Rijksoverheid

Gemeenschappelijk Normenkader Rijksoverheidbreed Identity Management IdM-componenten 1 t/m 4

Datum 11 mei 2009
Status Definitief

Op maandag 11 mei 2009 is dit Gemeenschappelijk Normenkader Rijksoverheidbreed Identity Management vastgesteld door de Interdepartementale Commissie van Chief Information Officers (IC-CIO) als standaard voor de Rijksdienst.

Het besluitvormingstraject voor dit normenkader was als volgt:

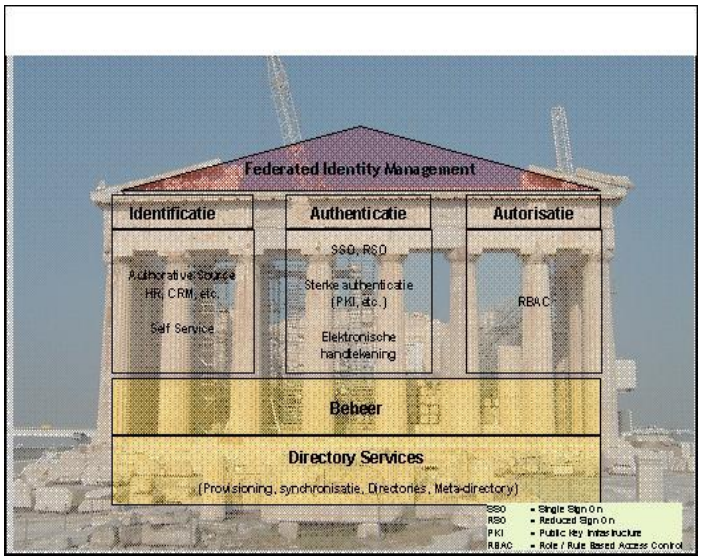
- Vastgesteld in het overleg van de departementale vertegenwoordigers IdM op 26 maart 2008;
- onderschreven door het ROA in de bijeenkomst van 13 mei 2008 (onder voorbehoud van het nader uitzoeken van het gebruik van het BSN in de bedrijfsvoering);
- vermeld in MARIJ 1.0 dd. juli 2008 als (kandidaat)standaard;
- vastgesteld door het IODI in de bijeenkomst van 28 augustus 2008;
- op 19 november 2008 door de Standaardisatiecommissie voor de Rijksdienst van het advies voorzien om door de IC-CIO als standaard voor de Rijksdienst te laten vaststellen.

Inhoudsopgave

1 Inleiding

Achtergrond

Identity Management (IdM) omvat de processen en alle benodigde technische hulpmiddelen voor het beheer van elektronische identiteitsgegevens.
Bij een zorgvuldig Identity Management worden de gegevens die van personen en organisatie-eenheden zijn vastgelegd in een autoritatieve bron gerelateerd aan de elektronische voorkomens van identiteiten, zoals accounts, (rijks)pasjes, tokens en biometrische kenmerken.
Doel daarvan is om op geautomatiseerde wijze personen te kunnen identificeren, authenticeren en autoriseren, bereikbaar te maken (via contactgegevens) of om gepersonaliseerde informatie en -diensten aan te bieden. Identity Management wordt gezien als een infrastructurele component in de informatie-voorziening van de departementen én in die van het Rijk.



Om de diverse aspecten van IdM in een samenhangend geheel te kunnen plaatsen en tevens meer eenduidigheid te verkrijgen in de departementale inzichten en de gebruikte termen, is het “Huis van Identity Management” onderkend.
Het is nog “under construction” en er wordt gestaag aan doorgebouwd.

IdM is pas goed geregeld, als het “staat als een huis”.

Alle gezamenlijke, interdepartementale trajecten zoals Rijkskantoren, P-direkt, de Rijkspas en de Digitale Werkomgeving Rijksoverheid hebben een IdM-voorziening nodig waarmee op flexibele wijze aan medewerkers en andere (overheids-)organisaties toegang kan worden verleend tot informatie en functionaliteit in toepassingen en die tevens voorziet in een goede beveiliging en waarmee inzichtelijk is wie wat mag.
Rijksoverheidbreed Identity Management is daarmee een randvoorwaarde voor de flexibilisering van de Rijksdienst en -veilig- elektronisch samenwerken.

Doel van dit normenkader

In het IODI is het “Stappenplan voor Rijksbreed Identity Management” d.d. 15 mei 2007 vastgesteld waarin de gezamenlijke ambitie, de aspecten van IdM en de te nemen stappen op zowel departementaal als interdepartementaal niveau zijn verwoord. Voor interdepartementale samenwerking is het van belang afspraken vast te leggen teneinde het Identity Management op een dusdanig gelijkwaardig niveau te krijgen dat er wederzijds vertrouwen ontstaat in de kwaliteit van de wijze waarop elektronische identiteiten worden vastgesteld en beheerd. Daarnaast is het van belang afspraken vast te leggen over gegevens om deze te kunnen uitwisselen ten behoeve van o.a. federatieve authenticatie.

In het onderhavige document is het normenkader opgenomen voor de eerste 4 (van de totaal 16) IdM-componenten die in het plan zijn onderkend om tot zo'n vertrouwensniveau te komen. Bedoeling is, samen met de departementale projectleiders IdM en specialisten te komen tot een verdere operationalisering van deze normen en de IdM-componenten.

De normen zijn bewust beperkt in omvang en complexiteit. Het benadrukt de gemeenschappelijke afspraken die minimaal noodzakelijk zijn voor de beoogde elektronische samenwerking.
De verwachting is dat het normenkader op termijn nog op praktische aspecten zal aanscherpen naar aanleiding van de toepassing ervan.

Relatie met andere normenkaders
Bij deze "normen vanuit de praktijk" wordt voortgebouwd op reeds bestaande normenkaders van P-direkt, de Rijkspas en de Rijks-adresgids1 waarbij de focus ligt op de samenhang en de specifieke -aanvullende- normen voor Identity Management.
Dat wil ondermeer zeggen, dat er een procedurebeschrijving is voor het beheer van identiteiten, accounts, tokens en dergelijke, vergelijkbaar met die voor het beheer van de rijkspassen. En dat er rollen zijn gedefinieerd binnen het geheel van die beheerprocessen. Met name de rol van proceseigenaar IdM, die verantwoordelijk is voor de kwaliteit van de uitvoering van de processen conform dit normenkader.

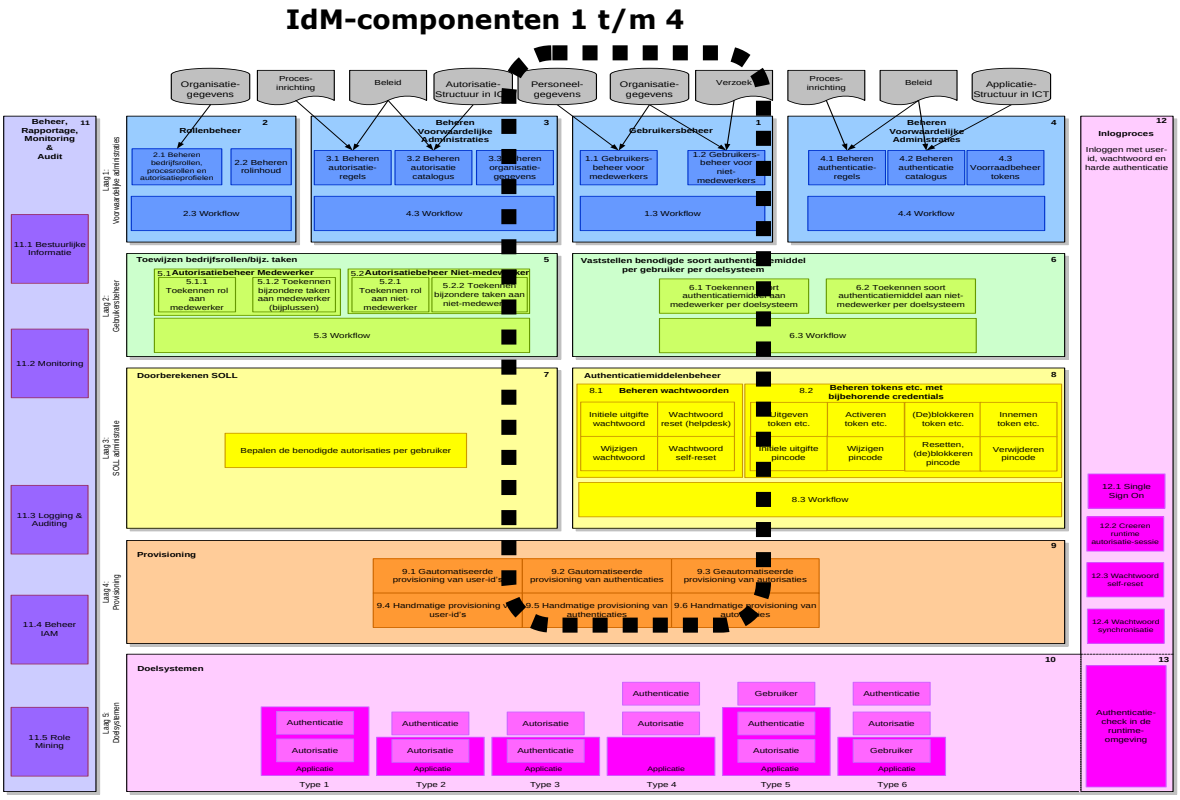
[1] *De gebruikte documenten zijn opgenomen in de samenwerkruimte IdM*

2 Context

Het normenkader beperkt zich momenteel tot de eerste 4 IdM-componenten, te weten:

1. De beheerde IdM-registratie
2. Life-cycle-management van die identiteiten
3. Een geautomatiseerde koppeling met het ICT-systeem (accounts)
4. Een geautomatiseerde koppeling met Fysieke toegangscontrole (Rijkspassen)

Deze “basis”-componenten zijn onderdeel van het gehele aandachtsgebied Identity Management. Ze dekken dus niet alle functionaliteiten, processen en registraties van IdM. Dat illustreren we aan de hand van een functioneel overzicht van Identity and Access Management (IAM). Dit overzicht wordt door de Belastingdienst gehanteerd2 en is nu door de departementale vertegenwoordigers van IdM ook voor het Rijksoverheidbrede Identity Management geadopteerd.



Het zwarte kader laat schematisch zien waar het onderhavige normenkader voor de IdM componenten 1 t/m 4 op is gericht.
De IdM-componenten 5 t/m 9 en 10 t/m 15 omvatten het resterende gedeelte van dit functioneel overzicht en zijn met name gericht op (het beheer van) authenticatie-middelen en autorisaties.
De normen voor laatstgenoemde IdM-componenten zullen op termijn separaat worden uitgewerkt.

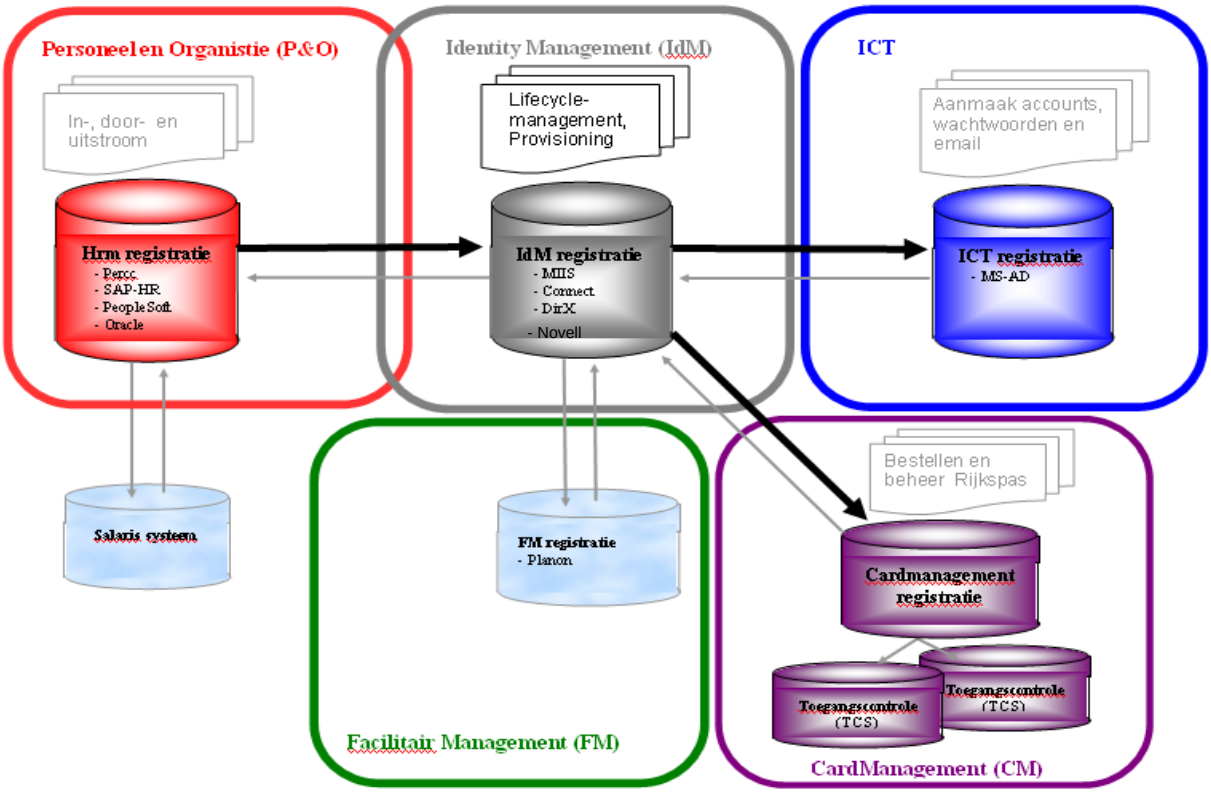
---

2 *Er zijn wereldwijd veel overzichten van dit speelveld, bijvoorbeeld van Gartner, Burton of Microsoft. Het overzicht van de Belastingdienst is mede daarvan afgeleid en is -inclusief toelichting- beschikbaar op de samenwerkruimte IdM op Rijksweb: schema IdM + toelichting.*

De IdM-componenten 1 t/m 4 moeten daarnaast ook worden bezien in de context van specifieke aandachtsgebieden van de huidige bedrijfsvoering bij de departementen:

- Personeel en Organisatie (Hrm),
- Informatievoorziening en Communicatie Technologie (ICT) en
- CardManagement (CM) c.q. Facilitair Management (FM).

In onderstaand schema is een grofmazig kader geschetst waarmee de samenhang tussen de initiële persoonsregistratie en het hergebruik voor toegangscontrole e.d. tot uitdrukking komt.
In het schema zijn de aandachtsgebieden afzonderlijk gekleurd en door middel van de pijlen is de relatie tussen deze aandachtsgebieden weergegeven.
Het normenkader gaat sec in op de normen t.a.v. elke IdM-component.



NB-1. De aangegeven processen zijn niet in het normenkader IdM beschreven aangezien dat al afdoende is gebeurd in de normenkaders van P-direkt en Rijkspas.
Voor de herkenbaarheid is een aantal bestaande systemen genoemd, zónder hiermee een norm te zetten voor het gebruik van één van deze systemen.

NB-2. Ten aanzien van het gebruik van persoonsgegevens ontvingen de SG's van de ministeries op 23 november 2007 een brief waarin de invoering GBA als basisregistratie als gevolg van de gewijzigde wet Gemeentelijke Basisregistratie Persoonsgegevens wordt vermeld.
Daarin werden zij geattendeerd op de verplichting om voor 1 januari 2010 te voldoen aan de consequenties die dit met zich meebrengt.

De GBA dient als formele authentieke-bron van persoonsgegevens in Nederland en overheidsorganisaties zijn verplicht deze gegevens uit de GBA te hanteren voor hun contacten met burgers. Dat geldt ook voor diverse persoonsgegevens van ambtenaren: die worden nu handmatig overgenomen van het paspoort, maar zouden bij voorkeur op geautomatiseerde wijze binnen het departement beschikbaar moeten komen.
In dit verband is principe 2.2.3.4 van Marij relevant: De definitie en taxonomie van gegevens die zijn opgenomen in nationale basisregistraties zijn leidend.

3 Normen voor de IdM-componenten 1 t/m 4

IdM-registratie

De basis voor IdM is een beheerde registratie[3] met basisgegevens over alle voor een organisatie relevante natuurlijke personen. Hierdoor moet zekerheid bestaan over de relatie van een persoon van vlees en bloed met zijn elektronische identiteit(en) en de beschikbaarheid van de juiste en volledige gegevens van alle relevante elektronische identiteiten.
Dit betreft twee belangrijke aspecten: over welke groepen van personen het gaat en over welke gegevens daarbij relevant zijn. Zekerheid over de juistheid van gegevens ontstaat door enerzijds afdoende identificatie van de personen (gebaseerd op identificatie-processen e.d.) en anderzijds door correcte registratie van gegevens.

In de werkprocessen van een organisatie dienen bevoegdheden voor het uitvoeren van de identificatie en registratie te zijn geborgd. Verder dienen de wettelijke eisen (Wbp en VIR) voor het opzetten van Identity Management te worden gevolgd:

- De gegevensverwerking voor Identity Management dient ter instemming aan de ondernemingsraad te worden aangeboden (de departementale ondernemingsraden hebben formeel instemmingsrecht)
- De gegevensverwerking dient aangemeld te zijn bij de departementale functionaris gegevensbescherming t.b.v. een goed privacy reglement conform de Wbp (en te voldoen aan het kader van de Wbp AV23)

Norm-1: In de IdM-registratie zijn tenminste alle personen opgenomen -van zowel het kerndepartement als de uitvoerende diensten- waaraan een ICT-account en / of een toegangspas is uitgereikt[4].

Met “alle personen” wordt bedoeld: alle in- en externe medewerkers, zoals[5]:

1. Medewerkers in vaste dienst
2. Medewerkers in tijdelijke dienst
3. Interim Functievervullers
4. Stagiaires
5. Ingehuurd personeel, onderhoudspersoneel en medewerkers van ingehuurde diensten

[3] *Het kan zijn dat deze IdM-registratie niet één fysieke registratie is, maar bestaat uit een samenhangend stelsel van registraties waarin de verschillende doelgroepen zijn opgenomen. In dat geval spreken we over een “virtuele” IdM-registratie.*

[4] *Een goede IdM-registratie is voor diverse bedrijfsprocessen van belang. De relatie met logische toegang (o.b.v. netwerkaccounts) en met fysieke toegang (o.b.v. toegangspassen) is in dit normenkader expliciet benoemd opdat de identificatie- en authenticatie-middelen die aan personen worden verstrekt ook weer ingetrokken en tussentijds geblokkeerd kunnen worden. Dat is niet alleen nodig vanuit departementale veiligheidsoverwegingen, maar ook om te voldoen aan het interdepartementaal afgesproken vertrouwensniveau.*

[5] *Bezoekers vallen vooralsnog buiten de scope van dit Normerkader IdM. Maar bezoekers doorlopen in feite ook een life-cycle: ze worden (vooraf) aangemeld, melden zich bij de balie, krijgen toegang en melden zich weer af. Een bijzondere groep van “bezoekers” zijn wij zelf, indien we elkaars departement bezoeken; dit zal gelden zolang plateau 2 van de Rijkspas nog niet is gerealiseerd.*

Norm-2: Voor elk van deze personen is de volgende basis-gegevensset vastgelegd[6]:

1. Rijksoverheidbreed uniek referentiekenmerk (BSN[7] of - indien niet aanwezig - de combinatie landcode-paspoortnummer)
2. Naam[8] (voorletters, voorvoegsels, achternaam)
3. Datum aanvang/einde geldigheid life-cycle (de datum aanvang/einde dienstverband of contract)
4. Status Life-Cycle (actueel, ïnactief[9], geblokkeerd, beëindigd)
5. De organisatie(eenheid) die de identiteit heeft vastgesteld en een elektronische identiteit heeft uitgegeven (de Identityprovider, IdP)[10]

Life-cycle-management

Een operationeel proces van het life-cycle-management van de identiteiten in de IdM-registratie dient om zekerheid te hebben over de blijvende juistheid, volledigheid en actualiteit van de geregistreerde gegevens.
Het life-cycle-management is de basis voor de juiste toegangsverlening tot ICT-voorzieningen en voor de fysieke toegangscontrole.

Norm-3: Het life-cycle-management moet voor alle personen aantoonbaar voldoen aan de navolgende kwaliteitseisen:

1. Uiterlijk op de 1e werkdag zijn personen in de IdM-registratie geregistreerd met een datum-geldigheid life-cycle;
2. Uiterlijk op de laatste werkdag zijn personen in de IdM-registratie geregistreerd met een datum-einde-geldigheid life-cycle;
3. De mogelijkheid tot tussentijdse inactivering of blokkade en re-activering in de IdM registratie (n.a.v. bijvoorbeeld schorsing of verdenking van fraude) van personen moet zijn opgenomen in de status life-cycle;
4. Dit life-cycle-management is beschreven, wordt gecontroleerd[11] en is aantoonbaar juist werkend.

---

[6] *Deze basis-gegevensset is gebaseerd op eisen vanuit de processen en afnemende systemen voor logische- en fysieke toegangscontrole en is het minimum aan gegevens dat nodig is. Binnen alle departementen wordt een meer uitgebreide set van gegevens geregistreerd in de bedrijfsvoering. De noodzaak bestaat om afspraken te maken over de te gebruiken gegevensstandaards in het interdepartementale berichtenverkeer. Vanuit het Rijksoverheidbrede Identity Management zal hiertoe een eerste set van gegevens ter standaardisatie worden aangeboden.*

[7] *Zie ook Marij 0.9: principe 1.2.1.14: Ambtenaren hebben een unieke, digitale identiteit. Toelichting: deze identiteit zal gebaseerd zijn op het Burger Service Nummer, zoals wettelijk is bepaald (http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vhlfem1shvqw/f=y.pdf)*

[8] *De naam kent de bijzonderheid van "tenaamstelling", waarbij al dan niet de naam van de partner relevant is. Dit gegeven is een voorbeeld van eerder genoemde uitgebreide gegevensset.*

[9] *(Tijdelijke) inactivering wanneer daar aanleiding voor is, bijvoorbeeld bij schorsing of verdenking van fraude.*

[10] *Zie ook Marij 0.9: principe 3.2.1.5: databasegegevens zijn herleidbaar tot de bron.*

[11] *Uitgangspunt is dat controle plaatsvindt in de lijn en/of door de departementale- of interdepartementale auditdienst en dat die in overleg nader bepalen met welke regelmaat deze controle plaatsvindt. De verwachting vanuit het Rijksoverheidbrede IdM is een jaarlijkse controle.*

Koppeling IdM-registratie en ICT-systeem[12]
De koppeling tussen de IdM-registratie en het ICT-systeem dient om meer zekerheid te krijgen dat alléén ICT-accounts zullen worden uitgegeven aan -en logische toegangsautorisaties zijn ingesteld voor- personen die daar recht op hebben en waarvan het life-cycle-management goed is geregeld.

Norm-4: Er is een (semi-)automatische[13] koppeling tussen de IdM-registratie en het systeem waar de accounts voor logische toegang[14] worden beheerd, waarbij op basis van het life-cycle-management van de betreffende persoon:

1. Accounts (semi-)automatisch worden aangemaakt;
2. Accounts (semi-)automatisch (tijdelijk) kunnen worden geïnactiveerd, ge-reactiveerd, gewijzigd of geblokkeerd;
3. Accounts (semi-)automatisch worden verwijderd c.q. gearchiveerd;
4. Deze geautomatiseerde koppeling tussen IdM en ICT is beschreven, wordt gecontroleerd[15] en is aantoonbaar juist werkend.

NB. Het gaat bij deze norm niet om wat met het account wordt gedaan, zoals wachtwoord toevoegen om het als authenticatie-middel te gebruiken of de rechten die aan het account worden toegekend. Dat valt namelijk onder Autorisatie-beheer (RRRBAC e.d.) en Authenticatie (RSO/SSO e.d.). Zie ook het Stappenplan Rijksoverheidbreed IdM.

Koppeling IdM-registratie en het Fysieke toegangscontrole-systeem
De koppeling van de IdM-registratie met het Fysieke Toegangscontrole-systeem dient om zekerheid te krijgen dat alléén Rijkspassen[16] zullen worden uitgegeven aan -en fysieke toegangs-autorisaties zijn ingesteld voor- personen die daar recht op hebben en waarvan het life-cycle-management goed is geregeld.

---

[12] *Het kan zijn dat accounts worden aangemaakt in diverse ICT-systemen. In dat geval wordt een koppeling voorzien met elk van die systemen.*

[13] *Het feit dat een (semi-)automatische koppeling tussen de IdM-registratie en het ICT-systeem als norm wordt gehanteerd biedt naast efficiëntie-voordeel vooral zekerheid over de integriteit van de gegevens, met name na mutaties in de bron-registratie. De (dubbele) handmatige invoer en achteraf-controles op basis van vergelijkende overzichten e.d. vervallen daarmee. Semi-automatisch verwijst naar de mogelijkheid om deze koppeling te laten verlopen via een workflow, waarbij de gegevens pas geautomatiseerd worden bijgewerkt na accordering daarvoor door een geautoriseerde medewerker.*
Hoe deze (semi-)automatische koppeling werkt, in de zin van processtappen en functionaliteit, zal expliciet beschreven moeten zijn.

[14] *Het streven is het gebruik van accounts te kunnen herleiden tot een natuurlijke persoon. Het programma IdM richt zich in eerste instantie op een "AD account" voor het inloggen op het werkstation en het netwerk. Accounts voor achterliggende applicaties vallen binnen de scope van de componenten RSO/SSO van het programma IdM.*

[15] *Zie de opmerking hierover bij Norm-3.*

[16] *Momenteel vindt de fysieke toegang plaats o.b.v. een departementaal uitgegeven pas. In de nabije toekomst zal dat de Rijkspas worden, gebaseerd op een uniek Rijksoverheidbreed uniek persoonsreferentiekenmerk.*

Norm-5: Er is een (semi-)automatische[17] koppeling tussen de IdM-registratie en het CardManagementsysteem waar de departementale (Rijks)passen voor fysieke toegang worden beheerd, waarbij op basis van het life-cycle-management van de betreffende persoon:

1. Het proces van toekenning en aanmaak van een (Rijks)pas (semi-)automatisch wordt geïnitieerd;
2. (Rijks)passen (semi-)automatisch (tijdelijk) kunnen worden geïnactiveerd of geblokkeerd;
3. Het proces voor inname en / of vernietiging van een (Rijks)pas (semi-)automatisch wordt geïnitieerd;
4. Deze (semi-)automatische koppeling tussen IdM en CardManagement is beschreven, wordt gecontroleerd[18] en is aantoonbaar juist werkend.

NB. Het life-cycle-management van een persoon vormt dus de basis voor het uitgeven en innemen van een (Rijks-)pas, ofwel de card-life-cycle. Het gaat bij deze norm *niet* om wat met de (Rijks-)pas wordt gedaan, zoals (toegangs-)rechten die aan een pas worden toegekend. Dat valt namelijk onder ontwikkelingen als Autorisatie-beheer (RRRBAC e.d.) en Logische toegang en/of PKI-Overheid met de Rijkspas. Daarbij zullen ook de interdepartementale aspecten van toegangscontrole worden afgesproken.
Zie ook het Stappenplan Rijksoverheidbreed IdM.

---

[17] *Hier gelden dezelfde argumenten als bij de koppeling met de ICT-registratie: reeds van een persoon geregistreerde gegevens worden met een geautomatiseerde koppeling overgenomen (zie Norm-4).*
Daarnaast is een relatie is gelegd met processen zoals die zijn onderkend vanuit het Normenkader Rijkspas.

[18] *Zie de opmerking hierover bij Norm-3.*

BIJLAGE Betrokkenen

De volgende personen zijn betrokken geweest bij het initieel opstellen van dit normenkader:

AZ	Ron van der Nat	r.vandernat@minaz.nl	070 3564045
BZK	Cisca Michon	cisca.michon@minbzk.nl	070 4266476
BuZa	Ben Elsinga	ben.elsinga@minbuza.nl	06 53547676
	Paul Welling	paul.welling@minbuza.nl	06 18194814
Defensie	Tom Binnekamp	t.binnekamp@mindef.nl	070 3396799
	Barry Dukker	aad.dukker@mindef.nl	06 12967361
EZ	Rob Jalving	r.r.jalving@minez.nl	070 3796076
	Paul van der Heemst	p.m.vanderheemst@minez.nl	070 3797447
FIN	Martin Krouwer	m.g.m.krouwer@minfin.nl	070 3427131
	Hille Huigens	hj.huigens@belastingdienst.nl	055 5776918
Justitie	Nico van Oldenbeek	n.j.van.oldenbeek@minjus.nl	06 18300055
LNV	Hans van der Burght	j.w.van.der.burght@minlnv.nl	06 48138372
OCW	Ko Heijboer	j.a.m.heijboer@minocw.nl	070 4124893
SZW	Herman Meijer	hmeijer@minszw.nl	070 3335416
VenW	Theo Arts	theo.arts@minvenw.nl	070 3516899
VWS	Marijke Deurloo	ma.deurloo@minvws.nl	070 3406821
	René van der Veen	jr.vd.veen@minvws.nl	070 3407257
VROM	Lisette Maas	lisette.maas@minvrom.nl	070 3392983
	Paul Leunissen	paul.leunissen@minvrom.nl	070 3391210
DG-OBR	Carl Adamse	carl.adamse@minbzk.nl	070 4267414
P-direkt	Cor van der Krogt	cor.krogt@p-direkt.minbzk.nl	06 50768178
	Bert van Bruggen	bert.van.bruggen@p-direkt.minbzk.nl	06 50768166
Rijkspas	Ramon Mulder	ramon.mulder@ictu.nl	070 8896065
Rijksweb	Eric Brouwer	eric.brouwer@ictu.nl	06 25081006
	Maarten de Roos	maarten.roos@ictu.nl	06 46425173
	Letty Velthuijs	letty.velthuijs@ictu.nl	070 8887745