



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

DWR 2 Directory concept

Versie 0.5

Datum	10 augustus 2009
Status	Concept

Samenvatting

Het Programma DWR heeft de opdracht van DG-OBR aanvaard om de Digitale Werkomgeving Rijksdienst (DWR) te ontwikkelen. De door DWR ontwikkelde diensten voorzien in de behoefte van departementen aan een uniforme, toekomstgerichte digitale werkomgeving.

Het programma DWR ontwikkelt DWR 2 Architectuur met specifieke kenmerken die in het document beschreven worden. De DWR 2 Architectuur kent volgende deelgebieden:

- Werkplek en werkplek applicaties en services
- Netwerk en netwerk services
- Portaal en web-enabled applicaties (email, samenwerkfunctionaliteit, zoek en vind etc)
- Content management
- Security (directories, IAAA, dreiging en kwetsbaarheid management)

Dit document beschrijft de DWR 2 directory architectuur dat onderdeel uitmaakt van het deelgebied Security. Het document richt zich op de IT architecten en technisch specialisten van de Rijksoverheid.

De opdracht voor de DWR 2 directory architectuur luidt: ontwerp een directory architectuur die het beheer van elektronische objecten optimaliseert en waarvan DWR applicaties gebruik kunnen maken. Dit dient bij voorkeur gerealiseerd te worden met behulp van open source software en de open standaard LDAP te ondersteunen.

Het directory architectuur ontwerp beschrijft: de DWR diensten die gebruik kunnen maken van de directory, de processen die de objecten met bijbehorende gegevens leveren en het DWR 2 directory concept. Buiten de reikwijdte van de opdracht valt het exact vaststellen van de gegevens in de directory met bijbehorende formaat en toegangsrechten. Dit vindt plaats in een apart project.

Deze architectuur is gebaseerd op de eisen die aan de directory service worden gesteld (zie paragraaf 2.3) en dient als input voor het technisch ontwerp.

Na een beschrijving van de DWR diensten die gebruik kunnen maken van de directory en de processen die gegevens leveren wordt de directory nader belicht. De definitie voor directory zoals die in het document wordt gehanteerd luidt als volgt: Een directory is een gegevensopslagfaciliteit waarin objecten, in een hiërarchisch model, worden vastgelegd. Het directory schema beschrijft het formaat waarin deze objecten worden vastgelegd inclusief hun bijbehorende attributen.

De hiërarchische database maakt gebruik van een naming context/suffix. Een LDAP naming context is de naam (distinguished name) van het startpunt in de directory hiërarchie. Voor de notatie van de LDAP naming context worden twee vormen veelvuldig gebruikt. Dit zijn een LDAP naming context gebaseerd op: Originele X500 stijl en Domain naming stijl. In de DWR 2 LDAP directory infrastructuur wordt gebruik gemaakt van een LDAP naming context gebaseerd op de domain naming stijl. Deze stijl wordt momenteel gebruikt in de DWR 1 infrastructuur. De exacte naamgeving zal plaats vinden tijdens het technisch ontwerp van de directory infrastructuur.

De gegevens in de directory kunnen worden benaderd op basis van de protocollen LDAP en DSML. Uit performance overwegingen wordt voor communicatie met de directory in de DWR 2 infrastructuur hoofdzakelijk gebruik gemaakt van het LDAP protocol. Voordat toegang kan worden verleend tot gegevens in de directory moet eerst verbinding worden gemaakt met de directory. Op dat moment kan authenticatie plaats vinden op de volgende drie manieren:

1. Geen authenticatie
2. Basic authenticatie
3. Secure authenticatie

De directory in de DWR infrastructuur biedt authenticatie mogelijkheden op basis van alle drie de bovenstaande manieren. Welke authenticatie manier wordt geïmplementeerd zal afhangen van het geëiste beveiligingsniveau van de gegevens. Op het moment dat de gegevens daadwerkelijk gebruikt (lezen, schrijven, wijzigen) worden vindt een autorisatie proces plaats. Het LDAP versie 3 protocol biedt geen autorisatie mogelijkheden. Het gevolg is dat elke directory implementatie zijn eigen "access control list" implementatie hanteert.

Tot op dit moment is gesproken over directory maar de literatuur kent de volgende drie typen directories met ieder zijn specifieke kenmerken:

1. *De virtuele directory*: De virtuele directory zal in de DWR 2 directory infrastructuur een centrale rol innemen en treedt naar de departementen op als het directory contactpunt.
2. *De metadirectory*: De metadirectory vervult in de DWR 2 directory infrastructuur een centrale rol in het authenticatie proces, in de opslag van DWR (generiek/applicatie specifiek) objecten en in het beheer van deze objecten. De metadirectory treedt naar de DWR applicaties op als centraal contactpunt/opslagfaciliteit.
3. *De applicatie specifieke directory*: Een applicatie specifieke directory treedt voor één specifieke applicatie op als opslagfaciliteit. Het gebruik van een applicatie specifieke directory wordt in de DWR 2 infrastructuur tot een minimum beperkt.

Omdat de directory van cruciaal belang is voor de DWR dienstverlening vereist deze een hoge mate van beschikbaarheid en performance. Dit wordt gerealiseerd met behulp van een zogenaamde gedistribueerde directory en de technieken replicatie en partitioneren. gedistribueerde directory bestaat uit meerdere databases op verscheidene fysieke servers. Deze verscheidene databases kunnen dezelfde gegevens bevatten (replicatie) of verschillende gegevens (partitioneren). Om de negatieve gevolgen van partitionering te minimaliseren, wordt van deze techniek in beperkte mate gebruik gemaakt.

Om de verscheidene partities als één directory te laten opereren worden deze met elkaar verbonden. Dit verbinden kan met behulp van referrals en met behulp van chaining. In de DWR 2 directory infrastructuur is gekozen om de verscheidene partities onderling te verbinden met behulp van chaining. De reden hiervoor is dat niet alle client applicaties referrals ondersteunen.

Bij replicatie zijn dezelfde directory gegevens op verscheidene servers aanwezig. Replicatie kan plaats vinden op basis van de single master techniek en de multi master techniek

Met de huidig beschikbare kennis kiest DWR voor het replicatie model single master. De reden hiervoor zijn:

1. De single master replicatie techniek heeft een substantieel kleinere kans op replicatie fouten dan de multi master replicatie techniek.
2. Probleem analyse is eenvoudiger in een single master replicatie omgeving dan in een multi master replicatie omgeving.
3. Een beperkte spreiding (Nederland) van locaties waar directory servers worden geplaatst. Deze locaties zijn tevens doormiddel van snelle verbindingen (lage roundtrip delay time) met ruim voldoende beschikbare bandbreedte met elkaar verbonden.

Het vaststellen van de definitieve directory replicatie techniek vereist een nader onderzoek. In dit onderzoek moet vastgesteld worden of de gewenste performance gerealiseerd kan worden met de single master techniek in combinatie met het aantal te verwachten schrijf acties (inclusief bijbehorend volume) in de DWR 2 directory infrastructuur.

In hoofdstuk 5 en 6 wordt de DWR 2 technische directory architectuur beschreven met de bijbehorende open source software. Met behulp van deze open source software wordt een Proof of Concept gerealiseerd.

Inhoudsopgave

Samenvatting	2	
1	Introductie	6
1.1	Doelgroep	6
1.2	Doelstelling document	6
1.3	Huidige Situatie	6
1.4	Leeswijzer	6
1.5	Versiebeheer	6
1.6	Referenties	6
2	Inleiding	7
2.1	Positionering	7
2.2	Opdracht	7
2.2.1	Reikwijdte opdracht	7
2.2.2	Opdrachtdoelstelling	8
2.3	Eisen directory service	8
3	Directory diensten	10
3.1	Aanleiding	10
3.2	DWR IT diensten	11
4	Directory	13
4.1	Directory ten opzichte van relationele database	13
4.2	LDAP naming context	13
4.3	Communicatieprotocol	14
4.4	Authenticatie	14
4.5	Autorisatie	15
4.6	Gegevensleverancier	15
4.7	Type directories	15
4.8	Topologie	16
4.8.1	Partitioneren	16
4.8.2	Referrals en chaining	17
4.8.3	Replicatie model	17
5	DWR 2 technische directory architectuur	19
5.1	Implementatie virtuele directory	19
5.2	Implementatie metadirectory	20
5.3	Implementatie applicatie specifieke directory	20
6	Mogelijke software	21
6.1	Virtuele directory	21
6.2	Metadirectory	21
6.3	Applicatie specifieke directory	21
Bijlage I	22	

1 Introductie

1.1 Doelgroep

IT architecten en technisch specialisten van de Rijksoverheid.

1.2 Doelstelling document

Beschrijving van de technische architectuur DWR 2 directory die als input dient voor het technisch ontwerp. Deze is daar waar mogelijk gebaseerd op open source software en is toegankelijk met behulp van open standaarden.

1.3 Huidige Situatie

De DWR infrastructuur maakt gebruik van meerder directories van verscheidene leveranciers (Siemens, Microsoft, ...). De DWR directory infrastructuur is beschreven in het document DWR Directory Services (DDS, auteur Wim Zeeff), inclusief hun samenhang.

1.4 Leeswijzer

Het document beschrijft de functie van de directory in zijn algemeen en de specifieke keuzes die de DWR dient te maken. Elke te maken keuze wordt door de schrijver voorzien van een onderbouwing.

1.5 Versiebeheer

Versie	Datum	Steller	Opmerkingen
0.1	15-06-09	J. Mol	
0.2	22-06-09	J. Mol	Verwerkt commentaar J. Vytupil
0.3	24-06-09	J. Mol	Verwerkt commentaar J.A. ten Cate en W. Kramer
0.4	08-07-09	J. Mol	Verwerkt commentaar L. van der Zalm
0.5	10-08-09	J. Mol	Verwerkt commentaar DWR en WIT architecten

Tabel 1-1: Versies van dit document

1.6 Referenties

Referte	Document
	DWR Directory Service, auteur Wim Zeeff

Tabel 1-2: Literatuur waaraan in dit document wordt gerefereerd

2 Inleiding

Het Programma DWR heeft de opdracht van DG-OBR aanvaard om de Digitale Werkomgeving Rijksdienst (DWR) te ontwikkelen. De door DWR ontwikkelde diensten voorzien in de behoefte van departementen aan een uniforme, toekomstgerichte digitale werkomgeving.

Het programma DWR ontwikkelt DWR 2 Architectuur die getypeerd wordt door het bieden van:

1. voorzieningen die gebaseerd zijn op Open Source producten en open standaarden, in het bijzonder een Open Source gebaseerde Desktop
2. nieuwe interdepartementale voorzieningen zoals Rijks e-mail, samenwerkfunctionaliteit, content management
3. een multilevel/multisecure beveiliging
4. voorzieningen voor het consolideren van (distributie en beheer) van departementale applicaties, die ingezet worden voor de realisatie van nieuwe producten en diensten.

DWR 2 Architectuur kent volgende deelgebieden:

- Werkplek en werkplek applicaties en services
- Netwerk en netwerk services
- Portaal en web-enabled applicaties (email, samenwerkfunctionaliteit, zoek en vind etc)
- Content management
- Security (directories, IAA, dreiging en kwetsbaarheid management)

Dit document beschrijft het DWR 2 directory concept.

De directory vervult de rol van gegevensopslagfaciliteit en is binnen de DWR IT infrastructuur van cruciaal belang voor de dienstverlening van DWR. Deze directory vormt samen met de bijbehorende diensten (zie paragraaf 3.2) de directory service.

2.1 Positionering

Verscheidene DWR diensten zullen gebruik gaan maken van de DWR 2 directory. Deze directory wordt in eerste instantie naast de aanwezige directories geplaatst. Op termijn wordt de DWR 2 directory de leidende directory in de DWR dienstverlening.

2.2 Opdracht

Ontwerp een directory concept voor DWR die het beheer van elektronische objecten optimaliseert en waarvan DWR applicaties gebruik kunnen maken. Dit dient bij voorkeur gerealiseerd te worden met behulp van open source software en de open standaard LDAP te ondersteunen.

2.2.1 Reikwijdte opdracht

Het DWR 2 directory concept beschrijft: de DWR diensten die gebruik kunnen maken van de directory, de processen die de objecten met bijbehorende gegevens leveren en het DWR 2 directory concept. Buiten de reikwijdte van de opdracht valt het exact vaststellen van het directory gegevensmodel met bijbehorend formaat en toegangsrechten. Dit zal plaats vinden in een separaat project.

2.2.2 *Opdrachtdoelstelling*

Realisatie van een directory concept dat voldoet aan de gestelde opdracht met bijbehorende eisen. De architectuur dient als uitgangspunt voor het technisch ontwerp van de DWR directory.

2.3 **Eisen directory service**

1. **Architectuur:** het DWR 2 directory concept is gebaseerd op de architectuur principes zoals deze zijn beschreven in bijlage I.
2. **Beveiliging:** het DWR 2 directory concept geeft invulling aan het tactisch normenkader DWR en de bijbehorende operationele maatregelen.
3. **Organisatie:** de onderstaande organisatiestructuur wordt gehanteerd voor de DWR 2 directory service:

- **Beheerorganisatie:** verzorgt generiek (technisch) beheer van DWR 2 directory;
- **Departement:** afnemer van DWR 2 directory, treedt tevens op als gegevensleverancier;
- **DWR:** leverancier van de DWR 2 directory en tevens afnemer.

4. **Daar waar mogelijk, maakt de DWR 2 directory gebruik van open source software.**

De definitie van open source software die DWR hanteert is gebaseerd op de definitie uit het actieplan "Nederland Open in Verbinding" en luidt:

Open source software is software met twee kenmerken:

- a. De broncode van de software is vrij beschikbaar;
- b. In het licentiemodel is het intellectueel eigendom en het (her)gebruik van de software en bijbehorende broncode dusdanig geregeld dat de licentienemer de broncode mag inzien, gebruiken, verbeteren, aanvullen en distribueren.
- c. Een open source licentie dwingt af dat de broncode van het product en soms ook de aanpassingen daarop, vrij beschikbaar moet zijn.

5. **De DWR 2 directory maakt gebruik van de open standaard LDAP.**

De definitie van open standaard die DWR hanteert is gebaseerd op de definitie uit het actieplan "Nederland Open in Verbinding".

Onder een 'open standaard' wordt een standaard verstaan die voldoet aan de volgende eisen:

- a) De standaard is goedgekeurd en zal worden gehandhaafd door een not-for-profit organisatie, en de lopende ontwikkeling gebeurt op basis van

een open besluitvormingsprocedure die toegankelijk is voor alle belanghebbende partijen (consensus of meerderheidsbeschikking enz.);

- b) De standaard is gepubliceerd en over het specificatie document van de standaard kan vrijelijk worden beschikt of het is te verkrijgen tegen een nominale bijdrage. Het moet voor een ieder mogelijk zijn om het te kopiëren, beschikbaar te stellen en te gebruiken om niet of tegen een nominale prijs;
 - c) Het intellectuele eigendom - m.b.t. mogelijk aanwezige patenten - van (delen van) de standaard is onherroepelijk ter beschikking gesteld op een royalty-free basis;
 - d) Er zijn geen beperkingen omtrent het hergebruik van de standaard.
6. **Licentie overeenkomst**, de benodigde software voor de implementatie van de DWR 2 directory committeert zich aan de European Union Public Licence (EURL v 1.0) en/of GNU General Public License (GPL v 2) licentie overeenkomst of gelijkwaardig.
7. **Authenticatie**, op basis van de volgende authenticatie mechanisme vindt autorisatie plaats m.b.t. gegevens die in de DWR 2 directory zijn opgeslagen:
- a) **Basic authenticatie**, op basis van gebruikersnaam en wachtwoord wordt toegang verkregen tot de gegevens waartoe de gebruiker gemachtigd is;
 - b) **Kerberos**, op basis van een Kerberos ticket wordt toegang verkregen tot de gegevens waartoe de gebruiker gemachtigd is;
 - c) **X509 certificaat**, op basis van een persoonsgebonden X509 certificaat wordt toegang verkregen tot de gegevens waartoe de gebruiker gemachtigd is.

3 Directory diensten

3.1 Aanleiding

De DWR IT infrastructuur bestaat uit vele objecten. Gegevens met betrekking tot deze objecten worden momenteel in meerdere systemen opgeslagen. Voorbeelden van dergelijke systemen zijn: CMDB, locatieregistratiesysteem, personeelsregistratiesysteem, etc. Het resultaat van deze configuratie is dat dezelfde gegevens op meerdere plaatsen zijn vastgelegd en dat deze gegevens op meerdere plaatsen worden onderhouden. DWR heeft onderkend dat een dergelijke configuratie niet wenselijk is, ondermeer uit het oogpunt van beheerefficiëntie, gegevens integriteit, auditing en kosten. Het DWR 2 architectuurproject Directory service geeft mede invulling aan de optimalisatie van de geconstateerde onvolkomenheden in de huidige configuratie met betrekking tot de opslag/beheer van de objectgegevens.

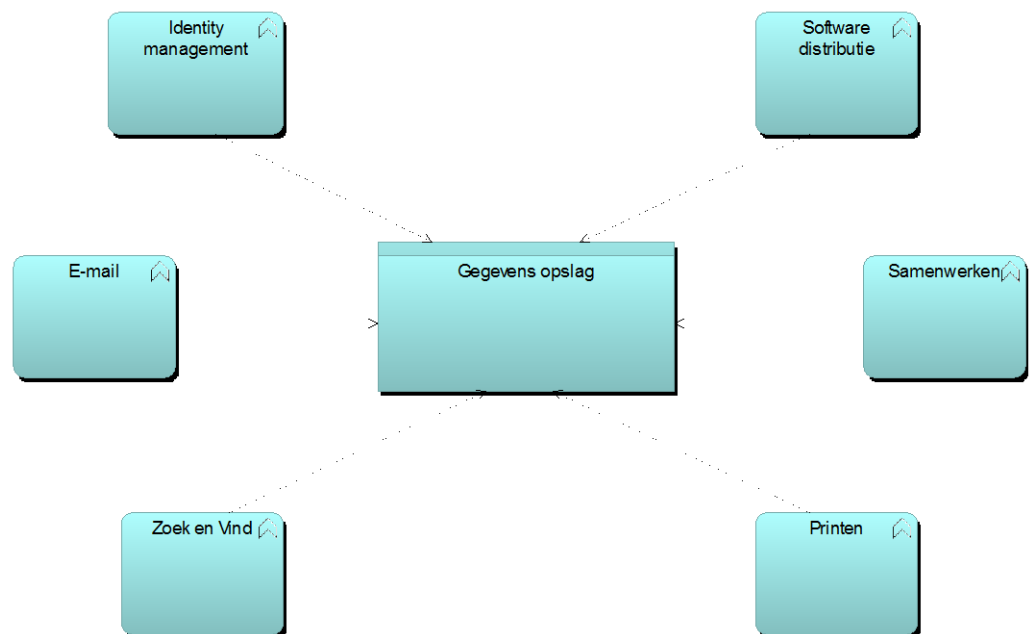
Deze objectgegevens zijn te verdelen in twee groepen:

1. **generiek**, objectgegevens die door meerdere applicaties worden gebruikt. Dit zijn voornamelijk identiteit gerelateerde gegevens bijvoorbeeld gegevens die betrekking hebben op identiteitobjecten als: gebruikers, computers, printers, etc.
2. **applicatie specifiek**, objectgegevens die door een specifieke applicatie worden gebruikt. Dit zijn objectgegevens die benodigd zijn voor een specifieke applicatie. De applicatie levert door middel van een directory schemawijziging het formaat waarin deze specifieke objectgegevens worden vastgelegd. De schemawijziging kan attributen toevoegen aan bestaande (identiteit)objecten en/of nieuwe objecten creëren.

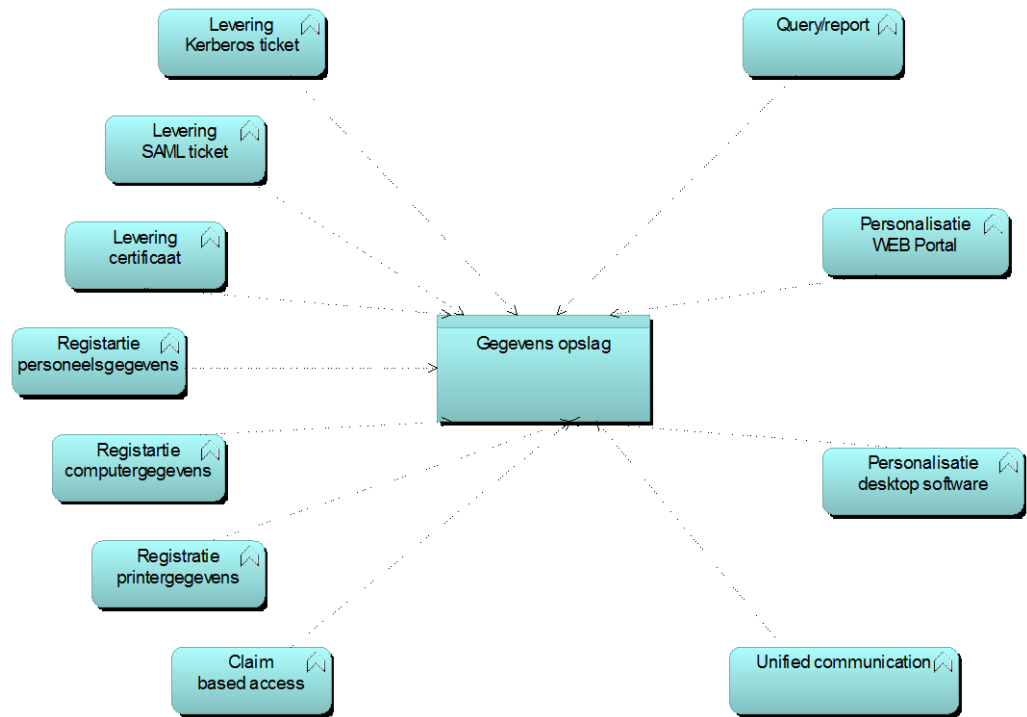
Om te bepalen welke objectgegevens gemeenschappelijk worden gebruikt, dienen allereerst de DWR IT diensten in kaart te worden gebracht.

3.2 DWR IT diensten

De voornaamste leverancier van generieke objectgegevens is de identity management dienst. Deze dienst levert gegevens gerelateerd aan objecten als: gebruikers, computers, printers en groepen. Andere diensten leveren hoofdzakelijk applicatie specifieke objectgegevens. Dergelijke gegevens worden merendeels vastgelegd in attributen van generieke objecten. De onderstaande afbeelding is een overzicht van de DWR diensten die gebruik maken van c.q. leveren van gegevens.



Deze DWR diensten bestaan uit de diverse processen. De onderstaande afbeelding is een overzicht van DWR processen die gebruik maken (leveren/raadplegen) van gegevens.



Uit de afbeelding valt af te leiden dat de centrale gegevensopslag een cruciale rol vervult in het authenticatie proces, het autorisatie proces en de opslag van applicatie specifieke configuratie gegevens.

Tevens toont de afbeelding dat een centrale gegevensopslagfaciliteit benodigd is voor het oplossen van de in paragraaf 3.1 geconstateerde onvolkomenheden van de huidige situatie.

4 Directory

In hoofdstuk 2 is vastgesteld dat een directory een gegevensopslagfaciliteit is. In dit hoofdstuk wordt nader ingegaan op de directory. Allereerst wordt de exacte definitie vastgesteld. Deze luidt als volgt:

Een directory is een gegevensopslagfaciliteit waarin objecten, in een hiërarchisch model, worden vastgelegd. Het directory schema beschrijft het formaat waarin deze objecten worden vastgelegd inclusief hun bijbehorende attributen.

Uit de definitie kan geconcludeerd worden dat een directory een type database is. De directory heeft specifieke eigenschappen ten opzichte van een relationele database.

4.1 Directory ten opzichte van relationele database

De belangrijkste specifieke eigenschappen van de directory zijn:

1. Hoofdzakelijk vinden lees en zoek acties plaats. Schrijf acties vinden in beperkte mate plaats. De directory is niet geschikt voor gegevens die vaak en snel wijzigen;
2. De gegevens die de database bevat zijn relatief statisch waardoor de database geoptimaliseerd is voor lees en zoek acties;
3. De directory ondersteunt geen ACID-compliant transacties in tegenstelling tot een relationele database.
4. Toegang tot gegevens in een directory vindt plaats op basis van de open standaard LDAP of DSML. Toegang tot gegevens in een relationele database vindt plaats op basis van Structured Query Language (SQL).

Bij de bovenstaande eigenschappen 1 en 3 moet aangemerkt worden dat deze niet gelden voor de moderne directory implementaties van bijvoorbeeld OpenLDAP, SUN Java System Directory Server en Fedora Directory server.

De kenmerken van de directory komen overeen met de kenmerken van een hiërarchische database. De hiërarchische database gaat er van uit dat elk record in een database weer kan verwijzen naar een n-aantal andere records. Op deze manier ontstaat een boomstructuur, die steeds verder kan vertakken. Kenmerkend is dat ieder object één en niet meer dan één eigenaar kent. Het hiërarchische model kent maar één boom per database, de takken hebben onderling geen samenhang en de enige ingang van de boomstructuur is van bovenaf (root).

4.2 LDAP naming context

Een LDAP naming context, ook wel suffix genoemd, is de naam (distinguished name) van het startpunt in de directory hiërarchie. Voor de notatie van de LDAP naming context worden twee vormen veelvuldig gebruikt. Dit zijn een LDAP naming context gebaseerd op:

1. Originele X500 stijl, o=<organisatie>, c=<land code>

2. Domain naming stijl deze komt overeen met de DNS naming stijl

In de DWR 2 directory infrastructuur wordt gebruik gemaakt van een LDAP naming context gebaseerd op de domain naming stijl. Deze stijl sluit aan bij de stijl die in de DWR 1 directory infrastructuur wordt gehanteerd. De exacte naamgeving zal plaats vinden tijdens het technisch ontwerp van de directory infrastructuur.

4.3 Communicatieprotocol

Zoals is aangegeven vindt toegang tot de gegevens in de directory plaats op basis van de open standaard Light Directory Access Protocol (LDAP, RFC 4512) of het Directory Service Markup Language (DSML).

Het LDAP protocol definieert het transport en het berichtenformaat dat tussen de client en de directory plaats vindt wanneer gegevens in de directory benaderd worden. Het LDAP protocol is ontwikkeld op basis van het X.500 protocol. Dit protocol is erg omvangrijk met het gevolg dat het veel rekenkracht kost en niet veel wordt gebruikt. Het LDAP protocol kost veel minder rekenkracht, is op open standaards gebaseerd en in de huidige tijd het protocol om gegevens in een directory te benaderen. Het TCP/IP poortnummer voor niet versleuteld LDAP is 389 en voor versleuteld LDAP 636.

DSML (Directory Services Markup Language) is een open, uitbreidbaar, en op standaards gebaseerd formaat voor het uitwisselen van gegevens met een directory. Met behulp van DSML kan de communicatie tussen verschillende directories worden gestroomlijnd en is het gemakkelijk om gegevens in directories met elkaar te delen. DSML maakt gebruik van XML gebaseerde vragen (requests) en antwoorden (responses) in plaats van ASN.1 BER encoding waarvan het LDAP protocol gebruik maakt. DSML kost meer rekenkracht dan het LDAP protocol.

Uit performance overwegingen wordt voor communicatie met de directory in de DWR 2 infrastructuur hoofdzakelijk gebruik gemaakt van het LDAP protocol.

Om gebruik te kunnen maken van gegevens in departementale gegevensbronnen ondersteunt de DWR 2 directory de protocollen LDAP, XML, JDBC en ODBC.

4.4 Authenticatie

Voordat toegang kan worden verleend tot gegevens in een directory moet eerst verbinding worden gemaakt met de directory. Op dat moment kan authenticatie plaats vinden op drie manieren:

1. **Geen authenticatie**, deze vorm van authenticatie is bijvoorbeeld geschikt is voor alleen het lezen van adresgegevens;
2. **Basic authenticatie**, deze vorm van authenticatie vraagt om een gebruikersnaam en wachtwoord. De desbetreffende authenticatie gegevens worden niet versleuteld verzonden;
3. **Secure authenticatie**, Simple Authentication and Security Layer (SASL) is beschikbaar in LDAP versie 3. SASL ondersteunt de authenticatie mechanisme Kerberos, S/Key en X509 certificaten.

De DWR 2 directory biedt authenticatie mogelijkheden op basis van alle drie de bovenstaande manieren. Welke authenticatie manier wordt geïmplementeerd zal afhangen van het geëiste beveiligingsniveau van de gegevens.

4.5 Autorisatie

Alle gegevens die in de directory worden opgeslagen krijgen bijbehorende specifieke toegangsrechten. Sommige van deze gegevens zijn voor iedereen toegankelijk en andere gegevens zijn alleen toegankelijk voor een specifieke groep medewerkers. In toegang kan onderscheid worden gemaakt tussen alleen de mogelijkheid van de gegevens lezen of ook de mogelijkheid van gegevens schrijven/aanpassen. LDAP versie 3 biedt geen mogelijkheden om toegang tot gegevens te regelen. Het gevolg is dat momenteel elke directory implementatie zijn eigen "access control list" implementatie hanteert.

Op het moment van schrijven is het niet mogelijk om autorisatie, tot gegevens in een open source gebaseerde directory, te verlenen op basis van claims.

4.6 Gegevensleverancier

Na het behandelen van de onderwerpen directory authenticatie en directory autorisatie is het tijd om te bepalen wie, welk soort gegevens levert. De twee gegevensleveranciers aan de DWR 2 directory zijn de departementen en DWR zelf. Deze leveren de volgende gegevens:

- **Departementen**, departementen leveren departementale gebruikersidentiteiten met gerelateerde gegevens en gegevens die benodigd zijn voor een specifieke applicatie.
- **DWR**, DWR levert DWR computeridentiteiten, DWR beheerderidentiteiten, beveiligingsgroepen, policies en DWR applicatie specifieke gegevens.

Waar en welke gegevens exact worden vastgelegd valt buiten de reikwijdte van deze opdracht maar een architectuur doel van DWR 2 is om de benodigde gegevens bij het bronsysteem op te halen (DWR 10 eenmalig opvragen).

4.7 Type directories

In dit document is tot en met deze paragraaf in het algemeen gesproken over LDAP directory. De literatuur maakt onderscheid in drie typen LDAP directories. Deze typen directories hebben allemaal hun eigen specifieke kenmerken.

1. Metadirectory

Een metadirectory is een directory waarin objectgegevens worden gesynchroniseerd uit meerdere opslagfaciliteiten (directories, databases, ...). Deze directory wordt ook wel enterprise directory genoemd. De objectgegevens in de metadirectory worden aan de afnemer aangeboden onder één LDAP naming context. Het synchroniseren van de gegevens kan plaats vinden op basis van specifieke regels naar een specifieke bron op een specifiek tijdstip/interval. Bij implementatie van een directory in de DWR 2 infrastructuur heeft dit type directory niet de voorkeur. De reden hiervoor is: dit type directory voldoet niet aan de eis *DWR 10 Eenmalig uitvragen* (zie bijlage I). Bij implementatie van een metadirectory in de DWR 2 infrastructuur zal de hoeveelheid objectgegevens die gesynchroniseerd wordt tot een minimum beperkt zijn. De metadirectory in de DWR 2 infrastructuur zal hoofdzakelijk gebruikt worden voor het ondersteunen van

het authenticatie en autorisatie proces en het opslaan van generieke objectgegevens aangevuld met applicatie specifieke objectgegevens.

2. Virtuele directory

Een virtuele directory is een directory waarin geen objectgegevens aanwezig zijn. Een virtuele directory bevat verwijzingen naar verscheidene opslagfaciliteiten waar de gevraagde objectgegevens opgehaald kunnen worden. De virtuele directory biedt de objectgegevens in de verscheidene opslagfaciliteiten aan onder één LDAP naming context. Bij implementatie van een directory in de DWR 2 infrastructuur heeft dit type directory de voorkeur omdat deze voldoet aan de eis *DWR 10 Eenmalig uitvragen* (zie bijlage I). Dit wordt gerealiseerd met behulp van een zogenoemd federatief gegevensmodel.

3. Applicatie specifieke directory

Een applicatie specifieke directory is een directory die alleen wordt gebruikt in het geval dat een applicatie/techniek dit vereist. Deze directory is hoofdzakelijk gevuld met applicatie specifieke objectgegevens. De implementatie van dit type directory wordt in de DWR 2 infrastructuur tot een minimum beperkt.

4.8 Topologie

Zoals in de inleiding is aangegeven, vervult de directory een cruciale rol in de DWR IT dienstverlening. Het gevolg hiervan is dat hoge beschikbaarheids- en performance eisen worden gesteld aan de directory. Voor het bereiken van een hoge mate van beschikbaarheid en performance kunnen de directory gegevens gedistribueerd worden. Gegevens distributie houdt in dat de directory gegevens over meerdere databases verspreid worden. Dit kan worden gerealiseerd met behulp van database partitionering en replicatie. Deze databases kunnen worden geplaatst op één fysieke server maar kunnen ook gedistribueerd worden over meerdere fysieke servers.

4.8.1 Partitioneren

Directory gegevens kunnen gedistribueerd worden met behulp van database partitionering. Het gevolg van database partitionering is dat elke database een gedeelte van de gegevens bevat van de directory. Database partitionering brengt de volgende negatieve gevolgen met zich mee ten opzichte van een directory bestaande uit één database:

1. **afname in performance.** Deze is het gevolg van koppelingen met/ verwijzingen naar andere databases.
2. **vergt een grotere beheerinspanning.** De grotere beheerinspanning wordt veroorzaakt door dat elke fysieke server met een suffix een planning/faciliteiten vereist op het gebied van backup, recovery en gegevens management.

Om de negatieve gevolgen van database partitionering in de DWR 2 directory infrastructuur te minimaliseren, wordt van deze techniek in beperkte mate gebruik gemaakt.

4.8.2 *Referrals en chaining*

Om te zorgen dat de verscheidene database partities als één directory aan te spreken zijn, worden de verscheidene database partities met elkaar verbonden.

Voor het verbinden van de verscheidene database partities zijn twee typen technieken beschikbaar:

1. Referrals

Op het moment dat een gedistribueerde directory gebruik maakt van referrals, dan krijgt de client applicatie een verwijzing terug op welke directory server de gevraagde gegevens gevonden kunnen worden;

2. Chaining

Op het moment dat een gedistribueerde directory gebruik maakt van chaining handelt de directory, uitnaam van de client applicatie, de vraag af en levert de gevraagde gegevens.

Op het moment dat in de DWR 2 directory infrastructuur gebruik gemaakt wordt van een database partitionering dan worden de verscheidene database partities met elkaar verbonden met behulp van de techniek chaining. De reden voor deze keuze is dat niet alle client applicaties referrals ondersteunen 1.

4.8.3 *Replicatie model*

Directory gegevens kunnen ook gedistribueerd worden met behulp van replicatie. Dit houdt in dat dezelfde directory gegevens op meerdere servers aanwezig zijn. Het gevolg van het meerdere keren aanwezig zijn van dezelfde directory gegevens is dat moet worden bepaald op welke database schrijf acties plaats vinden. Vervolgens moet worden bepaald op welke wijze deze schrijf acties worden gerepliceerd. Voor dit vraagstuk zijn in de hedendaagse directory software de volgende twee replicatie technieken aanwezig:

1. Single master techniek

Bij de single master techniek vinden schrijf acties altijd plaats op één specifieke server die de betrokken gegevens bevat. Vervolgens worden deze wijzigingen naar de desbetreffende servers gerepliceerd. Een bekende implementatie van deze techniek is DNS.

2. Multi master techniek

Bij de Multi master techniek kunnen schrijf acties plaats vinden op alle servers die de desbetreffende gegevens bevatten. Vervolgens worden deze naar de desbetreffende servers gerepliceerd. Een bekende implementatie van deze techniek is de MS Windows Active Directory.

De multi master techniek heeft een complexere replicatie implementatie tot gevolg dan de single master techniek.

Met de huidig beschikbare kennis kiest DWR voor het replicatie model single master. De reden hiervoor zijn:

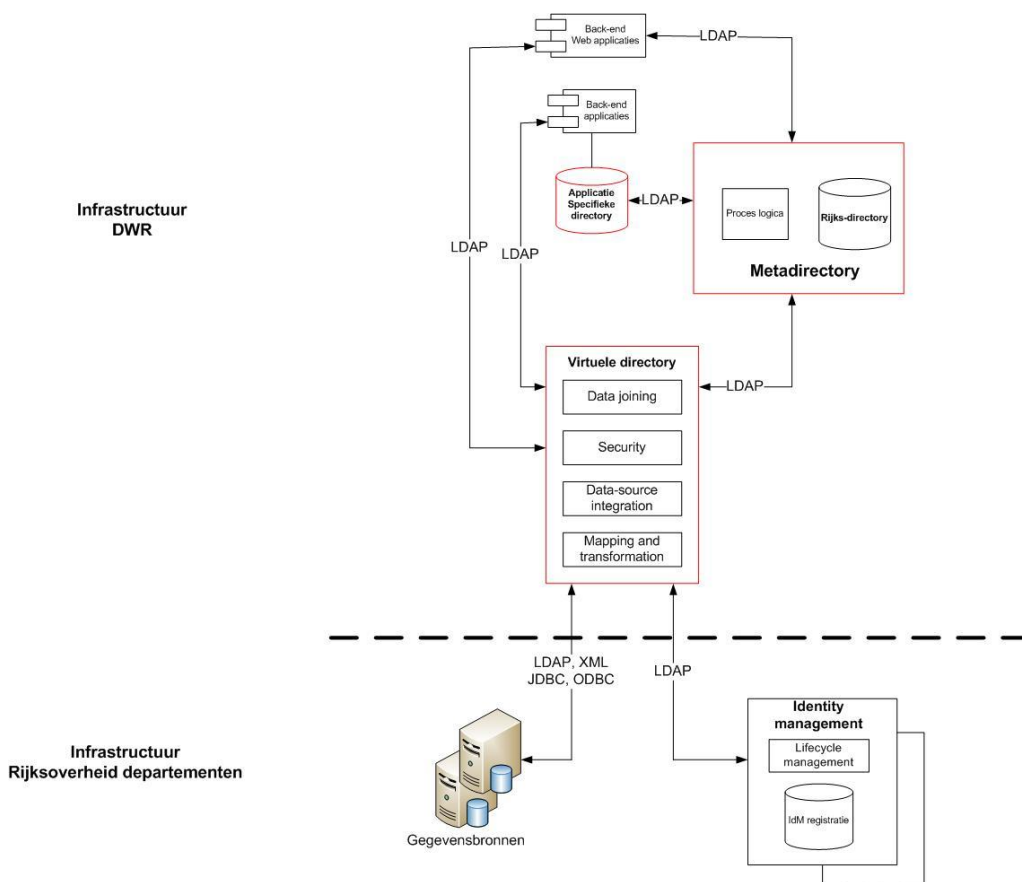
1 Een uitgebreide beschrijving van dit onderwerp is te vinden op de volgende web site: <https://www.redhat.com/docs/manuals/dir-server/deploy/7.1/referral.htm>

4. De single master replicatie techniek heeft een substantieel kleinere kans op replicatie fouten dan de multi master replicatie techniek.
5. Probleem analyse is eenvoudiger in een single master replicatie omgeving dan in een multi master replicatie omgeving.
6. Een beperkte spreiding (Nederland) van locaties waar directory servers worden geplaatst. Deze locaties zijn tevens doormiddel van snelle verbindingen (lage roundtrip delay time) met ruim voldoende beschikbare bandbreedte met elkaar verbonden.

Het vaststellen van de definitieve directory replicatie techniek vereist een nader onderzoek. In dit onderzoek moet vastgesteld worden of de gewenste performance gerealiseerd kan worden met de single master techniek in combinatie met het aantal te verwachten schrijf acties (inclusief bijbehorend volume) in de DWR 2 directory infrastructuur.

5 DWR 2 technische directory architectuur

Op basis van deze informatie uit de voorgaande hoofdstukken is de DWR 2 technische directory architectuur ontwikkeld die in de volgende paragrafen wordt beschreven. De onderstaande afbeelding is een logische weergave van de directory architectuur in de DWR 2 infrastructuur.



5.1 Implementatie virtuele directory

De virtuele directory vervult in de DWR 2 directory infrastructuur een centrale rol. De virtuele directory treedt naar de departementen op als centraal contactpunt waarmee departementale gegevensbronnen verbonden worden. De virtuele directory treedt in de DWR directory infrastructuur op als centrale naamgever voor LDAP directory gerelateerde zaken. Dit houdt in dat de overige DWR 2 directories onder de root suffix worden geplaatst van de virtuele directory.

De reden voor het gebruik van het directory type virtueel is:

1. Gegevens zijn uitsluitend opgeslagen in de bronsystemen

2. Gegevens zijn up-to-date
3. Te hanteren beveiliging wordt bepaald door gegevensbron(department)
4. Departement kan auditen wie, welke gegevens benadert op het bronsysteem
5. Lagere kosten dan implementatie van metadirectory

Het nadeel van het gebruik van een virtuele directory is de lagere performance die geboden wordt ten opzichte van de andere type directories.

5.2 Implementatie metadirectory

De metadirectory vervult in de DWR 2 directory infrastructuur een centrale rol in het authenticatie proces, in de opslag van DWR (generiek/applicatie specifiek) objecten en in het beheer van deze objecten. De metadirectory treedt naar de DWR applicaties op als centraal contactpunt/opslagfaciliteit. De metadirectory maakt gebruik van een LDAP sub suffix direct onder de LDAP root suffix (virtuele directory).

De reden voor het gebruik van het directory type meta is:

1. Performance
2. Applicatie eis
3. Automatisch afhandelen van synchronisatie met de departementale IdM systemen en wanneer dit gewenst is tussen de verscheidene directories in de DWR infrastructuur.

5.3 Implementatie applicatie specifieke directory

Het gebruik van een applicatie specifieke directory zal in de DWR 2 infrastructuur tot het minimum worden beperkt. Een applicatie specifieke directory treedt voor één specifieke applicatie op als opslagfaciliteit. De applicatie specifieke directory maakt gebruik van een LDAP sub suffix direct onder de suffix van de metadirectory. De applicatie specifieke directory wordt door middel van chaining verbonden met de metadirectory. De applicatie specifieke directory wordt tevens verbonden met de metadirectory voor het uitwisselen van generieke objecten met bijbehorende attributen. De enige reden die een applicatie specifieke directory rechtvaardigt, is dat de desbetreffende DWR applicatie deze vereist.

6 Mogelijke software

Op het moment van schrijven zijn nog geen specifieke productselectiecriteria bekend voor DWR 2. Ondanks dit gegeven kan de DWR 2 directory architectuur, zoals deze in hoofdstuk 5 is beschreven, worden gerealiseerd op basis van drie open source producten.

6.1 **Virtuele directory**

De virtuele directory kan geïmplementeerd worden met behulp van het product Penrose virtual directory (licentie: GPL).

6.2 **Metadirectory**

De metadirectory kan worden geïmplementeerd met een combinatie van twee open source producten. Dit zijn de LDAP synchronization module van Penrose virtual directory (licentie: GPL). Deze module verzorgt de automatische synchronisatie met de departementale IdM systemen en wanneer dit gewenst is tussen de verscheidene directories in de DWR infrastructuur. De opslagfaciliteit van de metadirectory kan geïmplementeerd worden met behulp van het product OpenLDAP (licentie: GPL).

6.3 **Applicatie specifieke directory**

De applicatie specifieke directory kan worden geïmplementeerd met behulp van het product OpenLDAP (licentie: GPL).

Bijlage I

DWR 2 principes	
Naam	Toelichting
DWR 01 Medewerker centraal	Bij de inrichting van de Digitale Werkomgeving Rijksdienst wordt de medewerker als uitgangspunt genomen. (scope), employability centraal. Een belangrijke succesfactor van de DWR is de acceptatie door de medewerker.
DWR 02 PTO/ APATAD	Plaats-, Tijd en Organisatieonafhankelijk/Any place, Any Time, Any Device. Informatievoorziening is zowel op kantoor, thuis als onderweg, zowel nationaal als internationaal, beschikbaar. Bovendien is informatie 24x7x365 beschikbaar.
DWR 06 Basiswerkomgeving	DWR biedt op termijn een basisvoorziening welke 80% van de behoefte kan dekken. Afwijkende behoeften van de basisvoorziening (zie DWR-principe 1) worden als mogelijke plug-ins gepositioneerd (zie DTO oplossing).
DWR 07 Gepersonaliseerd	De rijksambtenaar wordt voorzien van informatie welke zoveel mogelijk op de persoonlijke situatie is toegesneden. Informatie wordt zoveel mogelijk medewerker gerelateerd getoond (o.a. actuele werkplek-, rolgerelateerd). Medewerkers kunnen de stijl/opmaak
DWR 08 No Wrong Door	Geen terugverwijzing aan/door Rijksdienst collega's.
DWR 09 Digitale kennisdeling	De architectuuropbouw van de Rijksdienst is gericht op het verlenen van diensten en services via meerdere kanalen aan meerdere doelgroepen, evenals op onderlinge samenwerking door het koppelen van processen en het gezamenlijk gebruiken van gegevens. Medew
DWR 10 Eenmalig uitvragen	Informatie wordt éénmalig uitgevraagd. De Rijksdienst zal overwegend gebruik maken van informatie die reeds door uitvoeringsorganisaties is uitgevraagd. Veel informatie is al aanwezig in overheidsbrede basisregistraties.
DWR 11 Transparantie	Binnen de Rijksdienst worden metagegevens geregistreerd op het moment dat brongegevens worden ontvangen of zaakgegevens wijzigen. Bij voorkeur geschiedt dit automatisch. Transparantie kan tweeledig zijn: in afhandeling wereldgebeurtenissen in herleidbaar
DWR 12 Digitale duurzaamheid	Tbv portabiliteit van informatie dient met gearchiveerde informatie ook de voorziening waarmee de info beheerd kan worden, gearchiveerd te kunnen worden.
DWR 14 Re-use before buy before make	Hergebruik van architectuur componenten gaat boven het aanschaffen (binnenhalen) van componenten. In laatste instantie kan verklaarde ontwikkeling of aanpassing van componenten plaatsvinden.
DWR 15 OSOSS beleid is leidend	Toelichting: Er zal (is?) binnen de Rijksdienst een standaard moeten worden vastgesteld voor het vastleggen van gegevens, het berichtformaat en de datacommunicatie standaarden. Zie ook onder de paragraaf 'berichtenuitwisseling'. zie verder NORA. Toelichti
DWR 17 Comply, explain and commit	DWR-Principes, standaards en richtlijnen dienen door alle projecten te worden toegepast. Afwijking hiervan is tijdelijk mogelijk en dient onderbouwd te worden met tijdspad wanneer er wel voldaan wordt.