Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

ICT~OFFICE

ICT~Marktspiegel doelarchitectuur "Toegang"

Versie 1.0
Datum 9 december 2011

Inhoudsopgave

Samenvatting

Het Rijk heeft de volgende visie geformuleerd aangaande de werkomgeving van een individuele medewerker:

> *"Een Rijksmedewerker is in dienst van het Rijk (één werkgever), heeft binnen het Rijk een unieke digitale identiteit, heeft één e-mailadres, één Rijkspas, één of meerdere (eigen) mobiele devices en steeds vaker een flexibele werkplek.*
>
> *De Rijkspas geldt als standaard authenticatiemiddel voor zowel fysieke als logische toegang. Met de Rijkspas heeft een medewerker toegang tot elk relevant rijkskantoor, logt daarmee ook in (ook thuis of elders) om toegang te krijgen tot relevante bestanden, systemen en informatiediensten en kan daarmee een elektronische handtekening zetten."*

Het daadwerkelijk realiseren van een dergelijk Rijksbreed perspectief op en met Identity en Access Management vormt de belangrijkste uitdaging voor het programma Toegang.
Met de ICT~Marktspiegel wil BZK een spiegel voorgehouden krijgen over de effectiviteit en realiseerbaarheid van de Doelarchitectuur Toegang en de sterke en zwakke punten ervan.
De volgende vragen zijn voorgelegd aan de deelnemende partijen:

1. Draagt de doelarchitectuur bij aan de in de visie omschreven situatie, zo nee, waarom niet en wat mist u in de architectuur?
2. Zijn de 10 Basisprincipes duidelijk, volledig en houdbaar?
3. Wat is uw oordeel over de geschetste Soll-situatie; op welke terreinen voorziet de markt mogelijke problemen (organisatorisch, technisch, bestuurlijk…)?
4. Wat vindt u van de beschreven fasering en welke risico's en mogelijke beheermaatregelen ziet u?

De samengevatte antwoorden op de vragen zijn als volgt:

Ad 1. De doelarchitectuur draagt bij aan de in de visie omschreven situatie. Een uniek ID op basis van natuurlijk persoon is een sterk punt. Extra aandacht is nodig voor medewerkers in het grijze gebied, de verantwoordelijkheid van de datakwaliteit en de beveiliging anders dan de voordeur.

Ad 2. De basisprincipes zijn duidelijk, volledig en houdbaar.
Enkele kanttekeningen worden geplaatst bij de principes 1, 5, 6, 8, 9 en 10. Ad 1 en 6: Kijk ook goed naar asset-management. Ad 5: is er een rijksbreed HR-domein? Ad 8: Er zijn verschillende mechanismen, maar deze zijn niet concreet uitgewerkt. Ad 9: De basisvoorzieningen bestaan uit een Rijkspas (naam voor een pas) en een Rijksaccount (niet bestaande identiteit). Dit laatste is een scopebeperking. De suggestie wordt gedaan om hierom 'Rijksaccount' aan te passen in 'account'. Ad 10: De governance en mapping op de organisatie ontbreekt.

Ad 3. RIdM en P-Direkt moeten de juiste informatie bevatten, dit vereist op centraal en decentraal niveau goede, maar ook pragmatische procedures. Houd een scherpe scheiding tussen identity management en access management. Definieer wanneer het project een succes is. Houd rekening met oude aannames en nieuwe ontwikkelingen en breng een scheidslijn aan voor je naar concrete projecten toegaat.

Ad 4. Een nog meer gefaseerde uitrol (bijvoorbeeld per departement) is aan te bevelen. Er kan gedacht worden aan twee stromen die deels parallel lopen: (1) de ontwikkeling van de basisfunctionaliteit loopt naast (2) de uitrol per departement.

Bij de beantwoording heeft de markt zelf een aantal vragen gesteld. De markt adviseert BZK, aanvullend aan bovenstaande antwoorden, rekening te houden met de volgende vragen:

1. Wat zijn de functionaliteiten van de Rijkspas?
2. Het document mist nog de logica waar we mee bezig zijn. Waarom doe je het? Wat gebeurt er als je het niet doet?
3. Stel expliciet regels aan de hybride situatie, aangezien deze lang zal gaan duren.

1 Inleiding

Dit rapport is opgesteld naar aanleiding van de ICT~Marktspiegel Doelarchitectuur Toegang die is uitgevoerd door ICT~Office in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijks-relaties.
Uit de bedrijven die gereageerd hebben op de openbare bekendmaking heeft het ministerie vijftien leveranciers geselecteerd met de procedure uit de openbare aankondiging. Op 28 november 2011 is daarvoor een bijeenkomst georganiseerd waarin deze leveranciers hebben gereageerd op de vragen vanuit de openbare bekendmaking.

1.1 Aanleiding

Het ministerie van Economische Zaken Landbouw en Innovatie en ICT~Office hebben het initiatief genomen tot het programma `Verbetering samenwerking Rijksoverheid en de ICT-sector´. Het uitvoeren van ICT~Haalbaarheidstoetsen is een van de onderdelen van dit programma. Op basis van een evaluatie is geconcludeerd dat projecten en programma's die nog in de strategiefase zitten, ook gebaat zouden zijn bij een precompetitieve dialoog. Hiervoor is de ICT~Marktspiegel ontwikkeld.

1.2 Doel van de ICT~Marktspiegel

De ICT~Marktspiegel is een nieuw product van ICT~Office en heeft als doel te reflecteren op de plannen en projecten in het ICT-domein bij overheidsorganisaties. De ICT~Marktspiegel levert een beeld op dat in een vroegtijdig stadium aangeeft of het plan of project tot een succes kan leiden en hoe de kans op succes vergroot kan worden.

1.3 Aanpak

Het concept ICT~Marktspiegel kent de volgende stappen:

- De overheid legt een kort omschreven vraag aan ICT~Office voor;
- ICT~Office brengt een aantal door de vragende overheidsinstantie geselecteerde ICT-bedrijven bijeen om commentaar te leveren op de haalbaarheid van het idee/concept. Een lijst met deelnemers is opgenomen in de bijlage;
- ICT~Office organiseert een workshop waarin de deelnemende partijen (de markt) en de vragende partij BZK een dialoog aangaan over de vraagstelling.
- ICT~Office verwerkt de input vanuit de markt tot een geanonimiseerde rapportage.

1.4 Indeling rapport

In hoofdstuk 2 wordt de vraagstelling van BZK aan de markt over de Doelarchitectuur Toegang uiteengezet. Deze vraagstelling is samengevat in vier hoofdvragen, die samen een breed beeld geven van de relevantie, juistheid en haalbaarheid van de doelarchitectuur. De vragen worden beantwoord in de hoofdstukken 3, 4, 5 en 6.

In bijlage A staan de deelnemers aan de workshop genoemd.

In dit rapport wordt generiek verwezen naar 'de markt'. Niet in alle gevallen hebben alle deelnemers een bepaalde mening onderstreept.

Voor meer informatie of vragen inzake dit rapport kunt u contact opnemen met ICT~Office:
Evert Janssen, tel. 0348 – 49 38 45 of via e-mail: marktspiegel@ictoffice.nl

2 Vraagstelling

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft de afgelopen maanden de Doelarchitectuur Toegang ontwikkeld. Deze doelarchitectuur is een belangrijke stap in de richting van het Rijksbreed werken. BZK heeft een ICT~Marktspiegel uitgevoerd met bedrijven die ervaring hebben met Identity en Access Management.
In dit hoofdstuk hebben wij de achtergrond en de vraagstelling uitgewerkt.

2.1 Achtergrond

Het Kabinet heeft in de nota Compacte Rijksdienst de contouren van een vernieuwde Rijksdienst geschetst. De beweging naar organisatieoverstijgend c.q. Rijksbreed werken (zowel in het primaire proces als in de bedrijfsvoering) stelt eisen aan de werkomgeving van een individuele medewerker. Concreet laat zich dat vertalen naar de onderstaande visie:

> *"Een Rijksmedewerker is in dienst van het Rijk (één werkgever), heeft binnen het Rijk een unieke digitale identiteit, heeft één e-mailadres, één Rijkspas, één of meerdere (eigen) mobiele devices en steeds vaker een flexibele werkplek.*
>
> *De Rijkspas geldt als standaard authenticatiemiddel voor zowel fysieke als logische toegang. Met de Rijkspas heeft een medewerker toegang tot elk relevant rijkskantoor, logt daarmee ook in (ook thuis of elders) om toegang te krijgen tot relevante bestanden, systemen en informatiediensten en kan daarmee een elektronische handtekening zetten."*

Het daadwerkelijk realiseren van een dergelijk Rijksbreed perspectief op en met Identity en Access Management vormt de belangrijkste uitdaging voor het programma Toegang. Doel van het programma is het ontwikkelen en (verder) implementeren van Rijksbrede oplossingen op het gebied van Identity en Access Management die een veilige toegang van medewerkers tot panden en systemen moeten borgen, ook over organisatiegrenzen heen.

Deze doelarchitectuur is een eerste stap in het programma Toegang, dat één van de geprioriteerde projecten in het ICCIO-jaarplan 2011 is en als randvoorwaardelijk wordt gezien voor een efficiëntere en effectievere overheid. Bij de bespreking van de hoofdlijnennotitie Toegang in de ICCIO van mei en juni jl. is het belang onderstreept van een gefaseerde en daarmee beheersbare implementatie. Daarbij zou het accent in eerste instantie moeten liggen op de verdere uitrol van de Rijkspas en het verder op orde brengen van het Identiteitenbeheer. Pas daarna zou access management op Rijksniveau verder moeten worden onderzocht. Deze lijn is uitgewerkt in het ICCIO jaarplan voor 2012.

De Doelarchitectuur Toegang gaat vooral over identity management. Maar ook access management - en met name federatieve authenticatie – is in dit document globaal uitgewerkt. Mede omdat er ook op dit moment al concreet behoefte is aan sturing op dit terrein. Een goed voorbeeld daarvan is de inrichting van de single signon dienst door SSO-ICT.

2.1.1 Korte beschrijving van het systeem Toegang

Principes en uitgangspunten

De principes en uitgangspunten van de doelarchitectuur zijn als volgt te formuleren:

- Rijks Identity Management (IdM) als identity service provider (ISP) registreert de unieke personen met daarbij al hun werkrelaties met het Rijk;
- Iedere persoon met een werkrelatie krijgt een uniek medewerker nummer (het "RIN");
- HRM-administratie (P-Direkt) als gezaghebbende bron: uniformering en optimalisatie van HRM- en IdM-beheerprocessen;
- Oorspronkelijke authenticatiegegevens worden alleen gevraagd bij het aangaan of wijzigen van werkrelatie;
- De in het register RIdM geregistreerde personen hebben de mogelijkheid tot inzage in de inhoud en het gebruik van de gegevens die over henzelf zijn geregistreerd;
- Het toegangsbeleid van het Rijk is gebaseerd op rollen, regels en requests (Federatieve authenticatie op basis van open standaarden).

Transitie

Transitie van IST naar SOLL zal in twee fasen geschieden.

Fase 1: Toevoegen van het Rijks Identificatie Nummer (RIN) aan de departementale IdM-omgevingen: inrichten centrale verwijsindex (RIdM)

a. Inrichten proces uitgifte RIN voor nieuwe medewerkers
b. Inrichten centrale verwijsindex (RIdM)
c. RIN voor zittende medewerkers

In deze fase wordt het fundament van de rijksbrede IdM store gelegd; de gegevensverzameling van rijksbrede identificerende nummers. De Rijks IdM store moet gevoed worden vanuit HRM (P-Direkt), hierin staat echter niet iedereen geregistreerd. Hierna zal een verwijsindex worden gerealiseerd met mensen die relatie hebben met rijksdienst op basis van een uniek nummer.

Fase 2: Transformatie Rijksbreed identiteitenbeheer en centrale ontsluiting van departement-overstijgende voorzieningen.

a. Inrichting provisioning departementale IdM-stores naar RIdM
b. Hybride tussenfase
c. Identificatiebeheer als rijksbrede dienst: access management van rijksbrede voorzieningen gekoppeld aan RIdM

In deze fase worden bestaande departementale processen getransformeerd naar een gestandaardiseerd rijksbreed beheerproces. Dit wordt gekoppeld aan de HRM-processen. Hierna zal het access management worden ingericht. Alle informatievoorzieningen zullen hierop worden aangesloten. De specificaties op deze dienst kenbaar maken is ook doel van de architectuur.

P-Direkt

Omdat P-Direkt een gezaghebbende bron moet zijn voor attributen van de personen, heeft dit traject consequenties voor P-Direkt als dienstverlener. De intakeprocessen moeten worden geïmplementeerd in het systeem, de "warme" HRM-processen moeten worden gesynchroniseerd, er moeten kwaliteitseisen worden geïmplementeerd zoals tijdigheid van de processen en de scope van P-Direkt moet uitgebreid worden (externe medewerkers, service medewerkers, etc. moeten ook worden geregistreerd in het systeem). Ook zal P-Direkt eigenaar worden van het proces "uitgifte RIN" (generieke rijksbrede dienst) en eigenaar/beheerder van de verwijsindex "Rijks werkrelatie-register". Tot slot wordt P-Direkt wellicht de beheerder van Rijks IdM.

2.2 Vraagstelling ICT~Marktspiegel

Met de ICT~Marktspiegel wilde BZK een spiegel voorgehouden krijgen over de effectiviteit en realiseerbaarheid van de doelarchitectuur en de sterke en zwakke punten ervan.
De volgende vier vragen zijn voorgelegd aan de deelnemende partijen:

Vraag 1. Draagt de doelarchitectuur bij aan de in de visie omschreven situatie, zo nee, waarom niet en wat mist u in de architectuur?

Vraag 2. Zijn de 10 Basisprincipes duidelijk, volledig en houdbaar?

Vraag 3. Wat is uw oordeel over de geschetste Soll-situatie; op welke terreinen voorziet de markt mogelijke problemen (organisatorisch, technisch, bestuurlijk…)?

Vraag 4. Wat vindt u van de beschreven fasering en welke risico's en mogelijke beheermaatregelen ziet u?

Voor het uitwerken van de vragen zijn de deelnemers aan de marktspiegel verdeeld in groepen. Hieraan voorafgaand vond nog een korte plenaire discussie plaats over enkele inhoudelijke aspecten van de doelarchitectuur. Omwille van de toepasbaarheid van dit document hebben we deze discussie verwerkt bij de antwoorden van de vragen 2 en 3.

3 Bijdrage doelarchitectuur aan de visie op toegang (vraag 1)

Visie

De visie op toegang is:

> *"Een Rijksmedewerker is in dienst van het Rijk (één werkgever), heeft binnen het Rijk een unieke digitale identiteit, heeft één e-mailadres, één Rijkspas, één of meerdere (eigen) mobiele devices en steeds vaker een flexibele werkplek.*
>
> *De Rijkspas geldt als standaard authenticatiemiddel voor zowel fysieke als logische toegang. Met de Rijkspas heeft een medewerker toegang tot elk relevant rijkskantoor, logt daarmee ook in (ook thuis of elders) om toegang te krijgen tot relevante bestanden, systemen en informatiediensten en kan daarmee een elektronische handtekening zetten."*

Vraag 1

Draagt de doelarchitectuur bij aan de in de visie omschreven situatie, zo nee, waarom niet en wat mist u in de architectuur?

Het antwoord van de markt samengevat

De doelarchitectuur draagt bij aan de in de visie omschreven situatie. Een unieke ID op basis van een natuurlijk persoon is een sterk punt. Er zijn echter zaken die missen of onduidelijk zijn:

- De architectuur mist A2A (access to archives) authenticatie;
- Er is weinig aandacht voor "het grijze gebied" (bijv. servicemedewerkers lopen met eigen manager mee naar binnen);
- Iedereen zou in het RiDM moeten worden geregistreerd: ook externe medewerkers, outsourcing partijen (bijv. India) en IT-beheerders;
- Het zwaartepunt ligt op de beveiliging aan de voordeur, maatregelen aan de achterdeur missen nog;
- De verantwoordelijkheid voor de kwaliteit van de data is nog onvoldoende duidelijk uitgewerkt, waardoor er een risico van vervuiling van de database is.

Verloop van de discussie

Een unieke ID op basis van een natuurlijk persoon is een sterk punt. Let wel op dat de authenticiteit van een natuurlijk persoon gecheckt moet kunnen worden tijdens de registratie in het systeem. Het systeem zal zo ingericht moeten worden dat de persoon er zelf voor zorgt dat de informatie up to date en correct is. Zoek dus naar incentives. De ervaring leert dat met goede incentives reiniging aan de voorkant vanzelf ontstaat als er iets niet klopt.

Naast de controle aan de voordeur moet ook de bron kloppen; enkelvoudige registratie is niet per definitie kwaliteit verhogend.

Houd ook rekening met uitzonderingen. Bijvoorbeeld: de bijzondere functionaris die niet met naam en toenaam in het systeem zichtbaar mag zijn.

Zorg ervoor dat de lijnmanager en andere actoren in het proces zo goed mogelijk ondersteund worden. Het systeem moet faciliterend zijn in plaats van hinderend.

Als laatste wordt gerefereerd aan de Rijkspas als standaard authenticatiemiddel. Rekening houdend met toekomstige ontwikkelingen (zoals identificerende smartphones): welke functionaliteiten van de Rijkspas zijn van belang voor rijksbrede toegang? Deze moeten functioneel worden gespecificeerd.

4 Basisprincipes Doelarchitectuur (vraag 2)

De 10 basisprincipes

Onderstaande basisprincipes gelden als voorlopige rijksbrede afspraken (status „concept"). Naar aanleiding van verdere ontwikkelingen, discussies en/of besluitvorming, kunnen de principes in volgende versies van de doelarchitectuur nog worden gewijzigd en/of aangevuld.

1: Een persoon kan niet meer dan één keer geregistreerd staan in het register RIdM en wordt daarbij geïdentificeerd met een uniek Rijks Identificatie Nummer

2: Oorspronkelijke authenticatiegegevens van personen worden alleen gevraagd en gebruikt bij het aangaan of wijzigen van een werkrelatie, met het doel te verifiëren of de betreffende persoon al eerder in het register RIdM is opgenomen

3: Registratie van nieuwe, gewijzigde of beëindigde werkrelaties in het register RIdM, gebeurt onder verantwoordelijkheid (en in opdracht) van het lijnmanagement dat de werkrelatie is aangegaan.

4: De in het register RIdM geregistreerde personen hebben de mogelijkheid tot inzage in de inhoud en het gebruik van de gegevens die over henzelf zijn geregistreerd

5: De verantwoordelijkheid voor correcte registratie van personen en werkrelaties in het register RIdM, berust bij het rijksbrede HRM-domein.

6: Handelingen met voorzieningen van het Rijk zijn te herleiden tot een natuurlijke persoon.

7: Het systeem RIdM waarborgt de (wettelijke) privacy van geregistreerde personen, door adequate op risicoanalyse gebaseerde beveiligingsmaatregelen, zowel technisch als administratief organisatorisch.

8: Het toegangsbeleid van het Rijk is gebaseerd op rollen, regels en requests.

9: Alleen personen die zijn opgenomen in het register RIdM krijgen toegang tot de basisvoorzieningen van het Rijk.

10: Het systeem RIdM is een samenhangend geheel van onafhankelijke herbruikbare services, en maakt gebruikt van vastgestelde open standaarden en bestaande rijksbreed herbruikbare voorzieningen en services.

Vraag 2

Zijn de 10 Basisprincipes duidelijk, volledig en houdbaar?

Het antwoord van de markt samengevat

Het begrip 'houdbaar' wordt geïnterpreteerd als toekomstvast en implementeerbaar. Op hoofdlijnen wordt ingestemd met de 10 principes. Vervolgens worden de volgende kritische noten geplaatst:

- Ad 1 en 6: Kijk niet alleen naar identiteitmanagement maar ook naar asset-management. Dit in het belang van plaats en tijd onafhankelijk werken; dat wordt met deze principes niet voldoende ondersteund. Bijvoorbeeld: op naam verstrekte ICT-middelen die nu een departementale status genieten.

- Ad 5: Het is maar de vraag of er wel een rijksbreed HR-domein is of dat er meerdere domeinen zijn die door één systeem worden ondersteund?

- Ad 8: Dit principe gaat over autorisaties (access management). In paragraaf 2.1 is al toegelicht dat access management in de doelarchitectuur slechts globaal is beschreven. De hier genoemde mechanismen moeten bij de nadere uitwerking van access management in meer detail worden beschreven.

- Ad 9: De basisvoorzieningen bestaan uit een Rijkspas (naam voor een pas) en een Rijksaccount (niet bestaande identiteit). Dit laatste is een scopebeperking. De suggestie wordt gedaan om 'Rijksaccount' aan te passen in 'account' (waardoor ook departementale accounts niet meer buiten de scope vallen).

- Ad 10: De rationale van dit principe ontbreekt: waarom wordt deze richting gekozen? De governance en de mapping op de organisatie missen. Wie is er eigenaar? Welke rollen kun je onderkennen? Is het centraal of decentraal?

Verloop van de discussie

Het HR domein heeft de verantwoordelijkheid dat het dossier compleet is. De registratie vindt echter decentraal plaats. Lijnmanagers beslissen wie welke rollen krijgt. De verantwoordelijkheid van het lijnmanagement voor het P-dossier moet worden benadrukt, anders kan het centrale HR domein de verantwoordelijkheid niet invullen.

Departementen hebben verschillende systemen voor het registreren van externen.

Autorisatie: access management is door de ICCIO in de planning voor 2012 opgenomen. Toch heeft men in de doelarchitectuur alvast iets willen definiëren. Men is zich daarbij bewust van de complexiteit: identity en access management zijn verschillende functies. De scheiding moet duidelijk zijn: hoe helderder hoe meer succes voor de doelarchitectuur.

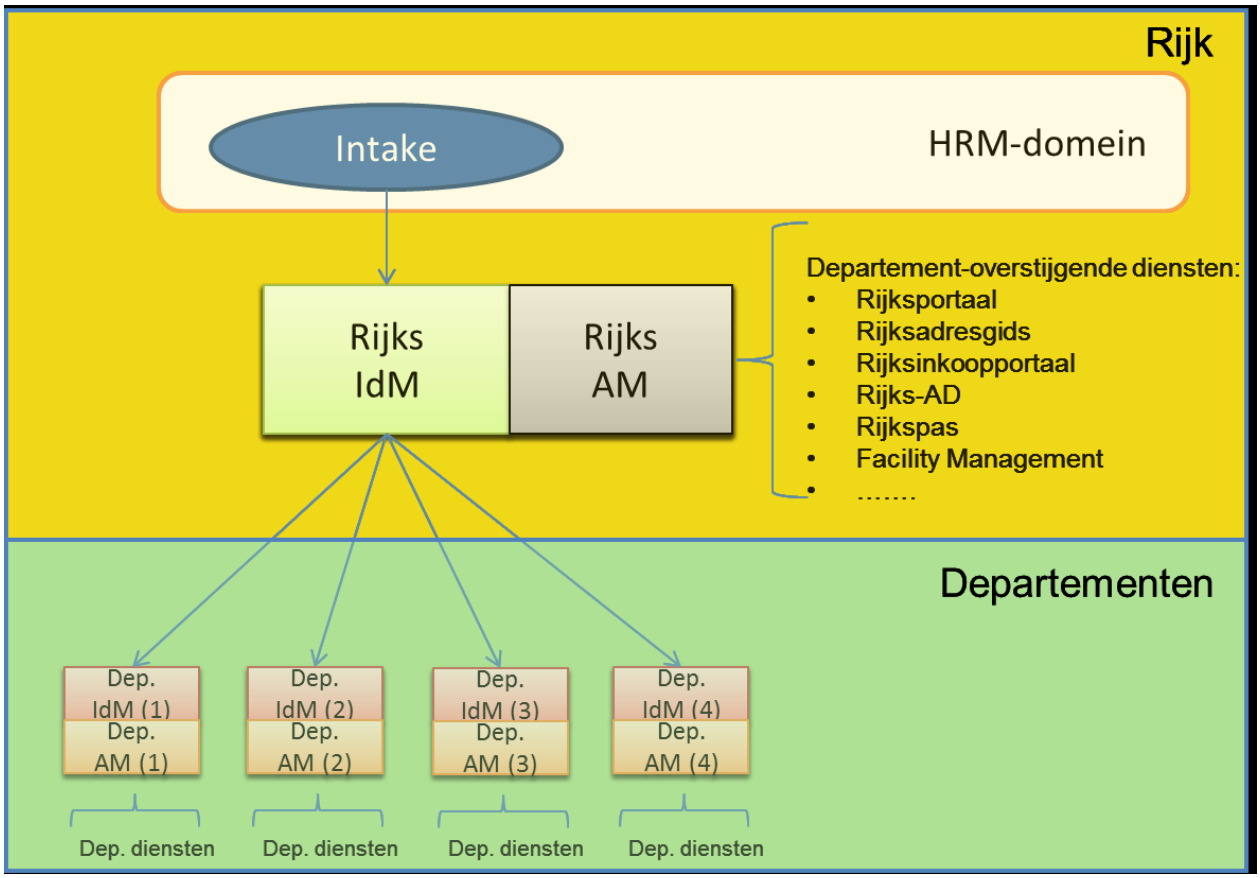
Vaak wordt eigenlijk identity proofing bedoeld waar authenticatie is geschreven. Let op de woordkeuze.

Het principe "Webbased, tenzij", dat de rijksarchitectuur heeft voorgeschreven, heeft de voorkeur voor de toekomst. Er zullen echter nog lange tijd decentrale en departementale applicaties (legacy) bestaan, waarvoor uitzonderingen nodig zijn.

Het document mist nog de logica waar we mee bezig zijn. Waarom doe je het? Wat gebeurt er als je het niet doet? Belangrijk zijn de requirements en de eigenaar. De requirements volgen uit de eisen die worden gesteld door een compacte rijksdienst, waaraan moet worden getoetst of het goed is gedaan.

5 Mogelijke problemen in de Soll-situatie (vraag 3)

Beschrijving soll-situatie



Zie verder het document Doelarchitectuur Toegang.

Vraag 3

Wat is uw oordeel over de geschetste Soll-situatie; op welke terreinen voorziet de markt mogelijke problemen (organisatorisch, technisch, bestuurlijk…)?

Het antwoord van de markt samengevat

De markt ziet de volgende problemen en risico's:

- RIdM en P-Direkt moeten de juiste informatie bevatten;
- Aangezien P-Direkt de aanleverende bron is, zullen er veel maatregelen in P-Direkt moeten worden genomen. Dit kan de tijdigheid in gedrang brengen. In de architectuur is er geen rekening mee gehouden dat er andere partijen brongegevens zouden moeten kunnen aanleveren;

- Er moet een functionele scheiding worden gemaakt tussen enerzijds de locatie van en de verantwoordelijkheid voor de gegevens (in de soll-situatie P-Direkt) en anderzijds het proces waarin (eventueel door verschillende partijen) de gegevens worden geleverd.
- Pragmatisch omgaan met het aanmaken van een persoon in RiDM is gewenst. Bij externe medewerkers zou het inhurende decentrale lijnmanagement moeten kunnen beslissen of registreren in de bronadministratie vereist is (inclusief pas, account en screening).
- Governance: hoe zorg je voor verantwoordelijkheid bij de departementen?
- Wanneer is rijksbrede toegang een succes?
- Bestaande middelen versus nieuwe ontwikkelingen (zoals Rijkspas).
- Helder onderscheid tussen identity management en access management.
- Rijksbreed vs. Departementaal. Rijksbreed wordt gewerkt met attributen en claims, terwijl departementaal nog met RBAC en CBAC wordt gewerkt.

Verloop van de discussie

De markt geeft verschillende aanbevelingen:
Creëer duidelijkheid in de knip tussen identity en access management. Neem het access gedeelte wel mee, maar zorg ervoor dat eerst de basis van identity management kwalitatief goed is. Dataclassificatie komt daar nog na.

Wanneer informatiemanagement niet op orde is, dan kan de deur naar mobile devices niet open.

Het is nog onduidelijk voor welke vertrouwelijkheidniveaus van de informatie het stuk is bedoeld. Wellicht is dataclassificatie, een van de parameters van het identitysysteem, een noodzaak.

Enkele tips om “uit de krant te blijven”:

- Zorg voor een opdrachtgever;
- Stel heldere requirements;
- Bouw een check in;
- Houd het klein;
- Maak het zichtbaar;
- Lessons learned: bekijk rapporten van andere ICT projecten bij de overheid.

6 Risico's en beheermaatregelen fasering (vraag 4)

Fasering

Fase 1: Toevoegen van het Rijks Identificatie Nummer (RIN) aan de departementale IdM-omgevingen: inrichten centrale verwijsindex (RIdM)

a. Inrichten proces uitgifte RIN voor nieuwe medewerkers
b. Inrichten centrale verwijsindex (RIdM)
c. RIN voor zittende medewerkers

Fase 2: Transformatie Rijksbreed identiteitenbeheer en centrale ontsluiting van departement-overstijgende voorzieningen

a. Inrichting provisioning departementale IdM-stores naar RIdM
b. Hybride tussenfase
c. Identificatiebeheer als rijksbrede dienst: access management van rijksbrede voorzieningen gekoppeld aan RIdM

Vraag 4

Wat vindt u van de beschreven fasering en welke risico's en mogelijke beheermaatregelen ziet u?

Het antwoord van de markt samengevat

Een nog meer gefaseerde uitrol (bijvoorbeeld per departement) is aan te bevelen. Er kan gedacht worden aan twee stromen die deels parallel lopen: (1) de ontwikkeling van de basisfunctionaliteit loopt naast (2) de uitrol per departement.

Risico's bij de huidige fasering zijn:

- het ontbreken van een toegevoegde waarde per fase, met mogelijk negatieve gevolgen voor de acceptatie door de departementen;
- het ontbreken van inzicht in de kosten en afspraken over de doorbelasting aan de departementen;
- de verantwoordelijkheden en de verschillende volwassenheidsniveaus van de departementen;
- geen gelegenheid voor leerervaring (terwijl je nu "nog niet weet wat je niet weet").

Een risico van de hybride tussenfase is dat gegevens verschillende zaken betekenen voor verschillende mensen. Hierbij kan gedacht worden aan woorden als 'toegangsrisico', 'functie' of 'gescreend'. De maatregel die hierop kan worden genomen is het definiëren van de belangrijkste begrippen.

Verloop van de discussie

Er wordt nog niet belicht hoe er voor de verschillende op te leveren onderdelen het succes wordt gemeten. De uitrol in fase 1 heeft geen toegevoegde waarde, geen meetbaar succes. Zorg dus dat het faciliterend is, dat mensen er niet omheen willen werken. Neem dit mee als basis in je ontwerp. Betrek hierbij de gebruikersorganisatie, de actoren: doe een processimulatie, geef opleidingen. Zo kom je gemakkelijker van IST naar SOLL.

Breng ook het financiële gedeelte goed in kaart: de kosten en de wijze van doorbelasten. De suggestie wordt gedaan om de kosten van IdM per medewerker per jaar te bepalen. Dit moet dan op basis van een norm worden vastgelegd.

Ook mist een visie op de verantwoordelijkheid voor departementen om aan te sluiten: hoe zorg je voor hen dat het een voordeel is om aan te sluiten? Een punt van aandacht hierbij is dat het RiDM binnen afzienbare tijd moet worden geïmplementeerd en iedereen dit moet doen. De beste volgorde van de aansluiting door departementen moet worden nagegaan.
Het verdient aanbeveling uitvoerenden bij het procesontwerp te betrekken (facilitaire dienst, pasuitreikers).

Het is de departementen verplicht gesteld eraan te voldoen, maar zij hebben verschillende volwassenheidsniveaus. Idee is om dit om te draaien door eisen te stellen waaraan departementen moeten voldoen. Het volwassenheidsniveau van een departement kan worden opgekrikt middels een normenkader.

De stroom van de identiteitsgegevens moet kloppen. De kwaliteit van de data moet zo goed zijn dat departementen mee willen. De functionaliteit volgt daarna. Het is essentieel dat de stroom aan informatie correct en helder is. En dat duidelijk in de keten is wie wat regelt. De hele keten moet werken en moet flexibel zijn om aan te passen.

Het opbouwen van rijksbrede identiteiten begint bottom-up vanuit de departementen. Op een gegeven moment draait dit om en worden ze top-down bepaald, op basis van de nieuwe processen.

Het RIN (Rijks identificatie nummer) wordt aan nieuwe medewerkers uitgereikt. Het zou slimmer zijn om eerst degenen die een Rijkspas hebben een RIN te geven. Die persoonsgegevens zijn goed en dit is dus snel scoren. Let hierbij wel op dat enkele medewerkers meerdere Rijkspassen in hun bezit hebben. Dit is niet heel erg, want het probleem krijg je toch. Oplossing is de attributen over werkrelaties er af te halen indien deze er op staan.

Tot slot wordt er geconstateerd dat de hybride tussenfase lang zal gaan duren (een “fact of life”). Omarm deze dynamiek en stel hier expliciet regels aan. Immers, de weg er naartoe is minstens zo belangrijk als het eindstation. Een risico van een hybride situatie is dat de gegevenswoordenboeken nog niet gesynchroniseerd zijn, waardoor schijnbaar gelijke elementen verschillende betekenissen hebben.

Bijlage A Deelnemers

Organisatie (op alfabet)	Deelnemer
Atos	De heer M. Haas
BT	De heer W. Weris
CA Technology	De heer P. Ferron
Cap Gemini	De heer H. Scholten
Cisco systems International B.V.	De heer W. Mooij
Crosscheck Networks	De heer R. Past (vervangt de heer D. Ansems)
Everett	De heer T. van Vooren
Grabowsky Identity Architects	De heer S. Daniëls
IBM	De heer S. van Daele
Logica	De heer N. IJzinga
Novell	De heer B. van Lith
Oracle	De heer R. Klomp
Quest Software	De heer R. van Es
Traxion	De heer J. van Westeneng
Trusted Id	De heer L. Kuunders (vervangt de heer D. Karamat Ali)
ICTU	De heer P. Bergman
Ministerie van Financiën	De heer H.P. van der Veer
Ministerie van Defensie	De heer B. Dukker
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Mevrouw H. Buyne De heer R. During De heer J. Flippo (inhoudelijke opening) De heer S. de Mooij De heer T. van der Togt
Het Expertise Centrum (HEC)	De heer A. Bloembergen (voorzitter) Mevrouw J. Koole (verslag)
ICT~Office	De heer E. Janssen Mevrouw A. ten Kate-Sloots