd worden?
4. Welke oplossing past het beste bij de organisatie in samenwerking met het huidige ICT-beleid?
5. Wat zijn de risico's die verbonden zijn aan de implementatie van een Single Sign-on oplossing?
6. Op welke wijze kunnen de risico's beheersbaar blijven?
7. Welke rol speelt informatiebeveiliging in de huidige omgeving?
8. Welke aanpassing moet er plaatsvinden op gebied van security?
9. Waarmee kan een Single Sign-on oplossing zich in de organisatie onderscheiden?
10. Wat zijn de voor- en nadelen voor de gebruikers?
11. Wat is de impact op de organisatie?

## 2.4 GEKOZEN AANPAK

Onderstaande taken worden opgeleverd bij voltooiing van de afstudeeropdracht.

- Onderzoek naar verschillende Single Sign-on mogelijkheden
- Inventarisatie van bestaande systemen en belangrijkste applicaties
- Beschrijving bestaande Infrastructuur
- Inventarisatie van bestaande logins
- Uitkomsten referentiebezoeken
- Uitkomst Pakketselectie
- Oplossingen uitwerken
- Advies uitbrengen aan organisatie

## 2.5 GEKOZEN METHODES

Het project wordt uitgevoerd binnen de huidige situatie. Een onderzoek is noodzakelijk om alle onderdelen goed in kaart te brengen. Het toepassen van de onderstaande onderzoeksmogelijkheden zal hieraan bijdragen.

### 2.5.1 MOSCOW

Door middel van de MoSCoW [3] methode zal er een analyse van eisen uitgevoerd worden. Hier worden de volgende vragen in gesteld:

1. **Must have this?** *(Noodzakelijk, Is nodig om een werkend product op te kunnen leveren)*
2. **Should have this if at all possible?** *(Heeft een hoge prioriteit, maar niet noodzakelijk)*
3. **Could have this if it does not affect anything else?** (*Lage prioriteit, niet noodzakelijk)*
4. **Won't have this but would like to have this in the future?** *(Geen prioriteit, maar wellicht voor in de toekomst)*

### 2.5.2 DESKRESEARCH

Om informatie over het onderzoek te verzamelen is het toepassen van deskresearch een goede methode.
De informatie kan bestaan uit artikelen, white papers, algemene literatuur en verslagen, dit zorgt ervoor dat er niet voor elk onderwerp een eigen onderzoek nodig is. Het kan tijdbesparend zijn voor het uitvoeren van het onderzoek.

### 2.5.3 FIELDRESEARCH

Het toepassen van fieldresearch bestaat uit het verzamelen van Informatie die verkregen wordt door het uitvoeren van eigen onderzoek.

## 2.6 OPBOUW SCRIPTIE

De scriptie bevat meerdere hoofdstukken en is op de volgende manier opgezet: In het 1$^{e}$ hoofdstuk wordt de context van de afstudeeropdracht en de positie binnen het bedrijf besproken. Hoofdstuk 2 behandelt de doelstelling en probleemstelling en tevens de gekozen aanpak van het onderzoek. Hoofdstuk 3 bevat informatie die tijdens het onderzoek is verzameld. In hoofdstuk 4 worden het functioneel- en technische ontwerp beschreven. Hoofdstuk 5 bevat informatie betreffende het Proof of Concept en in hoofdstuk 6 heb ik het advies geschreven voor de Bestuursdienst Ommen-Hardenberg. De evaluatie van het project is beschreven in hoofdstuk7 en hoofdstuk 8 bevat de bijlages.

# 3 ONDERZOEK

## 3.1 SSO OMSCHRIJVING:

In een bestaande ICT-omgeving zijn vaak meerdere applicaties beschikbaar waarbij de gebruiker telkens verschillende inloggegevens moet hanteren om toegang te krijgen tot systemen en applicaties.

***Wat wordt bedoeld met inloggen?***

Het inlogproces bestaat uit 3 stappen die uitgevoerd worden voordat daadwerkelijk van een systeem/applicatie gebruik gemaakt kan worden.
De 1e stap is de identificatie van de gebruiker, de identiteit wordt gebruikt voor het invoeren van inloggegevens op een inlogscherm. Een identiteit is meestal een combinatie van een unieke gebruikersnaam en een wachtwoord. Deze gegevens moeten vervolgens gecontroleerd worden.
En dat gebeurt in de 2$^{e}$ stap van dit proces, de authenticatie. Bij deze stap wordt er gecontroleerd of een gebruiker daadwerkelijk is wie hij beweert te zijn. In het systeem waar de identiteitsgegevens bewaard worden, volgt een controle op de gegevens die zijn ingevoerd op het inlogscherm.
Als de controle succesvol is dan kan de gebruiker inloggen op het systeem, echter heeft de gebruiker nog geen rechten of rollen om bestanden, mappen of applicaties te kunnen starten. De 3$^{e}$ en laatste stap is daarom de autorisatie, wat mag een gebruiker wel en wat mag een gebruiker niet benaderen op het moment dat ze succesvol is ingelogd. Autorisatie wordt meestal op gebruikersniveau toegepast, echter kunnen de rechten of rollen ook op afdelingsniveau of locatie worden uitgedeeld.

Een Single Sign-On oplossing kan er voor zorgen dat het authentiseren van een gebruiker op een andere manier wordt uitgevoerd.

De beveiliging van gegevens is steeds belangrijker geworden en daarom wordt er steeds vaker om een combinatie van gebruikersnaam en wachtwoord gevraagd. Eén Authenticatiebron zou in deze gevallen een goede oplossing kunnen zijn, bij een bestaande Microsoft omgeving wordt deze vorm al toegepast. Wanneer er van een Active Directory account gebruik gemaakt wordt dan kan de gebruiker ook aanloggen op Microsoft systemen zoals Microsoft Exchange, Microsoft SharePoint en Windows File Server. Dit alles op basis van het Active Directory account, dit kan tevens uitgebreid worden naar andere systemen die technieken kunnen ondersteunen zodat ze gekoppeld kunnen worden aan een Active Directory. Enkele voorbeelden hiervan zijn: Kerberos, LDAP, SAML

***Wat is nu precies Single Sign-on?***

Niet alle applicaties kunnen van deze technieken gebruik maken. Om de gebruikers en ook de beheerders van de systemen te ontlasten is er een oplossing ontwikkeld die ervoor kan zorgen dat het onthouden van meerdere inloggegevens verleden tijd kan zijn.

Single Sign-on [5] is een authenticatietechniek die ervoor zorgt dat een gebruiker die wil inloggen, eenmalig zijn loginnaam en wachtwoord in hoeft te geven om toegang tot het systeem en meerdere applicaties te krijgen.

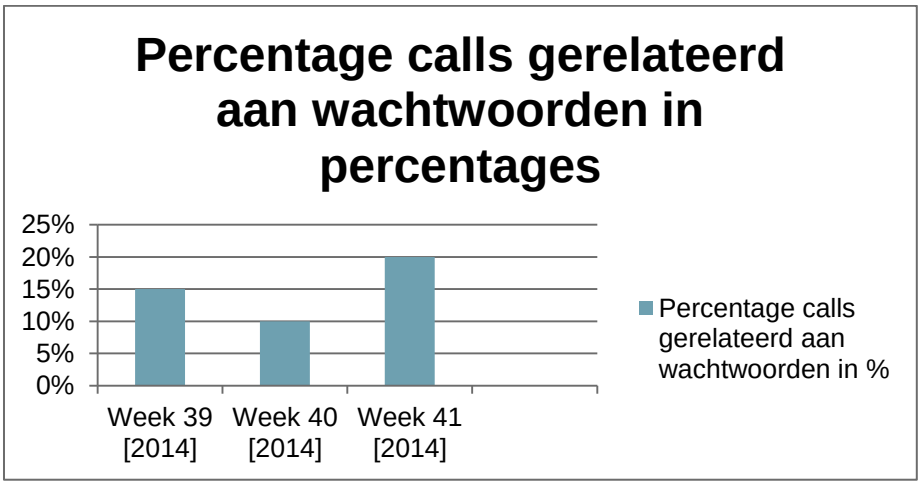
***Waarmee kan een Single Sign-on oplossing zich in de organisatie onderscheiden?***

Single Sign-on levert meerdere voordelen aan de gebruiker:
De gebruiker heeft slecht één loginnaam en wachtwoord nodig om van meerdere systemen gebruik te maken, dit kan ervoor zorgen dat er een betere informatiebeveiliging plaatsvindt. Wanneer een gebruiker meerdere inloggegevens moet hanteren dan gaat dit vaak ten koste van de beveiliging [7].
Het kiezen van korte en zwakke wachtwoorden omdat de gebruiker teveel moet onthouden, of het noteren van inloggegevens in een tekstdocument of op papier om ervoor te zorgen dat ze deze gegevens dan niet worden vergeten, is een bekend fenomeen binnen veel organisaties.

Het invoeren van een Single-Sign-on oplossing zodat het inloggen wordt vereenvoudigd, kan ervoor zorgen dat deze problemen verdwijnen. De gebruiker kan nu gedwongen worden om één sterk wachtwoord te hanteren welke voldoet aan bepaalde veiligheidseisen. Het risico dat de gebruikers deze gegevens nog op meerdere plekken zal gaan bewaren neemt daarmee flink af.

Het beheren van useraccounts en wachtwoorden wordt eenvoudiger voor beheerders, aangezien het aantal gebruikersnamen en wachtwoorden terug zal lopen. Wanneer een gebruiker 5 applicaties tot zijn beschikking heeft die allemaal gestart moeten worden met het invoeren van inloggegevens, dan kunnen dit al 5 unieke authenticatie gegevens zijn.

De Bestuursdienst Ommen-Hardenberg heeft 650 gebruikersaccounts en het aantal wachtwoorden voor 5 applicaties per gebruiker komt neer op 3250 unieke wachtwoorden die beheerd moeten worden. De helpdesk van de organisatie zal minder vaak een wachtwoord opnieuw in hoeven te stellen. Een steekproefsgewijze inventarisatie bij het Intern Service Punt ( ISP) van de Bestuursdienst Ommen-Hardenberg betreffende het aantal meldingen over een vergeten wachtwoord leverde de volgende gegevens op:



Het aantal telefoontjes/meldingen op gebeid van authenticatie kan wekelijks oplopen van 15% tot 20% van de inkomende meldingen. Na de vakantie periode kan dit aantal volgens het ISP oplopen tot 30% van alle binnenkomende incidenten.
Het invoeren van Single Sign-on kan daarom ook bijdragen aan het reduceren van tijd en de kosten voor support op wachtwoordbeheer.

### *Wat zijn de voor- en nadelen voor de gebruikers?*

De snelheid waarmee de gebruiker een applicatie start, wordt verhoogd door minder inlogschermen
Omdat er niet meer voor elke applicatie apart een gebruikersnaam en wachtwoord ingevuld hoeft te worden. Dit zorgt ervoor dat de gebruiker ook minder tijd kwijt is met het opstarten van diverse systemen en applicaties. De gebruiker heeft immers ook minder gegevens nodig om te onthouden. Het nadeel voor een gebruiker kan zijn dat deze niet meer op de hoogte is van de wachtwoorden die gebruikt worden voor het starten van diverse applicaties.

### *Wat zijn de risico's die verbonden zijn aan de implementatie van een Single Sign-on oplossing?*

Het grootste voordeel van Single Sign-on is tevens ook het grootste nadeel van deze oplossing. Wanneer de gebruiker slecht één gebruikersnaam en wachtwoord heeft, dan kan dit ervoor zorgen dat er een kwetsbaarheid in het systeem ontstaat [13]. Immers als deze gegevens bekend worden bij een onbevoegde dan krijgt deze directe toegang tot alle systemen en applicaties waarvoor de gebruiker geauthentiseerd is.
Het toepassen van versleuteling op de inloggegevens die over het netwerk gaan is daarom ook noodzakelijk.

Er zal een beleid toegepast moeten worden die de gebruikers verplicht om van een sterk en degelijk wachtwoord gebruik te maken. Door gebruik te maken van een twee-factor authenticatie kan er een eenvoudigere toegang tot systemen en applicaties plaats vinden. De gebruikersnamen en bestaande wachtwoorden worden dan vervangen door een toegangspas/token of biometriescanner [7].

Wanneer de gebruiker met een toegangspas moet inloggen dan wordt dit iets wat de gebruiker in zijn bezit heeft. Als daar vervolgens nog een wachtwoord aan wordt gekoppeld in de vorm van een pincode, dan wordt dat iets wat de gebruiker weet. Dit zorgt voor een verbetering op het gebied van authenticatie. Het is immers noodzakelijk om zowel de pas als de pincode te weten om in te kunnen loggen.

Bij het implementeren van Single Sign-on zullen de inloggegevens van de gebruikers centraal opgeslagen worden. Dit is voor de beheerders van de diverse systemen ideaal omdat zij hier alle gegevens op één plek kunnen wijzigen.
Echter deze centrale opslag is ook een Single Point of Attack. Het kan een onbevoegde directe toegang kan geven tot alle inloggegevens die daarin opgeslagen zijn. Deze kunnen aangepast of toegevoegd worden en daarmee een groot beveiligingsrisico veroorzaken. Het is daarom ook strikt noodzakelijk deze centrale opslag goed te beveiligen en de toegang te beperken tot enkele beheerders.

Tevens dient de opslag van deze gegevens afgesloten te zijn van de buitenwereld en mag deze alleen intern te benaderen zijn.

Echter kan Single Sign-on ook geclassificeerd worden als een Single Point of Failure. Wanneer er een storing plaatsvindt op de server waar de centrale opslag wordt beheerd/opgeslagen, dan is het voor de gebruikers niet meer mogelijk om in te loggen. Er zal daarom voor de beheerders een alternatieve inlogmogelijkheid aanwezig moet zijn die in geval van calamiteiten gebruikt kan worden.
Het spreekt voor zich dat het systeem dat verantwoordelijk is voor de centrale opslag/authenticatie voorzien wordt van een dagelijkse back-up en een schaduwkopie naar een uitwijkomgeving. De beschikbaarheid van deze server is een belangrijk aspect, en zal daarom op het hoogste niveau moeten liggen. Een redundante uitvoering van deze server is daarom ook een vereiste.

Tijdens de implementatie van Single Sign-on kunnen er applicaties ontdekt worden die geen gebruik kunnen maken van deze techniek. Het zou voor deze applicaties of systemen kunnen betekenen dat er doorgegaan moet worden met inloggen op traditionele wijze.

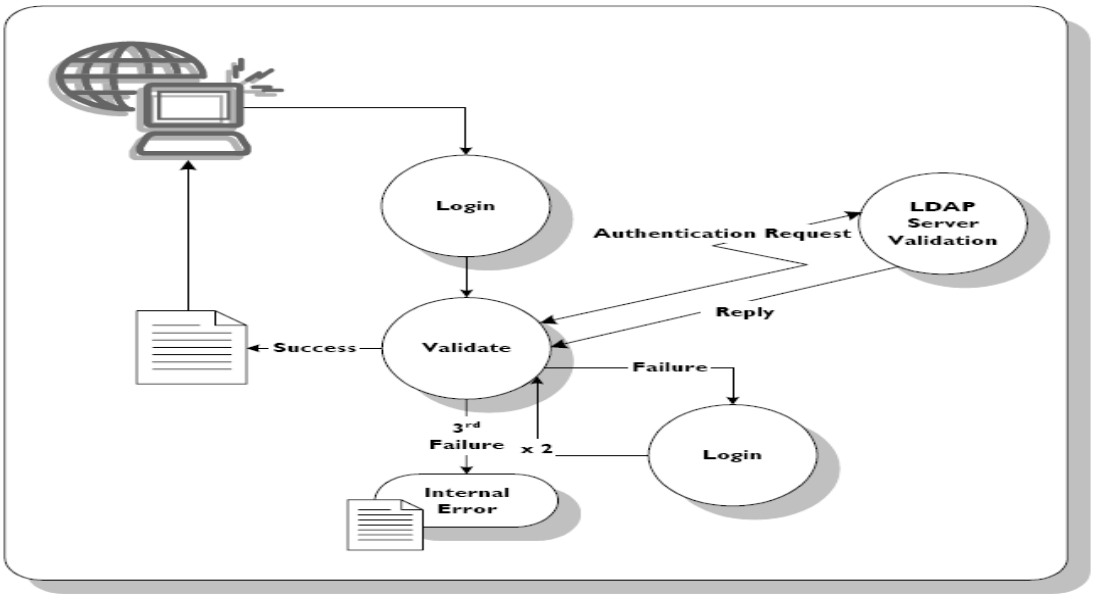
## 3.2 SSO TECHNOLOGIEËN

***Welke technologieën kunnen er bij een Single Sign-on oplossing gebruikt worden?***

Om een Single Sign-on oplossing technisch beter te kunnen begrijpen heb ik een aantal technologieën onderzocht waar een Single Sign-on oplossing gebruik van kan maken. Door het uitvoeren van eigen onderzoek en het lezen van white papers en artikelen heb ik de volgende technieken kunnen beschrijven: LDAP, Kerberos, SAML en E-SSO.

### 3.2.1 LDAP

Lightweight Directory Acces Protocol (LDAP) is een netwerkprotocol waarmee gebruikersgegevens uit directory services (Active Directory) uitgelezen kunnen worden [12].
Deze gegevens kunnen benaderd worden door middel van het TCP/IP netwerkprotocol. De informatie uit directory services wordt opgeslagen in een hiërarchische database, naar attributen die gegroepeerd zijn. De opbouw van deze database zou vergeleken kunnen worden met een telefoonboek, de gegevens worden opgeslagen per directory.
Bijvoorbeeld telefoonnummers en adressen van medewerkers uit een bedrijf. De directorynaam is dan gelijk aan de naam van de organisatie. Alle medewerkers zijn als objecten onder deze directory terug te vinden. Persoonsgegevens zoals e-mail adressen en telefoonnummers worden als attributen opgeslagen.



Figuur 1: LDAP proces
Bron: [16]

***Wat zijn de eigenschappen van LDAP?***

De gebruikers kunnen zich authentiseren met verkregen inloggegevens op de Active Directory en de LDAP [8] koppeling zorgt er vervolgens voor dat er in meerdere applicaties tegelijk ingelogd kan worden. Als LDAP op meerdere systemen/applicaties wordt geconfigureerd dan levert dit een voordeel op voor de gebruiker op het gebied van inlogtijden en een afname in het aantal wachtwoorden. Het is dan wel noodzakelijk dat de applicatie deze vorm van authenticatie ondersteunt.

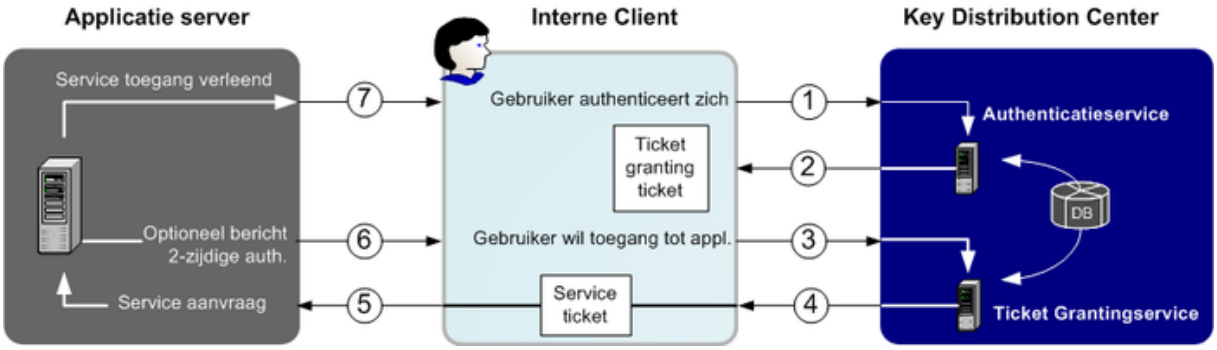
### 3.2.2 KERBEROS

Kerberos [14] is een service die gebruikers kan voorzien in netwerkauthenticatie voor systemen en applicaties. Het is ontwikkeld door Massachusetts Institute of Technology (MIT) om het Project Athena ( IT-omgeving voor het gebruik op de campus) dat destijds in ontwikkeling was te beveiligen.
De Kerberos authenticatie wordt uitgevoerd in een aantal stappen. Daarbij zijn er 3 belangrijke componenten: De client (gebruikers), service (Systeem of Applicatie) en Key Distribution Center [15] (KDC). De naamgeving is daarom ook afgeleid van een driekoppig Grieks wezen. Kerberos kan gekoppeld worden aan de Active Directory, om inloggegevens te verifiëren.

De Kerberos [6] functionaliteit maakt gebruik van een ticketsysteem om een beveiligde toegang te regelen:

De gebruiker die toegang tot een service wil krijgen, logt in met zijn gebruikersnaam en wachtwoord. Het KDC controleert vervolgens deze gegevens eerst bij het Active Directory en als deze informatie juist is dan ontvangt een de client een Ticket Granting Ticket (TGT) van de Key Distribution Center.
Dit Ticket Granting Ticket wordt door de client gebruikt om toegang aan te vragen voor bepaalde services aan de Key Distribution Center.

Het Key Distribution Center geeft bij goedkeuring een Session ticket af, waarmee de client de services die het wil benaderen kan uitvoeren.




Figuur 2: Kerberos authenticatieproces
Bron: [13]

***Wat zijn de eigenschappen van Kerberos?***

Door het gebruik van Kerberos worden er geen wachtwoorden over het netwerk verstuurd en het biedt een oplossing voor centrale opslag van inloggegevens (Active Directory). Wanneer Kerberos op meerdere systemen wordt geïmplementeerd dan hoeft een gebruiker minder vaak te authentiseren wat een voordeel oplevert qua inlogtijd en beveiliging (gebruiker hoeft minder wachtwoorden te onthouden). Kerberos is een authenticatiemethode, echter heeft het geen autorisatiemogelijkheden. Dat betekent dat er met Kerberos niet ingesteld kan worden wat een gebruiker wel of juist niet mag uitvoeren op het moment dat het inloggen voltooid is. Voor het toepassen van Kerberos zal dus een combinatie toegepast moeten worden met een techniek die dit wel uit kan voeren. In dat geval kan er het beste een combinatie gemaakt worden met LDAP, deze heeft immers wel de mogelijkheid om autorisatiefuncties af te handelen.

### 3.2.3 SAML

Security Assertion Markup Language (SAML) is een techniek die op het gebruik van XML is gebaseerd. Deze techniek is ontworpen om organisaties een Single Sign-on oplossing te bieden bij het gebruik van internet applicaties en voor het gebruik tussen meerdere domeinen. Een gebruiker kan met behulp van zijn webbrowser toegang krijgen tot diverse applicaties van verschillende partijen, door eenmalig in te loggen [12].

***Wat zijn de eigenschappen van SAML?***

SAML is een product van OASIS (Organization for the Advancement of Structured Information Standards), een bedrijf dat zich heeft gespecialiseerd op het gebied van standaarden. Op dit moment is SAML 2.0 de laatste versie van deze standaard.

SAML [11] maakt gebruik van enkele rollen:

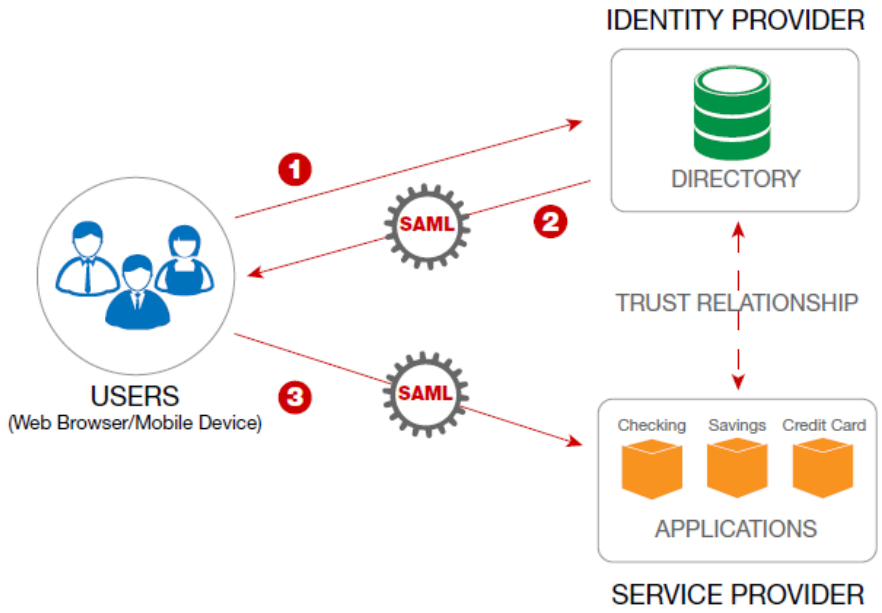
- De User ( dit is meestal een gebruiker maar kan ook een service zijn)
- De Service Provider (SP), deze heeft al rol het toekennen van services aan de gebruiker
- De Identity Provider (IDP), heeft als rol het controleren van de identiteit van de gebruiker die een verzoek om een service bij de SP heeft ingediend.

Op het moment dat er tussen de Identity Provider en de Service Provider een samenwerking is gecreëerd, dan noemt men dat een Circle of Trust.
Deze Circle of Trust komt tot stand door het uitwisellen van Metadata ( bestaat uit config informatie die de SP een IDP met elkaar kunnen delen).

Hoe werkt SAML:

SAML [12] werkt met meerdere stappen om authenticatie te verlenen:

1. De gebruiker authentiseert zich bij de Identity Provider door middel van een webbrowser.
2. Er wordt door de Identity Provider een SAML token uitgedeeld aan de gebruiker met daarin de gegevens over zijn identiteit.
3. De webbrowser van de gebruiker wordt vervolgens door de Identity Provider gerouteerd naar de locatie van de Service Provider. De webbrowser plaats vervolgens een verzoek bij de Service Provider met het SAML token inbegrepen. De Service Provider onderzoekt deze SAML token om te kijken of de inhoud van het token overeenkomt met de informatie die hij heeft door de samenwerking met de Identity Provider. Als dit akkoord is dan zal de toegang verleend worden.




Figuur 3: SAML inlogproces
Bron: [11]

***Wat is het risico van SAML?***

Als een gebruiker ingelogd is dan kunnen er vervolgens meerdere web applicaties gestart worden en wanneer deze uitlogt, dan bestaat de kans dat de resterende applicatie sessies op de achtergrond nog een openstaande connectie hebben. Naast het configureren van Single Sign-on mogelijkheid zal er ook een inrichting op het gebied van Single Sign-off moeten plaatsvinden. De gebruiker zou de mogelijkheid moeten hebben om door middel van één uitlogfunctie, alle openstaande sessies te verbreken.

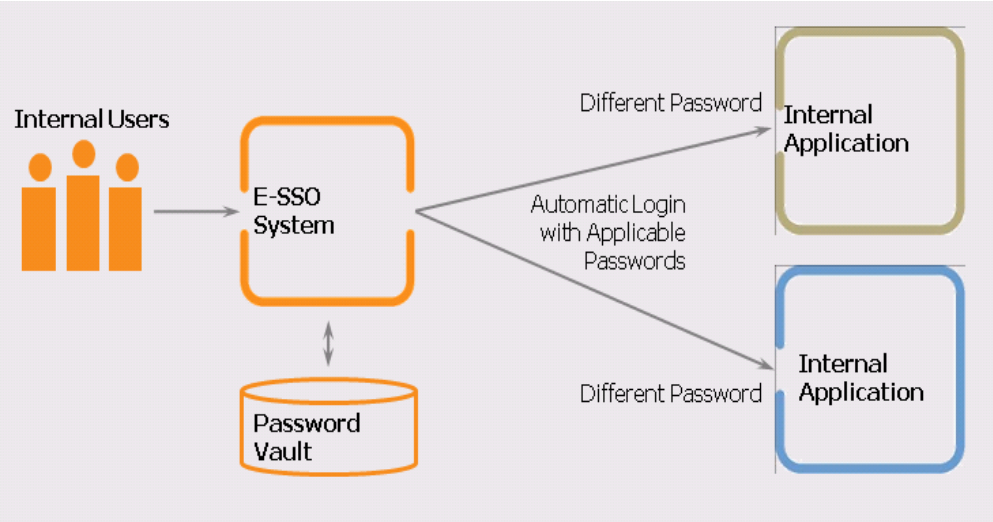
Wanneer er een storing plaatsvindt bij de Identity Provider of bij de Service Provider dan kan er geen toegang meer worden verleend aan de gebruiker die in wil loggen. Het wegvallen van één van deze schakels kan daarom een Single Point of Failure zijn.

### 3.2.4 E-SSO

Enterprise Single Sign-on (E-SSO) is een oplossing die voor meerdere applicaties gebruikt kan worden, voor zowel intern als externe applicaties (Cloud ). Op de desktop wordt er een Single Sign-on client geïnstalleerd en deze client heeft de mogelijkheid om diverse inlogschermen te herkennen en hiervan de gegevens op te slaan. Op het moment dat de gebruiker een applicatie opstart dan worden de inloggegeven automatisch ingevuld nadat deze eenmalig geconfigureerd is. Deze techniek van inloggen is niet afhankelijk van de leverancier en welke vorm van authenticatie deze toepast op zijn applicatie. E-SSO [9,18] oplossing is in staat om meerdere applicaties van diverse platformen te ondersteunen op het gebied van éénmalig inloggen dit is onafhankelijk van waar de gebruikers inlogt. Tevens is het mogelijk om met deze oplossing gebruik te maken van Single Sign-off zodat openstaande connecties worden voorkomen.

***Wat zijn de eigenschappen van Enterprise Single Sign-on?***

Er zijn veel Enterprise Single Sign-on oplossingen die gebruik maken van de LDAP authenticatie methode om gebruikersnamen te verifiëren. De gebruiker voeren bij het opstarten van de desktop de inloggegevens in en de Single Sign-on software op de client verstuurd deze gegevens naar de centrale server. De centrale server maakt connectie met het Active Directory door een LDAP koppeling en stuurt de gegevens van de gebruiker door. Als de ingevoerde gegevens kloppen dan wordt dit terug gekoppeld naar de client en kan de gebruiker succesvol inloggen.




Figuur 4: E-SSO systeem
Bron: [19]

De inloggegevens die de Enterprise Single Sign-on client verzamelt worden versleuteld opgeslagen in een database. Voor het gebruik van deze oplossing is een centrale server in het netwerk noodzakelijk, hier worden de gebruikers profielen beheerd. Door middel van een console kan de configuratie ingesteld worden.

Het uitvallen van één van de componenten (Centrale server, Database) kan er gelijk voor zorgen dat het niet meer mogelijk is om nog een succesvolle inlog op het systeem uit te kunnen voeren. De centrale server kan in twee uitvoeringen toegepast worden: Fysieke server die redundant uitgevoerd kan worden, met één server op de hoofdlocatie en één server op de uitwijk locatie. Daarnaast kan de centrale server virtueel aangemaakt worden, ook op beide locaties. Om de risico's te spreiden kan er gekozen worden voor een splitsing van beide keuzes. Een fysieke server en een virtuele server, dit kan de beschikbaarheid verhogen omdat de kans kleiner is dat zowel een fysieke en een virtuele server gelijktijdig niet benaderbaar zijn.

De authenticatiemethode van een Enterprise Single Sign-on systeem, is niet veilig als er geen twee-weg authenticatie wordt toegepast. Omdat enkel toegang met een inlognaam en wachtwoord op het systeem waar de gebruiker voor is geauthentiseerd niet voldoende is. ( wordt nader beschreven in 3.4.2 - *Op welke wijze kunnen de risico's beheersbaar blijven* )

## 3.3 SAMENVATTING

Er zijn diverse technieken die bijdragen aan de werking van een Single Sign-on oplossing, LDAP en KERBEROS zijn gebaseerd op het gebruik van directory services [17] en SAML is ontwikkeld om het inloggen op web applicaties te kunnen voorzien van Single Sign-on. De onderstaande tabel geeft van elke technologie de belangrijkste voor- en nadelen.

| Technologie | Voordelen | Nadelen |
|---|---|---|
| LDAP | - Gebaseerd op gebruik Active Directory.<br>- Authenticatie en autorisatie van gebruiker is mogelijk.<br>- Centrale opslag inloggegevens in Active Directory | - Applicatie moet beschikken over de mogelijkheid voor een LDAP koppeling om te functioneren. |
| Kerberos | - Wachtwoorden worden niet over het netwerk verstuurd.<br>- Sterke vorm van authenticatie.<br>- Centrale opslag inloggegevens in Active Directory | - Applicatie moet beschikken over de mogelijkheid voor een KERBEROS koppeling om te functioneren.<br>- Kan geen autorisatie bieden aan gebruikers. |
| SAML | - Single Sign on toepassing voor het gebruik van web-applicaties | - Alleen te gebruiken voor web-applicaties |
| E-SSO | - Centrale authenticatiebron voor meerdere applicaties, ongeacht welke soort authenticatie deze hanteert<br>- Single Sign-off toepasbaar | - twee-weg authenticatie noodzakelijk i.v.m. beveiliging.<br>- Centrale server moet redundant uitgevoerd worden, anders Single point of Failure. |

De Bestuursdienst Ommen-Hardenberg maakt gebruik van diverse applicaties en platformen die niet allemaal gekoppeld zijn aan één authenticatiebron. Een gedeelte van de applicaties maakt gebruik van een LDAP koppeling naar het Active Directory, er zijn ook web applicaties die een authenticatiebron hebben op het gebied van de SAML standaard.
De web applicaties die gebruik maken van een Cloud [10] oplossing, en waar de authenticatiebron dus niet binnen het eigen netwerk aanwezig is kunnen met LDAP en Kerberos niet voorzien worden van een Single Sign-on mogelijkheid.
Om ervoor te zorgen dat nagenoeg alle applicaties van Single Sign-on voorzien kunnen worden, is het implementeren van een Enterprise Single Sign-on oplossing een goede keuze.
Omdat er een centrale authenticatiebron aangemaakt wordt, die vervolgens met diverse authenticatiebronnen bestaande inloggegevens kan uitwisselen.
De centrale omgeving wordt gevuld met data die door een Single Sign-on client op de desktop verzameld wordt. Het is mogelijk om de database (Oracle/SQL) op een andere plek binnen het netwerk te plaatsen.
Deze kan dus ook geplaatst worden op een bestaande database server, dit kan een besparing in licentiekosten op gebied van database licentie opleveren ten opzichte van het plaatsen van de database op een centrale Enterprise Single Sign-on server.

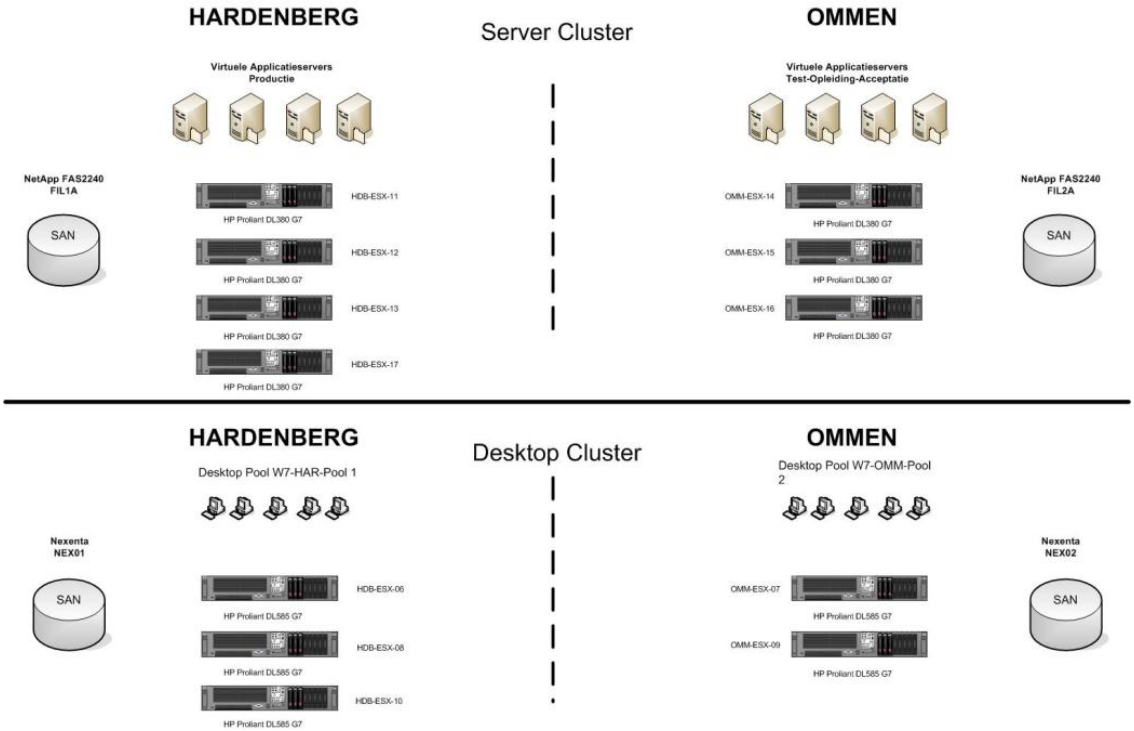
Het beheren van de gebruikersaccount kan dan op één plek plaatsvinden, voor het technische beheer kan dit een besparing opleveren qua tijd. De beheerder hoeft namelijk niet meer op verschillende authenticatiebronnen aan te loggen, om hier vervolgens de inloggegevens aan te passen.

## 3.4 HUIDIGE INFRASTRUCTUUR:

### 3.4.1 BESCHRIJVING BESTAANDE INFRASTRUCTUUR

De bestaande infrastructuur bij de Bestuursdienst Ommen-Hardenberg bestaat voornamelijk uit gevirtualiseerde systemen en desktops. De organisatie is fysiek verdeeld over meerdere gebouwen, er zijn diverse buitenlocaties ( zwembaden, theater, beheer openbaar gebied en het Lokaal Opleidingen Centrum) deze zijn opgenomen in het cluster van Hardenberg of Ommen. Er zijn in totaal 550 werkplekken, welke voorzien zijn van een thin-client ( DELL FX-100) in combinatie met een VDI desktop. De desktop is voorzien van een Windows 7 image met enkele applicaties lokaal geïnstalleerd.

De infrastructuur bestaat o.a. uit 12 ESX-hosts die gebruikt worden voor het hosten van 80 virtuele servers en 550 virtuele desktops. Er is een redundant Oracle platform aanwezig die bestaat uit twee fysieke servers en verdeeld is over de locatie Hardenberg en Ommen. Op de locatie Ommen is tevens de uitwijk omgeving opgezet, voor zowel de VMWare omgeving en de Oracle databaseserver.



Figuur 5: Bestaande VMWare infrastructuur

Het aantal ESX-hosts in het desktop cluster is niet evenredig verdeeld over de twee locaties, dit heeft te maken met het aantal gebruikers per locatie. In Hardenberg zijn er meer gebruikers actief dan in Ommen en wordt er meer van het desktop cluster gevraagd op gebied van resources. Daarom is er op de locatie Hardenberg één extra ESX-host ten behoeve van het desktop cluster.

Het verschil tussen het aantal ESX-hostst op het server cluster tussen Hardenberg en Ommen heeft te maken met de uitwijk. Er is voor gekozen om alle applicatie server (met uitzondering van enkele VMWare Virtual Console servers en VMWare connection Servers, voor het gebruik van VDI) op het server cluster van Hardenberg te plaatsen. Het server cluster in Ommen wordt gebruikt als uitwijklocatie in geval van calamiteiten en is in staat om de belangrijkste applicatieservers te hosten.

Op het gebied van beheer ICT is er geen onderscheid tussen ondersteuning aan beide gemeentes, door het samenwerkingsverband is er één organisatie ontstaan. Er heeft er een harmonisatie tussen applicaties en systemen van beide locaties plaatsgevonden en de desktop image die op beide locaties wordt gebruikt is identiek.

De gebruikers hebben de mogelijkheid om thuis te werken, dit wordt gefaciliteerd door middel van een software token dat de gebruiker tijdens het inloggen op zijn mobiele telefoon ontvangt.

***Hoe kan de Single Sign-on oplossing in de bestaande ICT-infrastructuur geïmplementeerd worden?***

Wanneer er wordt gekozen voor een Enterprise Single Sign-on oplossing dan zullen er aanpassingen op de bestaande omgeving plaats moeten vinden. Er moet een nieuwe virtuele server aangemaakt worden of er zal een fysieke server geplaatst kunnen worden. Om ervoor te zorgen dat er een Single Sign-on client beschikbaar is voor de gebruikers, zal de Windows 7 desktopimage van de Bestuursdienst aangepast moeten worden. De client moet namelijk lokaal geïnstalleerd worden om ervoor te kunnen zorgen dat de inloggegevens voor Single Sign-on gesynchroniseerd kunnen worden met de centrale server.

### 3.4.2 BESCHRIJVING HUIDIG TOEGANGSBELEID

***Welke rol speelt informatiebeveiliging in de huidige omgeving?***

In de afgelopen jaren is gebleken dat er een toenemende kwetsbaarheid ontstaat op het gebied van informatiebeveiliging, de oorzaak hiervan zijn diverse incidenten rondom overheidsinformatie en overheidssystemen. Er is op 29 november 2013 door een groot deel (95%) van alle gemeenten in Nederland een besluit aangenomen met daarin de afspraak dat alle gemeenten op 1 januari 2016 moeten voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) [20].

Het huidige ICT beleid op het gebied van wachtwoord en user policies, wordt op dit moment al getoetst aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De regels die nu gehanteerd worden zijn opgesteld na aanleiding van de informatie die wij als organisatie uit de BIG hebben gehaald *( zie bijlage 8.3).*

***Welke oplossing past het beste bij de organisatie in samenwerking met het huidige ICT-beleid?***

Het huidige ICT beleid op het gebied van toegangsbeveiliging zorgt ervoor dat de risico's zo veel mogelijk wegenomen worden.
Wanneer er een Single Sign-on oplossing gekozen wordt die de Bestuursdienst gaat toepassen, dan mag hier geen afbreuk op plaatsvinden. Om ervoor te zorgen dat het beveiligingsniveau gelijk blijft aan het beleid dat opgesteld is, zullen er op het gebied van authenticatie geen veranderingen mogen plaatsvinden die bijdragen aan een vergroting van de risico's.

***Op welke wijze kunnen de risico's beheersbaar blijven?***

Wanneer er voor een Single Sign-on oplossing wordt gekozen die tijdens het inloggen op het systeem al wordt toegepast, dan moet deze voorzien zijn van een twee-weg authenticatie. Een inlogprocedure die vervolgens de gebruikers voorziet van Single Sign-on op diverse applicaties mag niet enkel uit een inlognaam en wachtwoord bestaan. Wanneer de gebruiker deze gegevens verliest of ergens noteert dan is dit een groot risico op het gebied van security, omdat deze gegevens direct toegang geven tot het systeem en de applicaties waarvoor deze gebruiker geautoriseerd is. Het toepassen van een twee-weg authenticatie is in dit geval een voorwaarde waaraan te allen tijde moet worden voldaan. Een fysiek object gecombineerd met een wachtwoord of pincode zorgt ervoor dat de risico's beperkt worden. Het inloggen door derden zal door het toepassen van deze methode minder eenvoudig zijn, ze moeten immers beide authenticatiebronnen in bezit hebben.

***Welke aanpassing moet er plaatsvinden op gebied van security?***

Er moeten een aantal aanvullingen in het huidige beleid opgenomen worden, wanneer er een implementatie van Single Sign-on plaats gaat vinden. Onderstaande regels zouden opgenomen kunnen worden in het huidige beleid:

- Gebruikers moeten te allen tijde een twee-weg authenticatie doorlopen om toegang te krijgen tot het systeem/applicaties bij gebruik van Single Sign-on.
- Om verboden toegang voor derden te minimaliseren, moet de twee-weg authenticatie tenminste voorzien zijn van een token/toegangspas of biometriescanner.
- Zonder gebruik van twee-weg authenticatie kan de gebruiker alleen inloggen door middel van een gebruikersnaam/wachtwoord ende beantwoording van een reeks van geheime vragen.

## 3.5 BELANGRIJKSTE APPLICATIES BDOH:

Om een goed overzicht te krijgen van de belangrijkste applicaties heb ik een inventarisatie uitgevoerd. Er zijn op dit moment 17 applicaties die aan de voorwaarden van Prio 1 voldoen, van elke applicatie heb ik een korte beschrijving toegevoegd. Het aantal gebruikers verschilt per systeem.
Zo kan het voorkomen dat een applicatie waar 10 gebruikers mee werken, toch gekwalificeerd is als bedrijf kritisch.
Daarnaast zijn er ook applicaties die wel door de gehele organisatie gebruikt worden, maar niet onder deze categorie vallen (Microsoft Excel bijvoorbeeld). Het aantal gebruikers per applicatie is daarom geen graadmeter voor het criterium bedrijf kritisch.
Het uitgangspunt is de prioriteit waarmee de applicaties beschikbaar moeten zijn voor de organisatie of voor de externe dienstverlening. De belangrijkste applicaties zijn voorzien van het label Prio1.
Deze prioriteit is door de Bestuursdienst Ommen-Hardenberg samengesteld door elke applicatie te toetsen aan de onderstaande criteria:

Prio 1 voorwaarden:

- *Applicatie is bedrijf kritisch op het moment dat de gebruiker zonder toegang tot deze applicaties, niet in staat is om een goede dienstverlening aan de burger te verlenen.*
- *Applicatie wordt organisatie breed gebruikt, geen toegang verstoord de mogelijkheid tot uitvoeren van productie.*
- *Applicatie wordt door een volledige afdeling gebruikt, geen toegang verstoord de mogelijkheid tot het uitvoeren van productie.*
- *Applicatie is bedrijf kritisch op het moment dat de gebruiker zonder toegang tot deze applicaties, niet in staat is om een goede dienstverlening aan de organisatie te leveren.*

De onderstaande applicaties voldoen aan de criteria Prio 1 die door de Bestuursdienst Ommen-Hardenberg is opgesteld op het gebied van bedrijf kritische systemen.

***Recreatex***

Deze applicatie zorgt ervoor dat de gebruikers van het theater en de zwembaden de reserveringen van klanten digitaal in kunnen boeken. In de applicatie zit tevens een betaalmogelijkheid voor klanten, de zogenoemde kassamodule.

***Kofax***

De afdeling DIV is verantwoordelijk voor het archiveren en registreren van de binnen gekomen poststukken, brieven en contracten. Deze worden vervolgens digitaal gescand met behulp van de applicatie KOFAX, en aan de betreffende afdelingen aangeboden door gebruik te maken van onze DMS applicatie.

### *Verseon*

Verseon wordt binnen de organisatie gebruikt als het DMS (document management systeem), alle externe post die wordt digitaal gescand en vervolgens ingelezen in de applicatie. Ook interne documenten worden in Verseon opgeslagen onder zogenoemde zaak-archieven.

### *SBA*

SBA is een systeem voor vergunningverlening en handhaving. Het wordt binnen de Bestuursdienst gebruikt voor het verlenen van vrijwel alle vergunningen, inclusief gerelateerde processen zoals ruimtelijke ordening, toezicht- en handhaving. Daarnaast wordt SBA binnen de Bestuursdienst ook gebruikt voor de gemeentelijke verhuur van sportaccommodaties in de gemeenten Hardenberg en Ommen. Om deze processen goed te ondersteunen is SBA gekoppeld met diverse andere gemeentelijke systemen.

### *RAET*

De applicatie van RAET wordt gebruikt door de medewerkers van HRM (personeelszaken) voor het verwerken van de salarisadministratie. Het draaien van de maandelijkse salarisrun ’s die voor de medewerkers van HRM in kaart brengt wat de verwachte uitgaven zijn op gebied van salaris. Daarnaast wordt de applicatie gebruikt voor het invoeren en bijhouden van ziekte en verlof. Met deze gegevens kan er een management rapportage opgesteld worden. Het verwerken van declaraties verloopt ook via deze applicatie.

De medewerkers van de overige afdelingen maken ook gebruik van de applicatie. Binnen de applicatie kan de gebruiker zijn eigen verlof digitaal aanvragen. Het declareren van reiskosten of vergoedingen en het invoeren van gemaakte overuren.

### *NGDW / Nedbrowser*

NedBrowser is een web applicatie die gebruikt wordt voor het ontsluiten van de geo-data via intranet. Tevens levert het een gebruiksvriendelijke, en flexibele beheermodule voor beheerders. NedBrowser zorgt ervoor dat het raadplegen van geometrische en administratieve gegevens en het tonen van onderlinge relaties op een efficiënte manier uitgevoerd kan worden. Tevens is er de mogelijkheid om de verschillende gebruikers en groepen gecontroleerd toegang te geven tot informatie n functionaliteit.

### *Best Deal*

Met het doel om inkoop- en factuurprocessen te optimaliseren is in 2011 gekozen voor aanschaf van het inkoopsysteem Best Deal. Deze tool maakt het mogelijk het operationele inkoopproces, van bestellen tot factureren, efficiënter te laten verlopen. Daarnaast kan met dit systeem eenvoudig managementinformatie worden gegenereerd en de jaarlijkse spendanalyses worden uitgevoerd. Dit systeem ondersteunt ook de verplichtingenadministratie.

### *Topdesk*

Topdesk wordt door de Bestuursdienst Ommen-Hardenberg gebruikt voor de registratie van verschillende onderwerpen die te maken hebben met de bedrijfsvoering binnen de organisatie. Binnen Topdesk worden alle incidenten en wijzigingen bijgehouden. Het pakket is gebaseerd op ITIL V3. De functionaliteit meldingenbeheer wordt gebruikt om incidenten en wijzigingen toe te kennen aan de desbetreffende behandelaar of afdeling. De incidenten kunnen aan een groep worden gehangen en kunnen vervolgens bewaakt worden door de Change manager. Vanuit de objecten is er een directe toegang mogelijk naar het Configuratie beheer binnen Topdesk. De medewerkers van de Bestuursdienst Ommen-Hardenberg kunnen gebruik maken van de selfservice module om zelf een incident of verzoek te melden.
Het is een applicatie die gebruik maakt van een dedicated applicatieserver waarop de programmatuur geïnstalleerd is en hierop draait een webserver die ervoor zorgt dat de applicatie door de gebruiker via een webbrowser benaderd kan worden. De database is weggezet op een Oracle 11g server.

### *SAP*

SAP is een ERP-pakket, in een ERP pakket kunnen in principe alle bedrijfsfuncties worden uitgevoerd. SAP is een standaardpakket, wat wil zeggen dat het pakket voor vele soorten bedrijven in uiteenlopende branches geschikt is.
SAP staat voor Systeme, Anwendungen und Produkte in der Datenverarbeitung (Systemen, Applicaties en Producten in gegevensverwerking). Oorspronkelijk bij de oprichting van het bedrijf SAP stond het voor System Analyse und Programmentwicklung.
SAP is een geïntegreerd informatie- en besturingssysteem waarin bedrijfsmatige processen kunnen worden vastgelegd en beheerd. Deze processen zijn ondergebracht in modules. De gegevens in de modules worden onderling direct uitgewisseld, waardoor een volledig geïntegreerd systeem ontstaat binnen SAP wordt alle informatie op een hiërarchische wijze vastgelegd. Deze structuur vindt zijn weerslag in de opbouw van de databases. In de SAP-structuur kunnen zeer grote organisaties worden vastgelegd met onderverdeling in bedrijfsnummers, fabrieken, magazijnen, etc.

### *GWS4All*

GWS4all wordt gebruikt om de gegevens van o.a. bijstandsgerechtigden, werkzoekenden en zorgvragers (WMO) te registreren.

Met dit systeem kunnen de bijstandsuitkeringen worden berekend en uitbetaald. Ook het verstrekken van voorschotten, doorbetalingen aan derden en het debiteurenbeheer wordt via GWS4all afgehandeld. Maar ook het aanleveren van CBS-statistieken en de financiële verantwoording gaat via GWS4all.

In het kader van Re-integratie en Inburgering worden gegevens van cliënten geregistreerd en wordt de applicatie als klantvolgsysteem gebruikt. Opleidingen, werkervaringstrajecten, betalingen, etc. van de cliënt worden in GWS4all vastgelegd.
Ook het aanleveren van CBS-statistieken en de financiële verantwoording gaat via GWS4all.

De aanvragen voor een voorziening Wet Maatschappelijke Ondersteuning worden in GWS4all geregistreerd, in behandeling genomen en afgehandeld. De betalingen aan cliënten en zorgleveranciers vindt ook via GWS4all plaats. De voorzieningen die aan de cliënten worden verstrekt, worden in dit systeem geadministreerd.

***JVS-Onderwijs***

Het Jeugd Volg Systeem (JVS) wordt gebruikt om gegevens over jongeren die voortijdig schoolverlaten of schoolverzuim plegen op te slaan.

***G-Kas***

G-KAS is een betalingssysteem dat bij de Bestuursdienst Ommen-Hardenberg gebruikt wordt om al het betalingsverkeer dat aan de publieksbalies plaatsvindt af te handelen. De applicatie is geïnstalleerd op de kassawerkplekken en maakt gebruik van diverse randapparatuur zoals pinapparaten, klantendisplays en bon-printers.

***G-Bos***

G-BOS is een klantgeleidingssysteem dat gebruikt wordt door de medewerkers van het Klant Contact Centrum om het proces vanaf het eerste contact met de klanten tot aan de afhandeling van de vraag te doorlopen. De applicatie is beschikbaar op zowel de kassawerkplekken maar ook op de virtuele desktop. Enkele onderdelen van de applicatie maken ook gebruik van randapparatuur zoals een klantenoproep scherm en een bon-printer.

***G-Rooster***

G-Rooster wordt gebruikt voor het aanmaken van dienstroosters. Er kunnen roosters voor de medewerkers van het KCC mee aangemaakt worden. Het bevat een grafisch planbord waar alle taken van de gebruikers aan gekoppeld kunnen worden.

***SUWINET***

De applicatie SUWINET wordt door gebruikt om persoonsgegevens uit te wisselen tussen de Bestuursdienst Ommen-Hardenberg en andere organisaties zoals: De Belastingdienst, IB-Groep, UWV, Rijksdienst Wegverkeer en het Kadaster.

***O-Prognose***

De applicatie O-Prognose wordt gebruikt door de afdeling gebouwbeheer om bouwkundige onderhoudsplannen te maken.

## 3.6 HUIDIGE LOGINS

Bij de Bestuursdienst Ommen-Hardenberg is de Active Directory het centrale punt voor authenticatie en autorisatie. Er zijn applicaties die gebruik maken van een LDAP- of KERBEROS koppeling. Echter zijn er ook applicaties die een andere vorm van authenticatie hanteren (Oracle of SQL) en daarom geen gebruik maken van Active Directory.

***Om hoeveel verschillende logins gaat het? Hebben die verschillende eisen aan het wachtwoord?***

Er zijn meerdere applicaties waarbij de authenticatie is geregeld op het platform waar het systeem ook op functioneert, enkele voorbeelden zijn: Microsoft SQL / Oracle en Firebird databases die tevens een authenticatiebron zijn voor de gebruikers van deze systemen. Daarnaast zijn er nog applicaties die een eigen authenticatie binnen de software hanteren. Ook het inlogproces op cloud-applicaties verloopt niet via het centrale punt van de organisatie, maar wordt door de leverancier van de dienst geleverd. Deze applicaties zijn niet voorzien van de standaard eis voor een sterk wachtwoord en verschillen allemaal van elkaar.

***Zijn de usernames wel overal gelijk?***

Het uitgangspunt binnen de organisatie is het hanteren van usernames zoals die ook zijn opgenomen in het Active Directory. De eerste letter van de voornaam samen met maximaal zeven letters van de achternaam vormen de inlognaam. Mijn eigen naam wordt in het Active Directory weergegevens als SBREUKEL, deze naamgeving wordt daarom ook toegepast in de applicaties die een eigen authenticatiebron hebben.

***Hoeveel applicaties hebben een eigen authenticatiebron in gebruik?***

Op dit moment zijn er bij benadering 200 applicaties in gebruik bij de Bestuursdienst Ommen-Hardenberg. Van deze applicaties zijn er 50 applicaties die wel voorzien zijn van een authenticatiebron maar geen gebruik maken van een koppeling naar het Active Directory.

## 3.7 UITKOMST LONG/SHORT LIST:

Om tot een pakketkeuze te komen ga ik gebruik maken van een pakketselectie [2]. Het uitvoeren van een pakketselectie draagt bij aan het tot stand komen van een goede en weloverwogen keuze. Er zijn meerdere fases die doorlopen moeten worden om ervoor te zorgen dat er uiteindelijk een leverancier en een pakket geselecteerd kan worden.

Deze fases worden hieronder beschreven:

1. Opstellen Longlist
   - Mogelijke leveranciers en pakketten verzamelen.
   - Lijst maken van leveranciers en pakketten.

2. RFI: Request for information
   - Opvragen informatie diverse leveranciers.
   - Longlist eventueel terugbrengen.
   - Korte vragenlijst versturen.

3. RFP: Request for Proposal
   - Uitgebreide vragenlijst versturen.
   - Overzicht maken met informatie van elke leverancier en pakket.

4. Longlist reduceren to shortlist
   - Vaststellen welke leveranciers het beste scoren op het gebied van eisen/functionaliteiten
   - In kaart brengen welk product in samenwerking met de leverancier het beste bij de organisatie zou passen.
   - Maken van shortlist en daarmee aantal leveranciers terugbrengen in aantal.

5. Proof of Concept
   - Vragen om demonstratie van pakket.
   - Opvragen van referenties en informatie.

6. Keuze leverancier en pakket
   - Keuze maken voor pakket en leverancier op basis van reeds verworven informatie en goedgekeurde Proof of Concept.

***FASE 1:***

In de eerste fase heb ik door middel van het opvragen van informatie bij leveranciers en het zoeken van producten, een lijst gemaakt van enkele aanbieders die een Enterprise Single Sign-on oplossing kunnen leveren.
De keuze voor een specifieke Enterprise Single Sign-on oplossing heb ik genomen na aanleiding van het onderzoek naar de diverse technologieën en de conclusie die ik daaruit heb getrokken.

| Leverancier | Applicatie |
|---|---|
| Evidian | Enterprise SSO |
| Tools4Ever | E-SSOM |
| Imprivata | OneSign |
| Oracle | Enterprise Single Sign-on |

***FASE 2:***

Van alle leveranciers heb ik informatie terug ontvangen betreffende het pakket dat ze aanbieden en de mogelijkheden hiervan. De Enterprise Single Sign-on oplossingen van Evidian en Tools4ever vallen af om de reden dat ze niet door geleverd kunnen worden door een leverancier of reseller waar de organisatie bekend mee is. Daarmee kan niet voldaan worden aan onze corporate policy ( leverancier moet bekend zijn binnen de organisatie en zich bewezen hebben door levering van goede diensten).

***FASE 3:***

In fase 3 heb ik van de volgende leveranciers informatie ontvangen met daarin de mogelijkheden van het product dat ze aanbieden:

- Enterprise Single Sign-on van Oracle
- Onesign van Imprivata

De functionaliteiten die aangeboden worden lijken in eerste instantie gelijk aan elkaar. Echter bij nadere inspectie van de documenten die ik van beide leveranciers heb ontvangen komen er een aantal verschillen en tekortkomingen naar voren.
Deze heb ik in fase 4 opgenomen in een tabel, om zo tot een goede pakketkeuze te komen waarin alle belangrijke punten voor de bestuursdienst Ommen-Hardenberg zijn meegenomen.

***FASE 4:***

In fase 4 heb ik een vergelijkingstabel op kunnen stellen met de belangrijkste punten op het gebied van functionaliteit. Hier moet een Enterprise Single Sign-on oplossing voor de Bestuursdienst Ommen-Hardenberg aan voldoen.

| Functionaliteit/eisen | Oracle E-SSO | Imprivata OneSign |
|---|---|---|
| Leverancier van E-SSO is binnen de organisatie bekend. | ✓ | ✓ |
| Automatisch uitloggen | ✓ | ✓ |
| Authenticatie d.m.v. Active Directory | ✓ | ✓ |
| Authenticatie met Toegangspas | ✓ | ✓ |
| 2-weg authenticatie | ✓ | ✓ |
| Sessie meenemen binnen VDI naar ander werkplek | X | ✓ |
| Terminal Server ondersteuning | ✓ | ✓ |
| Ondersteuning VMWare virtuele servers | ✓ | ✓ |
| Product bestaat uit een softwarematige oplossing | ✓ | ✓ |
| Wachtwoord resetten door gebruik van Self Service | ✓ | ✓ |
| Ondersteuning voor het gebruik van gastaccounts | X | ✓ |
| Voorzien van een web client | ✓ | ✓ |
| Dell FX-100 Teradici ondersteuning | X | ✓ |
| Single Sign-on voor Vmware Thinapp applicaties | ? | ✓ |
| Central wachtwoordbeheer | ✓ | ✓ |
| Zelf maken van scripts of connectors t.b.v. Single Sign-on is niet nodig | ✓ | ✓ |
| Installatie mogelijk binnen bestaande infrastructuur | ✓ | ✓ |

Na aanleiding van de uitkomsten in de vergelijkingstabel is gekozen om de Single Sign-on oplossing van Oracle af te laten vallen, omdat er aan een aantal functionaliteiten, die voor de Bestuursdienst Ommen-Hardenberg belangrijk zijn, niet voldaan kan worden.

Voor de omgeving van de Bestuursdienst Ommen-Hardenberg is het noodzakelijk dat het pakket dat gekozen wordt, kan voldoen aan de hardware configuratie van de thin-clients (dell fx-100 inclusief Teradici firmware) die wij als organisatie gebruiken. Nader onderzoek (telefonisch contact met vertegenwoordiger van Oracle) heeft uitgewezen dat ze niet kunnen toezeggen dat de oplossing die Oracle aanbiedt technisch kan functioneren met de hardware van onze organisatie.
Aangezien dat dit noodzakelijk is voor het gebruik van twee-weg authenticatie met bijvoorbeeld een toegangspas.

Tevens het gebruik van Single Sign-on in samenwerking met VMWare Thinapp applicaties kan door Oracle niet bevestigd worden, daarom is besloten Oracle als leverancier af te laten vallen.

***FASE 5:***

Bij onze leverancier heb ik het verzoek geplaatst voor het inrichten van een Proof of Concept omgeving. Echter beschikt Imprivata Onesign niet over een trial versie en als zijn er kosten verbonden aan het inrichten van een Proof of Concept omgeving. De leverancier heeft niet de mogelijkheid om deze POC binnen de periode van mijn afstuderen in te richten. Wel heb ik referenties ontvangen om op deze manier toch een indruk te krijgen van het product dat ze leveren.

***FASE 6:***
Ondanks dat er geen nog Proof of Concept heeft plaatsgevonden, komt de Enterprise Single Sign-on oplossing van Imprivata als beste uit de pakketselectie. Deze zal zich echter in de toekomst nog wel definitief moeten bewijzen als er een functionerende testomgeving is opgeleverd.

## 3.8 REFERENTIEBEZOEKEN

Om te kijken hoe andere organisaties het traject van een Single Sign-on oplossing zijn doorlopen, heb ik gebruik gemaakt van een referentiebezoek.

Welke problemen zijn deze organisaties tegen gekomen en welke oplossingen hebben ze doorgevoerd? Door vragen te stellen krijg ik goed inzichtelijk wat voor ons eventuele valkuilen kunnen zijn. Zij hebben immers al de nodige ervaring met Single Sign-on en kunnen aanbevelingen geven of juist waarschuwen voor gevaren van een bepaalde keuze.

### 3.8.1 UMC GRONINGEN

De eerste organisatie die ik benaderd heb was het UMC Groningen na aanleiding van een telefonisch gesprek met onze leverancier. Zij hebben gekozen voor de Enterprise Single Sign-on oplossing van Imprivata.

Echter in het gesprek dat ik met de systeembeheerder van de afdeling ICT in het UMC Groningen heb gevoerd, kwam naar voren dat er nog geen productie omgeving aanwezig is. Andere projecten hebben bij het UMCG op dit moment een hogere prioriteit. Er is een pilot omgeving opgezet, waar nog druk in getest wordt. De bevindingen waren goed maar een definitieve uitrol in de productieomgeving hebben ze nog niet gepland. Ik heb daarom besloten om de omgeving niet op locatie te bekijken.

### 3.8.2 DEVENTER ZIEKENHUIS

Het tweede referentiebezoek heeft plaatsgevonden bij het Deventer Ziekenhuis. Op de website van Imprivata heb ik gezocht naar referenties die ik zou kunnen benaderen. Toen ik daar het Deventer Ziekenhuis als referentie zag staan, heb ik telefonisch contact opgenomen met de ICT afdeling van dit ziekenhuis. De Enterprise Single Sign-on oplossing wordt daar in praktijk toegepast.

Ik ben daar ontvangen op de ICT afdeling en heb alle onderdelen van het systeem mogen bekijken. De infrastructuur waarop de Single Sign-on omgeving geïnstalleerd is en de randapparatuur die gebruikt wordt binnen deze organisatie.
De centrale server voor de Imprivata software is in deze organisatie gevirtualiseerd en redundant uitgevoerd.
Er wordt gebruik gemaakt van een card-reader die in samenwerking met de toegangspas zorgt voor Single Sign-on. Daarnaast heb ik de configuratie kunnen bekijken en kunnen zien hoe het gehele proces verloopt om een applicatie gereed te maken voor Single Sign-on in deze organisatie.

Ze hebben aangegeven in de toekomst nog meer applicaties te willen voorzien van Single Sign-on, de noodzaak lag bij deze organisatie echter voornamelijk in het snel voorzien van inloggen op specifieke applicaties voor artsen en verpleegkundigen. Daar zijn ze in mijn ogen, zeer zeker in geslaagd.
Het referentiebezoek voor mij een toegevoegde waarde gehad, omdat ik heb kunnen zien hoe deze oplossing daadwerkelijk functioneert in de praktijk.

# 4 ONTWERPFASE

## 4.1 FUNCTIONEEL ONTWERP

Het functionele ontwerp beschrijft de functionaliteiten (eisen/wensen) waar de gekozen Single Sign-on oplossing aan moet voldoen. Om deze vraag te beantwoorden heb ik voor het functioneel ontwerp gebruik gemaakt van de MoSCow methode:

**Must have this?** *(Minimale eisen waaraan de Single Sign-on oplossing moet voldoen)*

- Van de Prio 1 applicaties moet 90% succesvol voorzien kunnen worden van een Single Sign-on functie.
- De resterende applicaties (client/server, legacy en web applicaties) moeten voor 80% succesvol geconfigureerd kunnen worden voor het gebruik van Single Sign-on.
- Na de initiële inlog-procedure is het mogelijk om deze applicaties zeer snel via dezelfde inlog-procedure te openen.
- Het wachtwoordbeheer moet gemakkelijk in gebruik zijn voor zowel de ICT medewerkers als de eindgebruikers.

- Het zelf schrijven van scripts, maken van connectors of specifieke integratie werkzaamheden ten behoeve van Single Sign-on is niet nodig.
- Een verandering van het wachtwoord moet automatisch doorgevoerd worden voor het gebruik van Single Sign-on in andere applicaties.
- De Single Sign-on oplossing moet redundant opgeleverd worden in de vorm van twee virtuele servers (VMWare).
- Dagelijkse back-up mogelijkheid van de omgeving moet aanwezig zijn.
- Restoren van de omgeving moet binnen enkele minuten plaats kunnen vinden.
- De Single Sign-on oplossing moet in de bestaande infrastructuur geïnstalleerd worden, en functioneel zijn bij het gebruik van een virtuele server, virtuele desktop en een fysieke pc.
- Het huidige beleid op het gebied van security moet minimaal gehandhaafd kunnen worden
- Het Active Directory blijft leidend op het gebied van identiteiten, rollen en rechten.
- Single Sing-on client software moet opgenomen worden in de Windows 7 image, en mag andere applicaties die lokaal zijn geïnstalleerd niet belemmeren in gebruik.
-

**Should have this if at all possible?** *(Eisen waaraan de Single Sign-on oplossing moet voldoen, maar een vergelijkbare oplossing is ook goed)*

- Het wijzigingen van wachtwoorden en het gebruik van applicaties door gebruikers moet worden opgeslagen in logboeken.
- De gebruikers van de Bestuursdienst Ommen-Hardenberg hebben geen training nodig om van Single Sign-on gebruik te maken.
- Gebruikers moeten zelf het wachtwoord kunnen wijzigen als ze deze vergeten is.
- De authenticatie moet minimaal de sterkte van de huidige login hanteren, en waar mogelijk vergroten.
- Implementatie wordt uitgevoerd in samenwerking met tenminste één collega van technisch beheer.

**Could have this if it does not affect anything else?** *( Wensen die gerealiseerd kunnen worden als er tijd over is)*

- Op het moment dat een gebruiker de organisatie gaat verlaten, moet er nu in diverse applicaties een verwijdering van het gebruikersaccount plaatsvinden. Een koppeling vanuit de Single Sign-on oplossing die dit automatisch kan uitvoeren is wenselijk.

**Won't have this but would like to have this in the future?** *(Wensen die geen prioriteit hebben, maar wellicht interessant zijn voor in de toekomst)*

- Functionaliteiten bekijken van diverse biometrie oplossingen voor het gebruik van twee-weg authenticatie.

### 4.1.2 VERWACHTE KOSTEN

Bij de verwachte kosten wordt er een indicatie gegeven van de kosten voor een implementatie van een Imprivata Onesign Single Sign-on oplossing bij de Bestuursdienst Ommen-Hardenberg. Er is uitgegaan van de bestaande infrastructuur. De kosten zijn gebaseerd op het contact dat heeft plaatsgevonden tussen de uitvoerder van dit project en de reseller van de software.

| Aantal | Omschrijving | Prijs | Totaal |
|---|---|---|---|
| 650 | License: SSO/AM | € 63,00 | € 40.950,00 |
| 650 | License: OneSign | € 10,00 | € 6630,00 |
| 650 | License: OneSign SSPW Management | € 9,00 | € 5850,00 |
| 12 | OneSign Standard Maintenance | € 1030,00 | € 12.360,00 |
| 2 | OneSign New Virtual Appliance | € 1555,00 | € 3100,00 |
| 2 | Installatie/configuratie on site per dagdeel | 486,00 | € 972,00 |
| 6 | Consultancy per dagdeel | €486,00 | € 2916,00 |
| 550 | RFIdeas AIR ID (Mifare) CSN USB Reader | € 62,00 | € 34.000,00 |
| | | | |
| 1 | Total prijs voor implementatie in de gehele organisatie | | € 106.778,00 |

### 4.1.3 VERWACHTE BESPARINGEN

Wanneer een gebruiker niet kan inloggen omdat deze het wachtwoord is vergeten, of omdat verlopen is dan moet er gebeld worden met het ISP. Hier wordt vervolgens de melding geregistreerd en doorgezet naar een medewerker van het team ICT. De gehele looptijd van dit proces kan oplopen tot 15 minuten per gebruiker.
Als dit jaarlijks 3 keer plaatsvindt, dan is dit een periode van ongeveer 45 minuten per gebruiker waarin geen productiewerkzaamheden kunnen plaatsvinden. De invoering van Single Sign-on kan daarom bijdragen aan reductie van inactiviteit voor een gebruiker op dit gebied.

De ondersteuning vanuit het team ICT die aan de gebruiker geboden wordt op het moment dat deze niet in kan loggen, zal ook verminderen.
Dit kan bijdragen aan minder support op gebruikersaccounts en deze tijd kan vervolgens benut worden voor het uitvoeren van andere werkzaamheden.

Als er een automatische koppeling gecreëerd kan worden in de Single Sign-on oplossing, die het aanmaken en verwijderen van gebruikers in diverse applicaties kan faciliteren vanuit één locatie, dan betekend dit dat er minder vanuit ICT minder tijd nodig is voor het beheer op gebruikersaccounts. De beheerder van deze gegevens hoeft immers niet meer voor elke applicatie apart de inloggegevens aan te passen of te verwijderen wanneer er een wijziging plaatsvindt. Dit levert dit een besparing op het gebied van ICT werkzaamheden.

De tijd die de gebruikers in de huidige situatie kwijt is bij het aanloggen van diverse applicaties wordt teruggebracht door middel van Single Sign-on. Dit zou een besparing op moeten leveren op gebied van tijd, minder inlogschermen en minder gegevens om te bewaren of op te zoeken.

### 4.1.4 CONSEQUENTIES VOOR DE ORGANISATIE

Als de implementatie van Single Sign-on wordt uitgevoerd, dan is het voor de gebruikers van de Bestuursdienst belangrijk om eventueel getraind te worden in het gebruik hiervan. Het aanleveren van een handleiding met daarin de uitleg en functionaliteiten van Single Sign-on kan voldoende zijn.

### 4.1.5 BEHEER SINGLE SIGN-ON

Voor het uitvoeren van het beheer op een Single Sign-on oplossing dient er binnen de Bestuursdienst Ommen-Hardenberg een beheerder beschikbaar te zijn. Deze beheerder moet beschikken over uitgebreide kennis en affiniteit met Single Sign-on. Het verzorgen van updates, configuraties en een dagelijkse back-up van dit systeem, valt ook onder deze werkzaamheden. Tevens dient er een 2$^{e}$ beheerder aanwezig te zijn binnen de organisatie, die kan ondersteunen. Zodat kennis niet op één plek bekend is.

### 4.1.6 VOORDELEN

Voordelen implementatie Enterprise Single Sign-on:

- Minder inlogschermen voor de gebruiker.
- Minder gebruikersnamen en wachtwoorden voor de gebruiker.
- Afdwingen gebruik sterke wachtwoorden.
- Minder beheer voor het ISP en ICT op gebied van wachtwoorden.
- Bij toepassing twee-weg authenticatie, verhoging van beveiligingsniveau.
- Hantering securityregels Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

### 4.1.7 NADELEN

Nadelen implementatie van Enterprise Single Sign-on:

- De kosten voor implementatie zijn relatief hoog (licenties, cardreaders en onderhoudskosten)
- De configuratie van Single Sign-on in de bestaande omgeving vergt tijd.
- Beheerders moeten kennis opdoen van Single Sign-on.

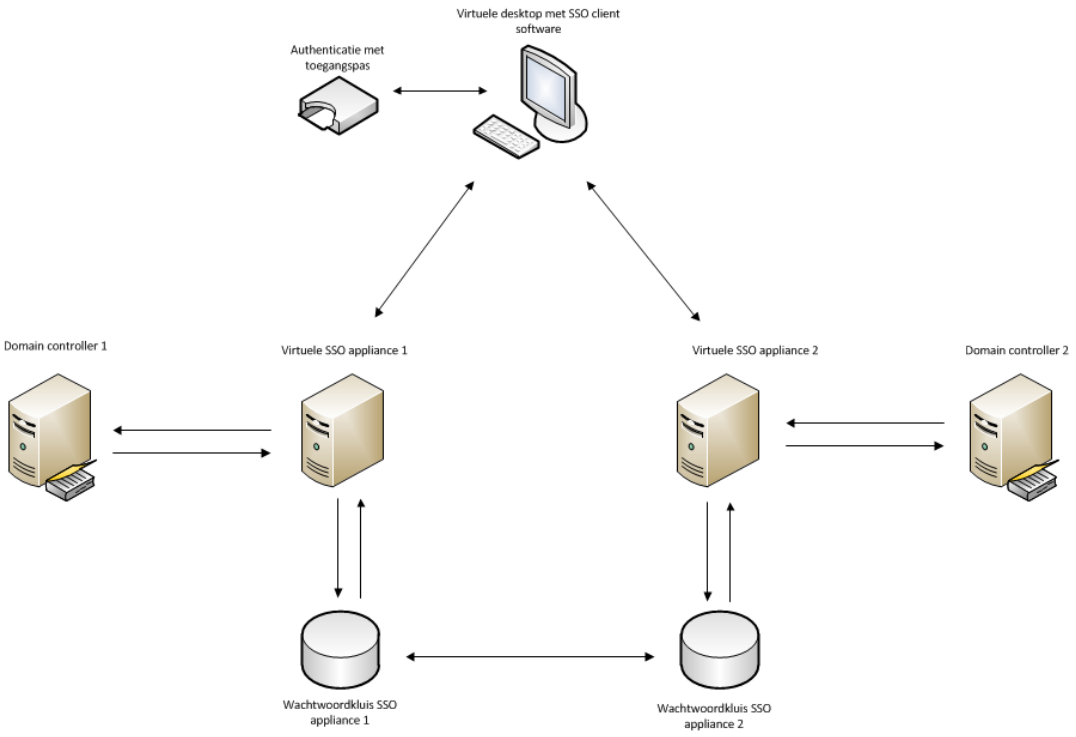
## 4.2 TECHNISCH ONTWERP

In het technische ontwerp volgt een beschrijving met daarin de apparatuur die noodzakelijk is om aan de eisen van het functioneel ontwerp te kunnen voldoen.

Benodigdheden voor implementatie Single Sign on:

- USB Cardreader of USB Biometriescanner
- Client Software Single Sign-on
- 2 x Virtuele Servers Microsoft Windows Server 2012
- 2 x Database server Oracle 11g of Microsoft SQL Server 2008
- 2 x Active Directory Domain controller

Onderstaande tekening geeft de gewenste situatie op technisch gebied weer:




Figuur 6: Gewenste opbouw infrastructuur voor E-SSO

# 5 PROOF OF CONCEPT

Bij onze leverancier heb ik het verzoek geplaatst voor het aanleveren van trial-software zodat ik hiermee een testomgeving in zou kunnen richten. Echter beschikt Imprivata Onesign niet over een trial versie die zelf ingericht mag worden.

De reden die hiervoor wordt opgegeven, is dat de installatie alleen uitgevoerd mag worden door een medewerker van Imprivata of een Reseller die beschikt over de nodige competenties/certificering. Dit om de waarde van het product ten volle tot zijn recht te laten komen. Tevens zijn er kosten verbonden aan het inrichten van een Proof of Concept omgeving. Bij onze reseller heb ik daarom een offerte opgevraagd.

In overleg met mijn bedrijfsbegeleider heb ik afgesproken dat we de offerte afwachten, maar dat de testomgeving in de toekomst wel ingericht moet worden.

# 6 VOORSTEL NA ONDERZOEK

De Bestuursdienst Ommen-Hardenberg maakt gebruik van diverse applicaties en platformen die niet allemaal gekoppeld zijn aan één authenticatiebron. Voor de gebruiker betekent het dat er bij het opstarten van diverse applicaties meerdere keren ingelogd moet worden.
De uitkomst hiervoor is het invoeren van een Single Sign-on oplossing die ervoor kan zorgen dat de gebruiker door middel van éénmalig inloggen meerdere applicaties en systemen kan starten vanaf dezelfde werkplek.

Het grote voordeel is dat er een centrale authenticatiebron aangemaakt wordt, die vervolgens met diverse authenticatiebronnen bestaande inloggegevens kan uitwisselen.
De impact op de bestaande infrastructuur is niet ingrijpend en kan met aanvulling van enkele hardwarecomponenten (card-readers) probleemloos geïmplementeerd worden. Door strengere regels op het gebied van toegangsbeveiliging binnen de organisatie (BIG) is het invoeren van Single Sign-on tevens een verbetering op gebied van informatiebeveiliging.

Het gebruik van cloud-applicaties binnen de organisatie neemt toe, en daarmee ook het aantal gebruikers welke toegang hebben tot bedrijfsinformatie die vanaf het internet te benaderen is. Een oud-medewerker waarvan het account niet is verwijderd kan op deze manier toch nog steeds toegang krijgen tot systemen.
Met de invoering van Enterprise Single-Sign-on voor het centraal aanmaken- en verwijderen van gebruikers voor alle systemen waarop deze gemachtigd is kan dit voorkomen worden. Single Sign on kan mede bijdragen aan een hoger beveiligingsniveau bij het gebruik van cloud applicaties.

Mijn voorstel na aanleiding van het onderzoek dat ik heb uitgevoerd, is het implementeren van een Enterprise Single Sign-on oplossing. De keuze is gebaseerd op het feit dat meerdere applicaties, ongeacht van welk platform de applicatie gebruik maakt, voorzien kunnen worden van Single Sign-on. Na aanleiding van de pakketselectie en de referentiebezoeken is de keuze voor de applicatie OneSign van Imprivata het beste voor de organisatie. De huidige toegangspassen kunnen gebruikt worden voor de twee-weg authenticatie en Onesign heeft de mogelijkheid om te functioneren met de thin-clients die de Bestuursdienst Ommen-Hardenberg in gebruik heeft. De implementatie kosten zijn hoog, echter kan Single Sign-on op termijn wel een besparing opleveren in het verminderen van inactiviteit door een vergeten wachtwoord, en het afnemen van beheer op inloggeggevens.

# 7 LITERATUURLIJST


[1] Grit, R., Julsing, M. (2009). *Zo doe je onderzoek*. (Eerste druk). Groningen: Noordhoff.

[2] Zijlstra, W. *Methode en checklist pakketselectie en –implementatie*. (2006) http://www.zbc.nu/ict/projectmanagement-ict/methode-en-checklist-pakketselectie-en-implementatie-deel-1/ (geraadpleegd op 24-05-2014)

[3] Verbeek, T. *SWOT Analyse voorbeeld*. (2011) http://www.voorbeeldvinden.nl/swot-analyse-voorbeeld/ (geraadpleegd op 24-05-2014)

[4] Steehouder, M., Jansen C., Mulder J., Zeijl, W. (2006). *Leren communiceren*. (zesde druk). Groningen: Noordhoff.

[5] Bellaard, M. *Single Sign-on kan de oplossing zijn* (2014) http://www.computable.nl/artikel/opinie/security/5059222/1276896/single-sign-on-kan-d-oplossing-zijn.html/

[6] Merkow, M, Breithaupt, J. *Information Security: Principles and Practices, Second Edition. (*2014) http://proquest.safaribooksonline.com.www.dbproxy.hu.nl/book/networking/security/9780133589412/chapter-10dot-access-control-systems-and-methodology/ch10lev1sec5?query=((Single+Sign-on))

[7] Buecker, A. Patel,N. Rahnenfuehrer, D.Herzele van,J*. Enterprise Single Sign-On Design Guide Using IBM Security Access Manager for Enterprise Single Sign-On 8.2 ( Strong authentication by using biometrics) (*2012) http://proquest.safaribooksonline.com.www.dbproxy.hu.nl/book/networking/security/0738437034/appendix-cdot-configuring-strong-authentication/ww503942_xhtml?bookview=search&query=SSO

[8] Huntington Ventures Ltd. SSO and LDAP Authentication (2006) http://www.authenticationworld.com/Single-Sign-On-Authentication/SSOandLDAP.html

[9] Buecker, A. Patel,N. Rahnenfuehrer, D.Herzele van,J*. Enterprise Single Sign-On Design Guide Using IBM Security Access Manager for Enterprise Single Sign-On 8.2 (*2012) http://proquest.safaribooksonline.com.www.dbproxy.hu.nl/book/networking/security/0738437034

[10] Seinen, T. *De toekomst van Single Sign-on (*2014) http://www.xr-magazine.nl/artikelen/1938/security/de-toekomst-van-single-sign

[11] Forum Systems. *Introduction to SAML? (*2014) http://cdn2.hubspot.net/hub/343786/file-1488047591-pdf/White-Papers/Introduction_to_SAML.pdf?t=1411682657630

[12] ir. A.C.M. Smulders, ir D. Krukkert. SAML V2.0 (2009) http://forumstandaardisatie.nl/fileadmin/os/documenten/concept%20CS06-11-06%204b-SAML%20expertadvies.pdf

[13] NORA. Patroon voor single sign-on (2014) http://www.noraonline.nl/wiki/Patroon_voor_single_sign-on

[14] Walla, M. Kerberos explained (2000) http://technet.microsoft.com/en-us/library/bb742516.aspx

[15] Microsoft Technet. Key Distribution Center (2014) http://msdn.microsoft.com/en-us/library/windows/desktop/aa378170(v=vs.85).aspx

[16] Microsoft Technet. LDAP authentication (2013) http://technet.microsoft.com/en-us/library/ee690469.aspx

[17] Osmanoglu, E. *Identity and Access Management (*2013) http://proquest.safaribooksonline.com.www.dbproxy.hu.nl/book/networking/security/9780124081406/chapter-13dot-enforcement/st0040_chp013_html?bookview=search&query=SSO

[18] Oracle. Guide for Enterprise Single Sign-on (2014) http://www.oracle.com/technetwork/middleware/id-mgmt/essobg-1519075.pdf?ssSourceSiteId=ocomen

[19] Computing Blog. SSO in a federation (2011) http://my-computing-blog.blogspot.nl/2011/09/sso-in-federation.html

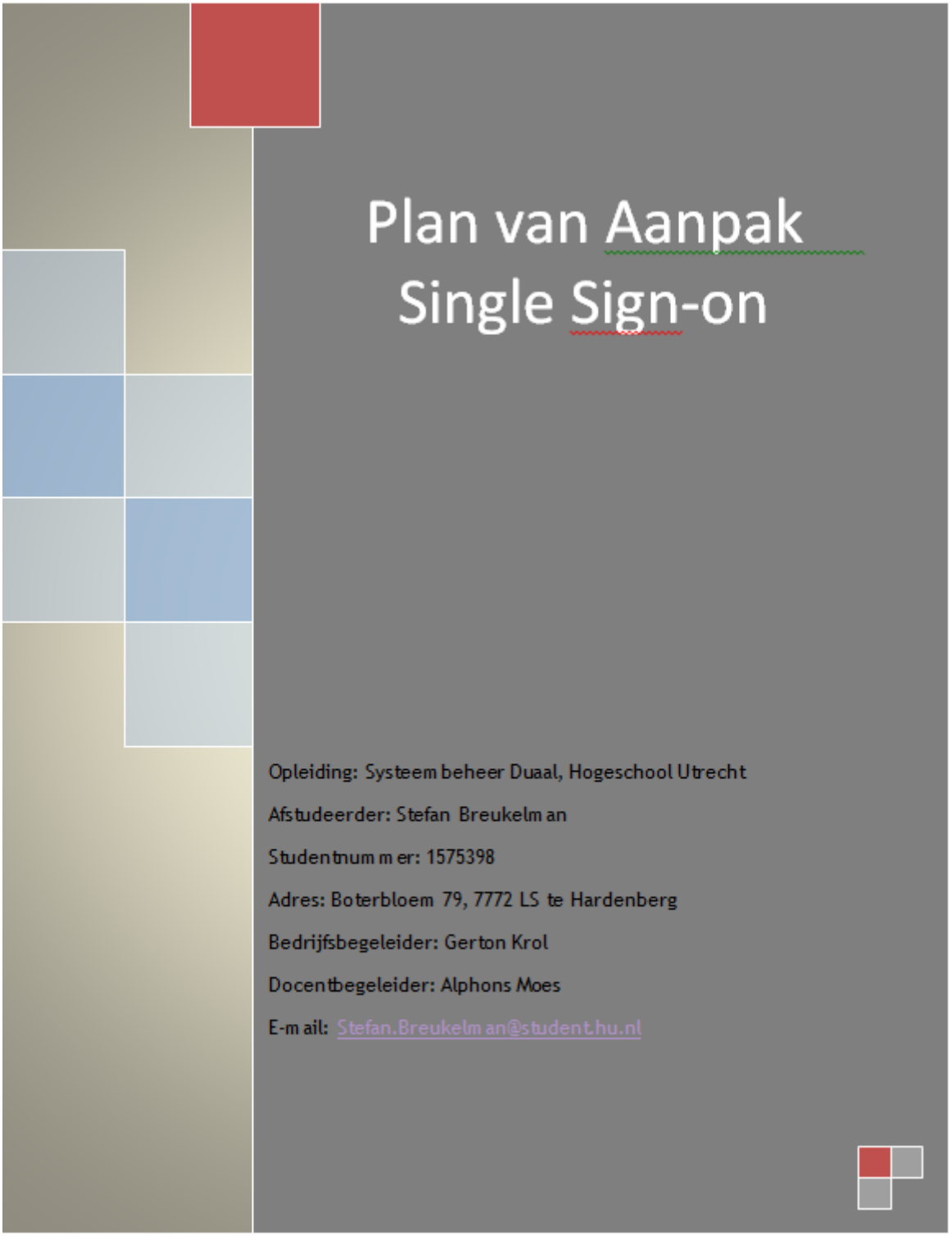
[20] BIG. Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (2014) https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-0506-Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.0.pdf

# 8 BIJLAGEN

Indeling:

Bijlage 1 bevat het Plan van Aanpak.
Bijlage 2 bevat de evaluatie.
Bijlage 3 bevat de huidige regels op gebied van security.

## 8.1 PLAN VAN AANPAK



## VERSIE BEHEER

| Datum | Persoon | Versie | Wijzigingen |
|---|---|---|---|
| **09-07-2014** | Stefan Breukelman | 1.0 | Eerste Opzet |
| **13-07-2014** | Stefan Breukelman | 1.1 | Verder uitgebreid |
| **27-07-2014** | Stefan Breukelman | 1.2 | Verder uitgebreid |
| 28-07-2014 | Stefan Breukelman | 1.3 | Verder uitgebreid |
| 30-07-2014 | Stefan Breukelman | 1.4 | Verder uitgebreid |
| 02-08-2014 | Stefan Breukelman | 1.5 | Versie 1.5 |
| 08-08-2014 | Stefan Breukelman | 1.6 | Aanpassing na feedback |
| 13-08-2014 | Stefan Breukelman | 1.7 | Aanpassing na feedback |
| 19-08-2014 | Stefan Breukelman | 1.8 | Aanpassing na feedback |

## DISTRIBUTIE BEHEER

| Datum | Persoon | Versie | Locatie | Vorm |
|---|---|---|---|---|
| **05-08-2014** | Docentbegeleider | 1.5 | Hogeschool Utrecht | Digitaal |
| **22-08-2014** | Docentbegeleider | 1.8 | Hogeschool Utrecht | Digitaal |
| | | | | |
| | | | | |
| | | | | |

# INHOUDSOPGAVE:

# INLEIDING

De Bestuursdienst Ommen-Hardenberg is voortgekomen uit een ambtelijke samenvoeging van de gemeente Hardenberg en de gemeente Ommen. Er wordt gebruik gemaakt van twee gemeentehuizen en er zijn een aantal buitenlocaties waaronder enkele zwembaden een lokaal opleidingscentrum en het theater.

Bij de Bestuursdienst Ommen-Hardenberg zijn 550 werkplekken aanwezig, waar 650 gebruikers zich op kunnen aanmelden. De desktop bestaat hoofdzakelijk uit een virtuele machine die met behulp van VDI gekoppeld wordt aan een thin-client en vervolgens aan de gebruiker wordt aangeboden.

Met deze afstudeeropdracht is het de bedoeling dat er een onderzoek plaats gaat vinden die de mogelijkheden van een Single Sign-on oplossing voor de Bestuursdienst Ommen-Hardenberg gaat uitzoeken.

# 1 AANLEIDING TOT ONDERZOEK

Binnen de Bestuursdienst Ommen-Hardenberg is er behoefte aan de implementatie van een Single Sign-On oplossing. Single Sign-on is een gebruikersauthenticatieproces welke ervoor zorgt dat de gebruiker slecht één keer zijn inloggegevens hoeft in te voeren om vervolgens toegang te krijgen tot meerdere systemen en applicaties. Het is dan voor de gebruiker niet meer nodig om verschillende inloggegevens te bewaren. Dit zal op termijn voor de gebruiker een tijdsbesparing opleveren.

De medewerkers maken gebruik van meerdere inloggegevens om diverse systemen te kunnen starten. Om de medewerkers te ontlasten is mij gevraagd om een project te starten waarin de mogelijkheden worden onderzocht om over te gaan naar een systeem dat kan voorzien in het éénmalig inloggen voor de gebruiker.

Met deze afstudeeropdracht is het de bedoeling dat de omgeving wordt uitgebreid met een Single Sign-on oplossing die wordt ontworpen en getest, waarbij de gebruiker geen hinder mag ondervinden tijdens de looptijd van het project

## 1.1 BETROKKENEN BIJ HET PROJECT

De projectorganisatie bestaat uit de volgende deelnemers:

| | | |
|---|---|---|
| Gerton Krol | Vakspecialist A ICT | Bedrijfsbegeleider |
| Alphons Moens | Docent Hogeschool Utrecht | Docentbegeleider |
| Stefan Breukelman | Netwerk/Systeembeheerder | Afstudeerder |

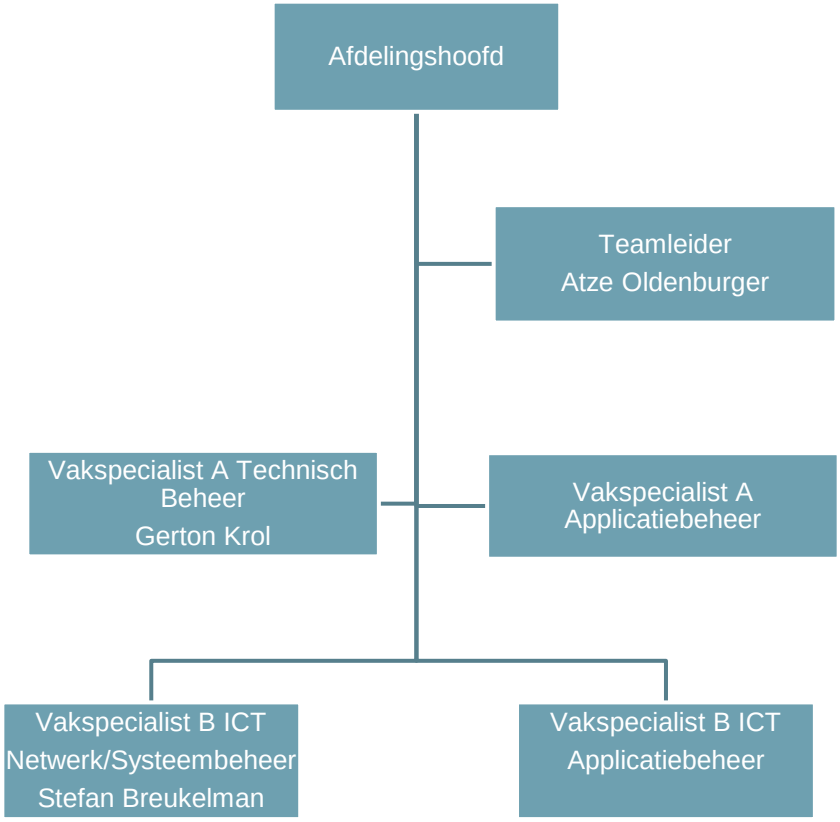
## 1.2 BEDRIJFSSITUATIE

De ICT afdeling bestaat uit 18 medewerkers die de organisatie adviseert bij ICT vraagstukken en dienstverlenend is in geval van calamiteiten. Daarnaast wordt er constant gekeken naar vernieuwingen en verbeteringen in de huidige infrastructuur.

De ICT afdeling bestaat uit de volgende functiegroepen:

- Vakspecialisten A
- Vakspecialisten B Applicatiebeheer
- Vakspecialisten B Netwerk/Systeembeheer

Organigram bedrijfspositie:




## 1.3 POSITIE STUDENT

In 2006 ben ik als netwerk/systeembeheerder gestart bij de gemeente Hardenberg en in 2012 ben ik overgegaan in de nieuwe organisatie de Bestuursdienst Ommen-Hardenberg. Mijn dagelijkse werkzaamheden bestaan uit het beheren van diverse servers, virtuele desktops, Databases van meerdere platforms en de netwerkapparatuur.

Deze werkzaamheden voer ik uit met meerdere collega's van het team netwerk/systeembeheer, in totaal zijn we binnen dit team met 6 medewerkers. Er is een onderverdeling qua expertise die voornamelijk door de jaren heen zo gegroeid is.

Het bijhouden van kennis wordt als een belangrijk aandachtpunt gezien binnen ons team, er zijn daarom ook voldoende mogelijkheden om ervoor te zorgen dat het kennisniveau op peil blijft.

# 2 DOELSTELLING EN PROBLEEMSTELLING

## 2.1 DEFINITIEVE DOELSTELLING

Het doel van mij onderzoek is om te komen tot een goede keuze voor een Single Sign-on functionaliteit die binnen de organisatie geïmplementeerd kan worden.
De aangeboden oplossing moet de mogelijkheid hebben om de belangrijkste applicaties in de virtuele omgeving van de Bestuursdienst Ommen-Hardenberg te benaderen via een enkele inlogprocedure.

Na het inloggen, moet het mogelijk zijn om de belangrijkste applicaties welke binnen de virtuele desktop omgeving worden aangeboden zeer snel via een Single Sign-on procedure te openen.
Het wachtwoord beheer moet gemakkelijk en overzichtelijk toegepast kunnen worden door meerdere collega's.

## 2.2 DEFENITIEVE PROBLEEMSTELLING

Binnen onze organisatie zijn er meerdere applicaties waarvoor de gebruiker een inlognaam en een wachtwoord nodig heeft om in te kunnen loggen.

Hier wordt vanuit dagelijks beheer veel tijd ingestoken. Gebruikers vergeten hun inloggegevens of voeren meerdere keren onjuiste informatie in.

Om ervoor te zorgen dat deze problemen structureel opgelost worden, is er gevraagd om de mogelijkheden van een Single Sign-on oplossing te onderzoeken

## 2.3 ONDERZOEKSVRAAG

Om de vragen die ontstaan tijdens de probleemomschrijving te kunnen beantwoorden heb ik onderstaande onderzoeksvraag opgesteld:

Op welke wijze kan het selecteren en implementeren van een Single Sign-on oplossing plaatsvinden, waarbij er ook rekening wordt gehouden met het bestaande ICT-beleid en de aanwezige ICT-architectuur?

### 2.3.1 DEELVRAGEN

12. Aan welke eisen moet het nieuwe systeem voldoen?
13. Wat is de haalbaarheid van een Single Sign-on oplossing?

14. Hoe kan de Single Sign-on oplossing in de bestaande ICT-architectuur geïmplementeerd worden?
15. Wat is de impact op de bestaande architectuur?
16. Welke oplossing past het beste bij de organisatie in samenwerking met het huidige ICT-beleid?
17. Wat zijn de risico's die verbonden zijn aan de implementatie van een Single Sign-on oplossing?
18. Op welke wijze kunnen de risico's beheersbaar blijven?
19. Welke rol speelt informatiebeveiliging in de huidige omgeving
20. Welke aanpassing moet er plaatsvinden op gebied van security?
21. Waarmee kan een Single Sign-on oplossing zich in de organisatie onderscheiden?
22. Wat zijn de voor- en nadelen voor de gebruikers?
23. Wat is de impact op de organisatie?

### 2.4 PROJECT GRENZEN

Het project heeft geen betrekking op andere lopende projecten en er hoeft om die reden geen afbakening plaats te vinden met andere projecten.

Het project wordt afgerond met een Proof of Concept welke door de opdrachtgever beoordeeld zal worden. De daadwerkelijke implementatie vindt niet plaats binnen de scope van de afstudeeropdracht. Daarnaast wordt er ook geen planning voor de daadwerkelijke uitrol vastgesteld. De reden hiervoor is de omvang die dit met zich mee brengt, deze is te omvangrijk om binnen dit project uit te voeren.

### 2.5 RANDVOORWAARDEN

De volgende randvoorwaarden zijn binnen dit afstudeerproject gedefinieerd:

- Beschikbaarheid bedrijfsbegeleider Gerton Krol
- Beschikbaarheid afstudeerbegeleider Alphons Moens
- Beschikbaarheid testomgeving voor Proof of Concept
- Beschikbaarheid collega's voor eventuele ondersteuning/expertise
- Beschikbaarheid student over ingeplande uren voor projectwerkzaamheden

## 3 OP TE LEVEREN PRODUCTEN

De onderstaande producten worden bij afronding van de afstudeeropdracht opgeleverd:

### 3.1 SCRIPTIE

- Onderzoek naar verschillende Single Sign on mogelijkheden
- Inventarisatie van bestaande systemen en belangrijkste applicaties
- Beschrijving bestaande Architectuur

- Inventarisatie van bestaande logins en key-users
- Uitkomsten referentiebezoeken
- Oplossingen uitwerken

### 3.2 ONTWERP

- Functioneel Ontwerp
- Technisch Ontwerp

### 3.3 PROOF OF CONCEPT

- Creëren testomgeving
- Opstellen testplannen
- Verwerken testplannen
- Evaluatie van Proof of Concept

### 3.4 VOORSTEL NA ONDERZOEK

- opstellen voorstel naar aanleiding van bevindingen.

## 4 UITVOERING

De uitvoering van het afstudeerproject wordt uitgevoerd in de onderstaande fases:

- Initiële Fase
- Onderzoeksfase
- Ontwerp Fase
- Test Fase
- Evaluatie Fase

### 4.1 INITIELE FASE

De eerste fase bevat activiteiten die uitgevoerd worden aan het begin van de afstudeeropdracht:

- Schrijven afstudeervoorstel
- Inleveren afstudeervoorstel bij de afstudeercommissie
- Goedkeuring ontvangen op afstudeervoorstel
- Schrijven Plan van Aanpak
- Inleveren Plan van Aanpak
- Ondertekenen van het afstudeercontract

#### 4.1.1 SCHRIJVEN AFSTUDEERVOORSTEL

Het schrijven van het afstudeervoorstel was de eerste opdracht die is uitgevoerd binnen dit project. Er staat in beschreven wat de opdracht is en dit wordt in het afstudeervoorstel nader toegelicht.

### 4.1.2 INLEVEREN AFSTUDEERVOORSTEL

Het afstudeervoorstel is ingeleverd bij de afstudeercommissie op 23-04-2014 via het digitale CRM webformulier. Na de verwerking van de feedback die ik van de afstudeercommissie heb ontvangen, is het voorstel ingeleverd op 26-05-2014

### 4.1.3 GOEDKEURING AFSTUDEERVOORSTEL

Op 27-05-2014 heb ik de goedkeuring op het afstudeervoorstel ontvangen van de afstudeercommissie.

### 4.1.4 SCHRIJVEN PLAN VAN AANPAK

In het Plan van Aanpak wordt de uitvoering van het project in stappen beschreven.

### 4.1.5 INLEVEREN PLAN VAN AANPAK

Het plan van Aanpak moet ingeleverd en goedgekeurd worden voor 22-08-2014

### 4.1.6 AFSTUDEERCONTRACT ONDERTEKENEN

Als de afstudeeropdracht en het Plan van Aanpak zijn goedgekeurd dan zal het afstudeercontract getekend moeten worden door de docentbegeleider, bedrijfsbegeleider en de student.

## 4.2 ONDERZOEK FASE

In deze fase vindt het onderzoek plaats, er wordt gekeken welke mogelijkheden van Single Sing-on er zijn en of die toegepast kunnen worden bij de Bestuursdienst Ommen-Hardenberg.

Het onderzoek wordt op verschillende manieren uitgevoerd:

Het lezen en vergelijken van literatuur over Single-Sign-on, het uitvoeren van referentiebezoeken bij soortgelijke organisaties als de Bestuursdienst en het toepassen van onderzoeksmethodes.

Vervolgens wordt er van deze fase een onderzoeksrapport geschreven die gelijktijdig met het onderzoek zal worden opgesteld.

### 4.3 ONTWERP FASE

De ontwerpfase bestaat uit meerdere activiteiten, die na aanleiding van het onderzoek plaats kunnen vinden.

Als eerste zal er een functioneel ontwerp geschreven worden, waarin een advies wordt geschreven hoe de omgeving er het beste uit kan komen te zien na aanleiding van de informatie die is verzameld in de onderzoeksfase.

Daarna zal er een technisch ontwerp gemaakt worden met daarin de technische aspecten die aan het functioneel ontwerp te grondslag liggen.

De ontwerpfase wordt afgerond met een voorstel dat aan de organisatie wordt opgeleverd, als hier goedkeuring op plaats vindt dan kan er begonnen worden met de testfase.

### 4.4 TEST FASE

In deze fase wordt er een testomgeving ( Proof of Concept) opgezet en deze zal door meerder collega’s getest moeten worden.

Eerst zal een testomgeving gecreëerd moeten worden die ontworpen wordt naar aanleiding van het functionele en technische ontwerp. Er moet een test plan geschreven worden die door de medewerkers gebruikt kan worden. De uitkomsten hiervan zullen in de scriptie worden beschreven.

### 4.4 EVALUATIE FASE

In de laatste fase vindt de evaluatie plaats, welke bestaat uit de volgende activiteiten:

- Schriftelijke beoordeling Bedrijfsbegeleider
- Inleveren schriftelijke beoordeling bedrijfsbegeleider aan Hogeschool Utrecht
- Voorbereiden afstudeerzitting
- Presentatie afstudeeropdracht

## 5 PLANNING

De planning is als een aparte bijlage toegevoegd aan dit document.

## 6 METHODEN EN TECHNIEKEN

### 6.1 METHODEN EN TECHNIEKEN

Het project wordt uitgevoerd binnen de huidige situatie. Een onderzoek is noodzakelijk om alle onderdelen goed in kaart te brengen. Het toepassen van de onderstaande onderzoeksmogelijkheden zal hieraan bijdragen.

### 6.1.1 MOSCOW METHODE

Door middel van de MoSCoW methode zal er een analyse worden uitgevoerd. Hier in worden de volgende vragen gesteld:

5. **Must have this?** *(Noodzakelijk, Is nodig om een werkend product op te kunnen leveren)*
6. **Should have this if at all possible?** *(Heeft een hoge prioriteit, maar niet noodzakelijk)*
7. **Could have this if it does not affect anything else?** (*Lage prioriteit, niet noodzakelijk)*
8. **Won't have this but would like to have this in the future?** *(Geen prioriteit, maar wellicht voor in de toekomst)*

Door het toepassen van de MoSCoW methode kan er prioriteit gegeven worden aan bepaalde eisen. Als de bovenstaande informatie wordt uitgewerkt dan kan er een beeld geschetst worden van de mogelijkheden conform te gestelde eisen.

### 6.1.2 REFERENTIEBEZOEKEN

Om te kijken hoe andere organisaties het traject van een Single Sign-on oplossing zijn doorlopen, ga ik gebruik maken van referentiebezoeken bij soortgelijke organisaties.

Welke problemen zijn deze organisaties tegen gekomen en welke oplossingen hebben ze doorgevoerd? Door vragen te stellen krijg ik goed inzichtelijk wat voor ons eventuele valkuilen kunnen zijn. Zij hebben immers al de nodige ervaring met Single Sign-on en kunnen aanbevelingen geven of daarentegen waarschuwen voor gevaren van een bepaalde keuze.

Om dit te realiseren ga ik korte vragenlijsten opstellen en deze versturen naar diverse andere gemeenten en overheidsinstanties. Daarnaast kunnen er nog referentiebezoeken plaatsvinden bij klanten van een leverancier, het is dan mogelijk om een werkende omgeving in de praktijk te bekijken, echter is dit minder onafhankelijk dan het zelf benaderen van organisaties. Een referentiebezoek bij klanten van de leverancier kan in sommige gevallen voor een vertekend beeld zorgen, immers zullen ze altijd een perfect werkende omgeving tonen.

Door deze methode toe te passen is het mogelijk om diverse pakketten van diverse leveranciers in de praktijk onder de loep te nemen en hiervan notities te maken. Deze kan ik verwerken en kunnen dan vervolgens meegenomen worden in de uiteindelijke keuze van een pakket en eventueel leverancier.

### 6.1.3 LITERAIR ONDERZOEK

Het uitvoeren van een literair onderzoek zorgt ervoor dat de kennis over het onderwerp uit diverse bronnen gehaald kan worden.

### 6.1.4 LONG LIST EN SHORT LIST SELECTIE

Om tot een eventuele pakketkeuze te komen ga ik gebruik maken van een long/short list selectie. Het uitvoeren van een selectie draagt bij aan het tot stand komen van een goede en weloverwogen keuze. Er zijn meerdere fases die doorlopen moeten worden om ervoor te zorgen dat er uiteindelijk een selectie gemaakt kan worden.

Deze fases worden hieronder beschreven:

**7.** Opstellen Longlist
- Mogelijke leveranciers en pakketten verzamelen.
- Lijst maken van leveranciers en pakketten.

**8.** RFI: Request for information
- Opvragen informatie diverse leveranciers.
- Longlist eventueel terugbrengen.
- Korte vragenlijst versturen.

**9.** RFP: Request for Proposal
- Uitgebreide vragenlijst versturen.
- Overzicht maken met informatie van elke leverancier en pakket.

**10.** Longlist reduceren to shortlist
- Vaststellen welke leveranciers het beste scoren op de gevraagde criteria.
- In kaart brengen welk product in samenwerking met de leverancier het beste bij de organisatie zou passen.
- Maken van shortlist en daarmee aantal leveranciers terugbrengen in aantal.

**11.** Proof of Concept
- Vragen om demonstratie van pakket.
- Opvragen van referenties en informatie.

**12.** Keuze leverancier en pakket
- Keuze maken voor pakket en leverancier op basis van reeds verworven informatie en goedgekeurde Proof of Concept.

# 7 CONTACT GEGEVENS

| Bestuursdienst Ommen-Hardenberg | |
|---|---|
| **Naam** | Bestuursdienst Ommen-Hardenberg |
| **Adres** | Stephanuspark 1 |
| **Postcode** | 7772 HZ |
| **Plaats** | Hardenberg |
| **Telefoonnummer** | T: 14-0523 |

| Bedrijfsbegeleider | |
|---|---|
| **Naam** | Gerton Krol |
| **Adres** | Stephanuspark 1 |
| **Postcode** | 7772 HZ |
| **Plaats** | Hardenberg |
| **Telefoonnummer** | T: 0523-289300 |
| **E-mail adres** | Gerton.krol@ommen-hardenberg.nl |

| Student | |
|---|---|
| **Naam** | Stefan Breukelman |
| **Adres** | Stephanuspark 1 |
| **Postcode** | 7772 HZ |
| **Plaats** | Hardenberg |
| **Telefoonnummer** | T:0523-289222  M:06-83001437 |
| **E-mail adres** | |

# 8 BIJLAGEN

## 8.1 BRONVERMELDING

| Bronvermelding: | |
|---|---|
| **Bron:** | Boek |
| **Adres:** | -- |
| **Titel:** | Zo doe je een onderzoek |
| **Geschreven door:** | Roel Grit, Mark Julsing |
| **Geraadpleegd op:** | -- |

| Bronvermelding: | |
|---|---|
| **Bron:** | Website |
| **Adres:** | http://www.zbc.nu/ict/projectmanagement-ict/methode-en-checklist-pakketselectie-en-implementatie-deel-1/ |
| **Titel:** | Methode en checklist pakketselectie en -implementatie |
| **Geschreven door:** | **Wiebe Zijlstra** |
| **Geraadpleegd op:** | 24-05-2014 |

| Bronvermelding: | |
|---|---|
| **Bron:** | Website |
| **Adres:** | http://www.voorbeeldvinden.nl/swot-analyse-voorbeeld/ |
| **Titel:** | SWOT analyse voorbeeld |
| **Geschreven door:** | **Thijs Verbeek** |
| **Geraadpleegd op:** | 25-05-2014 |

## 8.2 AFSTUDEERCONTRACT

HOGESCHOOL UTRECHT

**Contract afstudeeropdracht**
**Instituut voor ICT**
**Nijenoord 1, 3552 AS, UTRECHT**

**NB: Dit contract dient te worden opgenomen als vast onderdeel van het plan van aanpak**

Datum: 07-08-2014

---

Naam student: Stefan Breukelman

Opleiding: Systeembeheer Duaal

Variant: duaal

Adres student: Boterbloem 79

Postcode / Woonplaats student: Hardenberg

Studentnummer: 1575398

Telefoonnummer privé: 0683001437

E-mailadres: stefan.breukelman@student.hu.nl

---

Naam bedrijf (afstuderen): Bestuursdienst Ommen-Hardenberg

Adres bedrijf: Stephanuspark 1

Postcode / Woonplaats bedrijf: 7772 HZ Hardenberg

Naam bedrijfsbegeleider: Gerton Krol

Telefoonnummer bedrijfsbegeleider: 0523-289300

E-mailadres bedrijfsbegeleider: gerton.krol@ommen-hardenberg.nl

---

Beoogde datum van afstuderen: *Periode 1 26-05-2014 t/m 14-10-2014*

Geheimhouding geaccordeerd door HU op: *indien van toepassing*

---

***Ondergetekenden verklaren hiermee akkoord te gaan met de inhoud van bijgesloten PvA.***

Handtekeningen

Student :

Docentbegeleider :

Bedrijfsbegeleider[1] :

---

[1] **Door ondertekening van dit formulier verklaart de bedrijfsbegeleider minimaal een hbo- of vergelijkbare opleiding te hebben.**

| Taaknaam | Duur | Begindatum | Einddatum | % volt. |
|---|---|---|---|---|
| **Planning Afstudeeropdracht Single Sign-on** | **209 dagen** | **01-04-2014** | **nov. 2014** | **5%** |
| **1: Initiatieffase** | | | | 50% |
| Start afstudeervoorstel | 22 dagen | 01-04-2014 | 22-04-2014 | 100% |
| Inleveren afstudeervoorstel | 1 dag | 23-04-2014 | 23-04-2014 | 100% |
| Wachten op goedkeuring en eventuele aanpassingen | 33 dagen | 23-04-2014 | 26-05-2014 | 100% |
| Schrijven Plan van Aanpak | 28 dagen | 26-05-2014 | 22-08-2014 | 0% |
| Inleveren Plan van Aanpak | 1 dag | 09-07-2014 | 22-08-2014 | 0% |
| Tekenen afstudeercontract | 1 dag | 26-05-2014 | aug. 2014 | 0% |
| **2: Onderzoeksfase** | | | | |
| Uitvoeren onderzoek | 20 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Analyse huidige situatie | 10 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Referentiebezoeken | 5 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Long list/Short list | 5 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| **3: Ontwerpfase** | | | | 0% |
| Functioneel ontwerp beschrijven | 5 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Technisch ontwerp schrijven | 5 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Voorstel nieuwe omgeving schrijven | 5 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Voorstel bespreken met bedrijf | 1 dag | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| **4: Testfase** | | | | 0% |
| Bouwen testsituatie | 3 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Omgeving testen | 5 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Proof of Concept | 5 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| Testplan uitwerken | 3 dagen | Jul/aug/sept 2014 | Jul/aug/sept 2014 | 0% |
| **5: Evaluatiefase** | | | | 0% |
| Scriptie uitwerken | 20 dagen | sept 2014 | half okt. 2014 | 0% |
| Scriptie controleren op taal en spelling | 2 dagen | sept 2014 | half okt. 2014 | 0% |
| Scriptie inleveren | 1 dag | sept 2014 | half okt. 2014 | 0% |
| Evaluatie | 3 dagen | sept 2014 | half okt. 2014 | 0% |
| Schriftelijke beoordeling werkgever | 6 dagen | sept 2014 | half okt. 2014 | 0% |
| Inleveren schriftelijke beoordeling werkgever | 1 dag | sept 2014 | half okt. 2014 | 0% |
| Afstudeerpresentatie voorbereiden | 8 dagen | sept 2014 | half okt. 2014 | 0% |
| Afstudeerzitting | 10 dagen | sept 2014 | nov. 2014 | 0% |

## 8.2 EVALUATIE

In dit hoofdstuk evalueer ik de uitvoering van het afstudeerproject Single Sign-on.

De afstudeeropdracht heeft voor mij gebracht wat ik van te voren als doel gesteld had, namelijk het onderzoeken van de mogelijkheden voor een Single Sign-on oplossing voor de Bestuursdienst Ommen-Hardenberg. Het Plan van Aanpak is een goede leidraad geweest, omdat ik hiermee inzichtelijk had hoe ik de afstudeeropdracht in goede banen kon leiden en welke methodes ik kon gebruiken. Daarnaast heeft het PVA geholpen om het onderzoek uit te voeren, mede door de onderzoeksvragen die in het PVA opgesteld waren.

Het is jammer dat ik de uiteindelijke oplossing niet in een Proof of Concept heb kunnen tonen aan de organisatie tijdens mijn afstudeerperiode. Ik denk dat ik daar nog veel van had kunnen leren, maar gelukkig gaat dat in de nabije toekomst wel gebeuren.

Het vinden van informatie over het onderwerp Single Sign-on was niet moeilijk, echter was het wel lastig om deze informatie op een goede manier te gebruiken. Veel bronnen vertelden hetzelfde, na een bepaalde periode tijdens het onderzoek was ik beter in staat om te zoeken naar informatie die specifieker was. Dat heeft uiteindelijk ook bijgedragen aan een vergroting van mijn kennis

Alles bij elkaar genomen ben ik tevreden met de uitvoering van mijn afstudeeropdracht. De begeleiding die ik heb ontvangen was goed en mijn kennisniveau op het gebied van Single Sign-on is aanzienlijk gestegen en ik verwacht deze ook in de praktijk toe te kunnen passen in de toekomst.

## 8.3 HUIDIGE REGELS OP GEBIED VAN SECURITY

***Beleid op gebied van gebruikers:***

- Gebruikers worden bij de Bestuursdienst Ommen-Hardenberg bij het aanmaken vooraf geïdentificeerd door teamleider. Deze plaatst ook het verzoek bij het Interne Service Punt (ISP) voor het aanmaken van een account door middel van een ingevuld formulier, voorzien van een handtekening.
- Gebruikers worden op functieniveau ingedeeld en aan deze functiegroepen worden de bevoegdheden uitgedeeld.
- Gebruikers krijgen alleen toegang tot de applicaties die noodzakelijk zijn voor het uitvoeren van de werkzaamheden die bij zijn/haar functie horen.
- Wanneer een gebruiker van functie veranderd moet er rekening gehouden worden met wijziging van toegangsrechten.
- Iedere gebruiker ontvangt een unieke inlognaam, welke alleen bedoeld is voor persoonlijk gebruik.

***Beleid op gebied van wachtwoorden:***

- Initiële wachtwoorden worden alleen aan de teamleider verstrekt, nadat dit gecommuniceerd is met een nieuwe gebruiker dient het wachtwoord gewijzigd te worden.
- Het gebruik van applicaties binnen het netwerk van de Bestuursdienst dienen minimaal voorzien te zijn van een authenticatie.
- Elke 90 dagen moet het wachtwoord aangepast worden.
- Wanneer het wachtwoord verlopen is dan wordt het account geblokkeerd.
- Het wachtwoord mag geen aanzienlijk gedeelte van de accountnaam of de volledige naam van de gebruiker bevatten.
- De lengte moet minimaal acht tekens zijn.
- Het wachtwoord mag niet gelijk zijn aan de laatste zes wachtwoorden.
- Het wachtwoord moet tekens uit drie van de volgende categorieën bevatten:
    - Hoofdletters (A tot en met Z)
    - Kleine letters (a tot en met z)
    - Cijfers uit het tientallig getallenstelsel (0 tot en met 9)
    - Niet-alfanumerieke tekens (zoals, !, $, #, %)
    - Voorbeeld fout : Jansen01 - Voorbeeld goed : Kih3oZ!@
- Er wordt automatisch gecontroleerd of het wachtwoord voldoet aan de gestelde criteria.
- Wanneer er 3 keer verkeerd wordt ingelogd door het ingeven van een foutief wachtwoord, dan moet het account geblokkeerd worden.

- Het verzoek tot opheffen van de blokkade kan alleen door de gebruiker zelf worden ingediend.
- Het wachtwoord dient na een reset de eerste keer gelijk weer gewijzigd te worden.
- Wachtwoord dient direct gewijzigd te worden door ICT, wanneer het vermoeden bestaat dat deze bekend is geworden bij een derde partij.

***Beleid op het gebied van gebruik werkplek:***

- Bij het afdrukken van gevoelige informatie dient gebruik te worden gemaakt van beveiligd afdrukken ( printen naar mailbox).
- Medewerkers laten bij het verlaten van de werkplek geen gevoelige of vertrouwelijke informatie onbeheerd achter. Dit dient in de locker opgeslagen te worden.
- Bij het verlaten van de werkplek moet deze vergrendeld worden.
- Na een periode van inactiviteit op de werkplek ( 15 min.) wordt er een lock op de desktop toegepast.