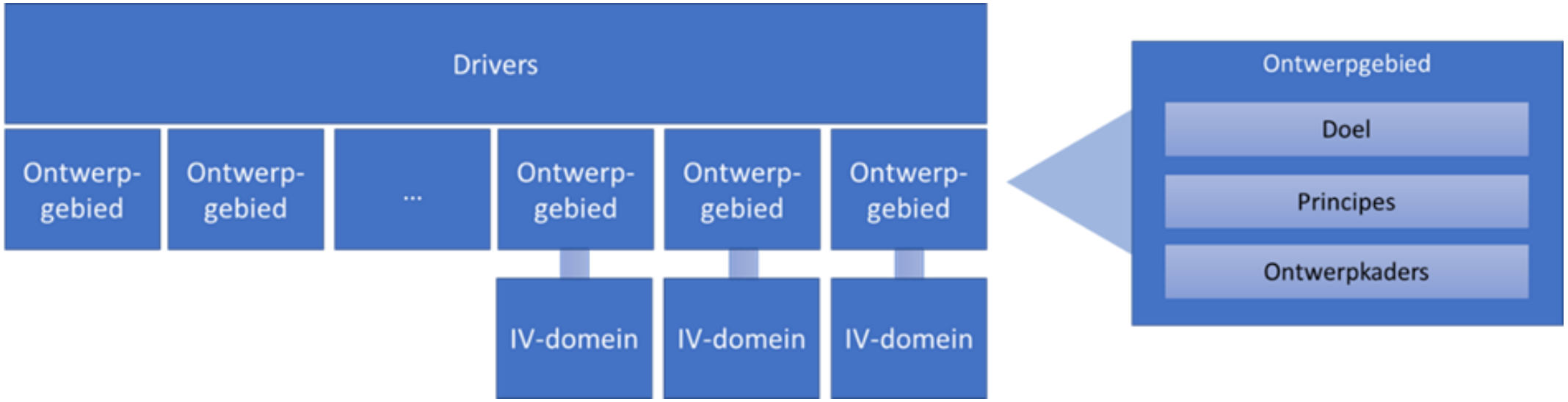
edustandaard

Doelen, Principes, Ontwerpgebieden
QA-team ROSA

Remco de Boer
Beheerteam ROSA
20 januari 2023

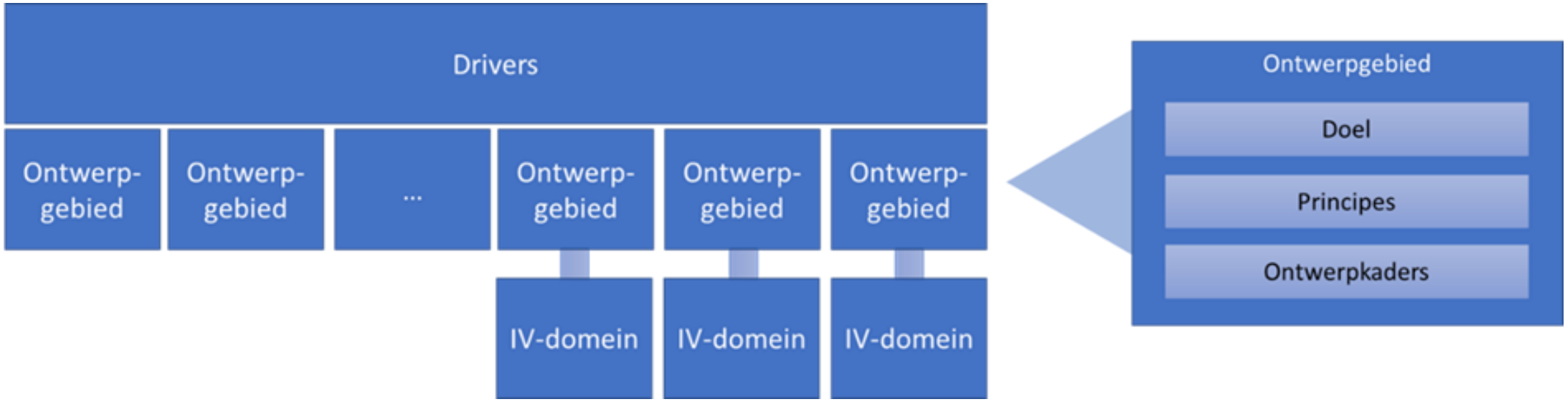
Huidige structuur van Doelen, Principes, Ontwerpkaders



- 7 ontwerpgebieden
- 1 doel per ontwerpgebied
- 3 ontwerpgebieden verbonden aan IV-domein (met dezelfde naam)

edustandaard

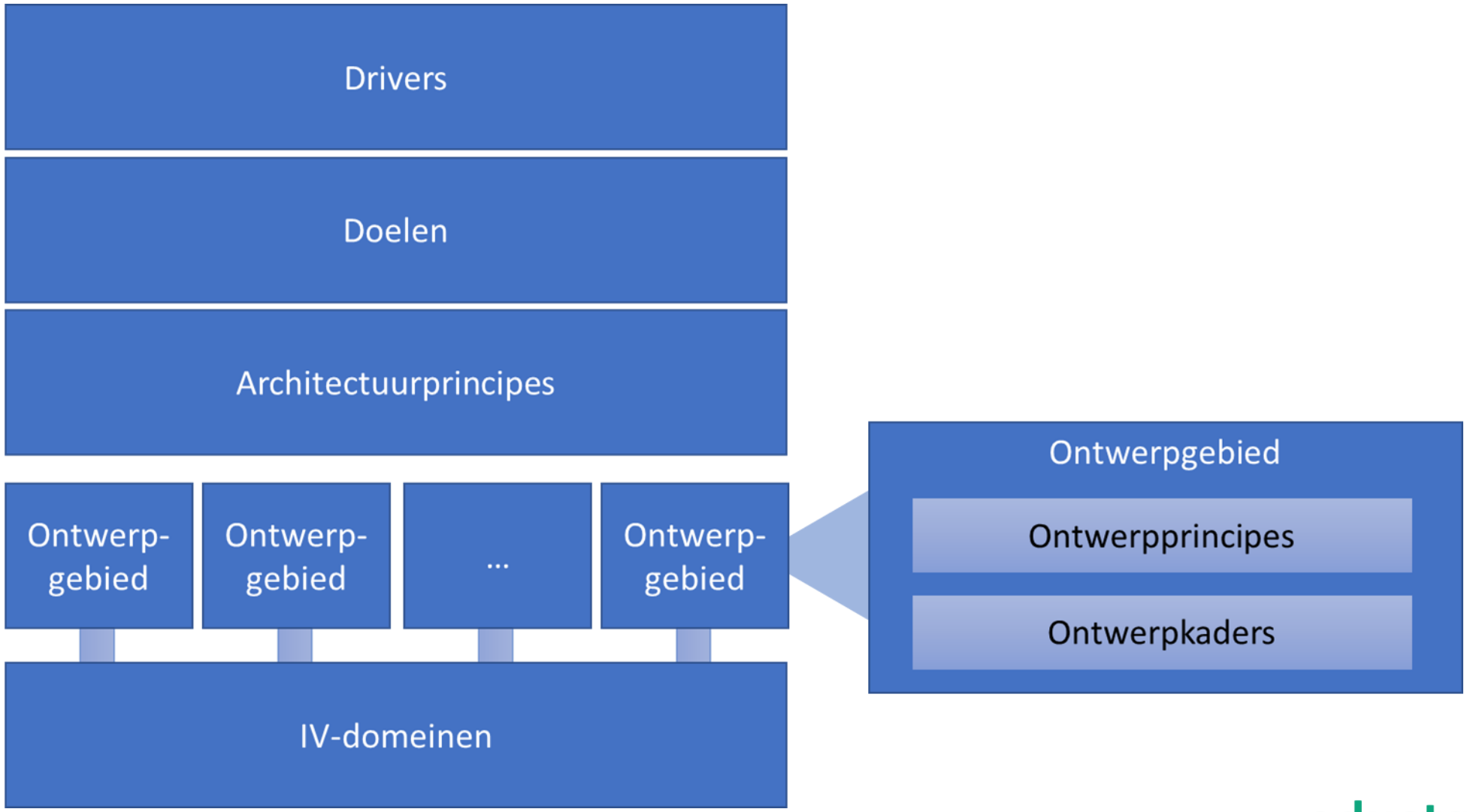
Huidige structuur van Doelen, Principes, Ontwerpkaders



- Geeft onvoldoende invulling aan de onderlinge samenhang en overlap tussen de IV-domeinen.
- Doelen maken niet alle relevante concerns zichtbaar
- (Nu al) behoorlijk veel ontwerpgebieden.

edustandaard

Nieuwe structuur van Doelen, Principes, Ontwerpgebieden

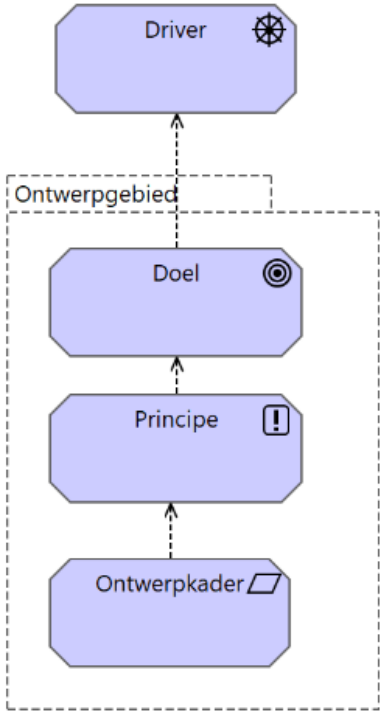


Voorbeelden van…

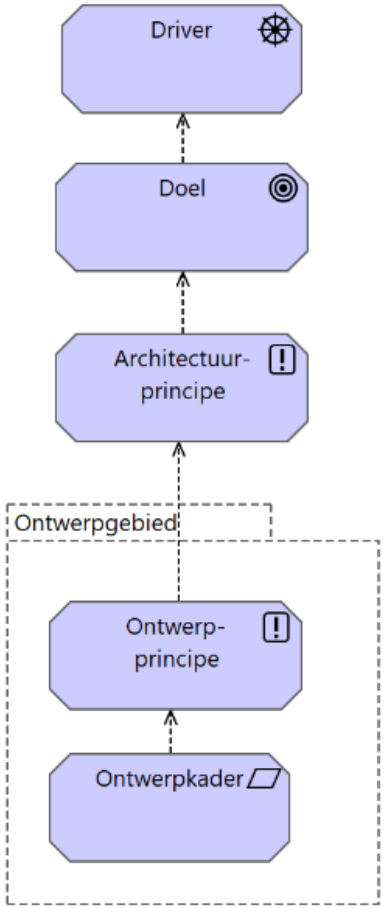
- Drivers
  - AVG
  - Regie op gegevens
  - Leven lang ontwikkelen
  - …
- Doelen
  - Zelfbeschikking
  - Privacy
  - Beschikbaarheid
  - Toegankelijkheid
  - …
- Architectuurprincipes
  - Gegevensbescherming
  - Dataminimalisatie
  - Doelbinding
  - Aandacht voor persoonlijke mogelijkheden en beperkingen
  - Gegevens worden niet langer bewaard dan strikt noodzakelijk
  - …

edustandaard

Aanpassing metamodel



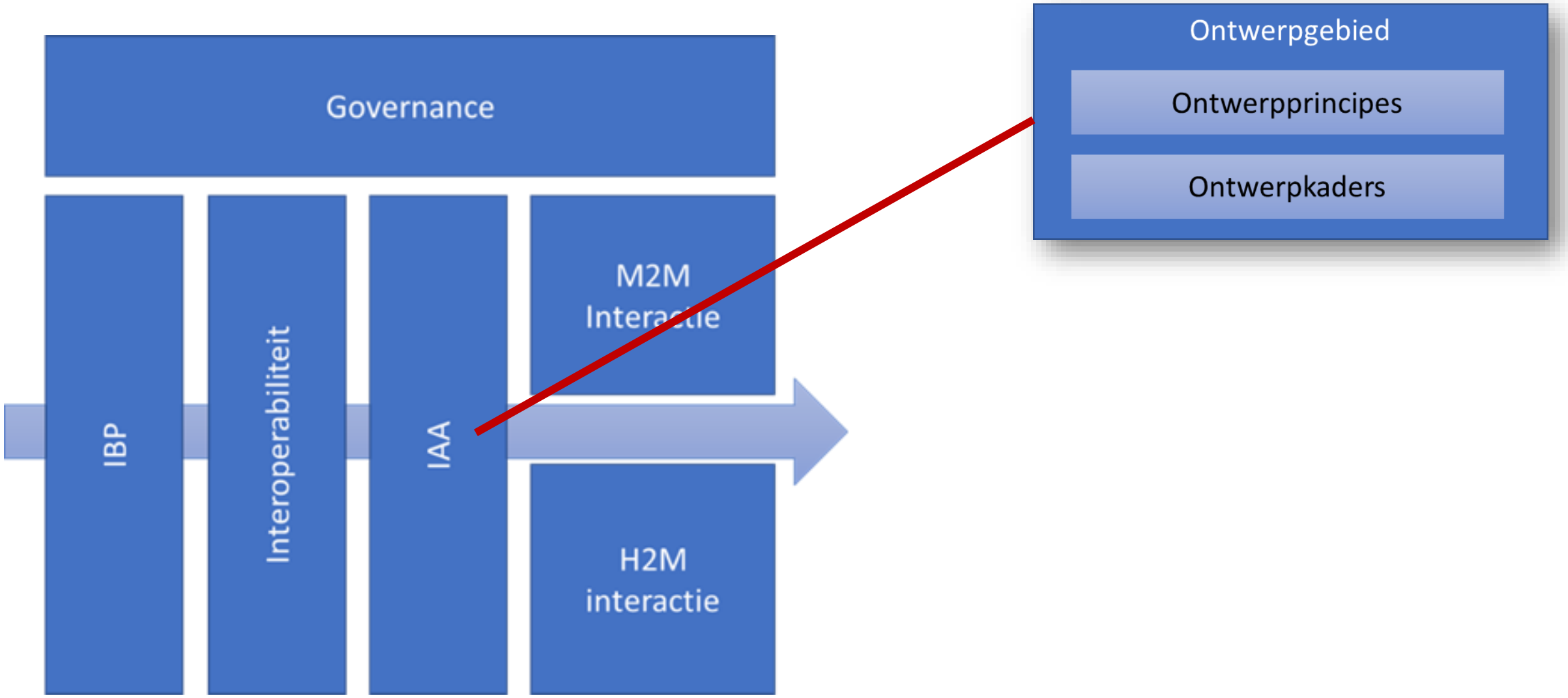
Huidig



Aangepast

edustandaard

Ontwerpgebieden



edustandaard

IV-domeinen

- Blauwdruk voor inrichting van informatievoorziening, binnen de kaders van de relevante ontwerpgebieden
- Drie ontwerpgebieden:
  - Inrichten gegevensinteractie
  - Inrichten Identity & Access Management (IAM)
  - Inrichten IBP-maatregelen

Principes en ontwerpkaders Toegang (v0.82)

- H3 - Principes
  - Gekwalificeerde digitale identiteit
  - Gebruikers kunnen een eigen decentrale identiteit gebruiken
  - Dataminimalisatie
  - Doelbinding
  - Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk
  - Bescherming gegevens
  - Zelfbeschikking
  - Gebruikersvriendelijk

Principes en ontwerpkaders Toegang (v0.82)

- Doelen
  - Zelfbeschikking
  - Gebruikersvriendelijk
- Architectuurprincipes
  - Dataminimalisatie
  - Doelbinding
  - (Persoons)gegevens worden niet langer bewaard dan strikt noodzakelijk
  - Bescherming gegevens
- Ontwerpprincipes IAA
  - Gekwalificeerde digitale identiteit
  - Gebruikers kunnen een eigen decentrale identiteit gebruiken

edustandaard

Principes en ontwerpkaders Toegang (v0.82)

- H4 - Ontwerpkaders
  - Een gekwalificeerde digitale identiteit stelt eisen aan een afsprakenstelsel
  - Maak in ontwerp transparant hoe privacy is geborgd
  - Maak uitvoering transparant
  - Modulaire architectuurkaders door het gebruik van toepassingspatronen
  - Inrichten authenticatiefunctie
  - Inrichten identiteitenbeheer
  - Inrichten authenticatiemiddelenbeheer

Principes en ontwerpkaders Toegang (v0.82)

- Architectuurprincipes
  - Modulaire architectuurkaders door het gebruik van toepassingspatronen
- Ontwerpprincipes IAA
  - Afsprakenstelsel voor toegang (*“Een gekwalificeerde digitale identiteit stelt eisen aan een afsprakenstelsel”*)
- Ontwerpkaders IAA
  - Maak in ontwerp transparant hoe privacy is geborgd
  - Maak uitvoering transparant
- IV-domeinen
  - Inrichten authenticatiefunctie
  - Inrichten identiteitenbeheer
  - Inrichten authenticatiemiddelenbeheer

edustandaard

Aanvullende ontwerpkaders

(OP) Gebruikers kunnen een eigen decentrale identiteit gebruiken.

Implicaties	• Een persoon heeft tenminste één digitale identiteit nodig, maar kan desgewenst ook meerdere digitale identiteiten verkiezen te gebruiken. • De digitale identiteit is niet alleen geschikt is voor het omgaan met attributen, maar ook bruikbaar is voor de betreffende persoon (denk bijvoorbeeld aan slechtzienden/slechthorenden, niet-Nederlands sprekenden, etc.). • Voor personen die voor het onderwijsdomein relevante rollen vervullen moet duidelijk zijn welke attributen beschikbaar worden gesteld voor deze rol. Het gaat dan niet alleen gaan over syntax en semantiek, maar ook over andere zaken die van belang zijn voor de personen of systemen die deze gegevens gebruiken[1], bijvoorbeeld om vast te kunnen stellen of zulke gegevens voor een specifiek doel valide zijn[2]. • Partijen die deze gegevens willen gebruiken voor een specifiek doel moeten nadenken over (a) de criteria waar die gegevens aan moeten voldoen om valide te zijn om voor dat doel te worden gebruikt, en (b) op welke

- Ontwerpkaders:
  - De digitale identiteit is bruikbaar voor de persoon
  - Een persoon heeft minstens één digitale identiteit

edustandaard

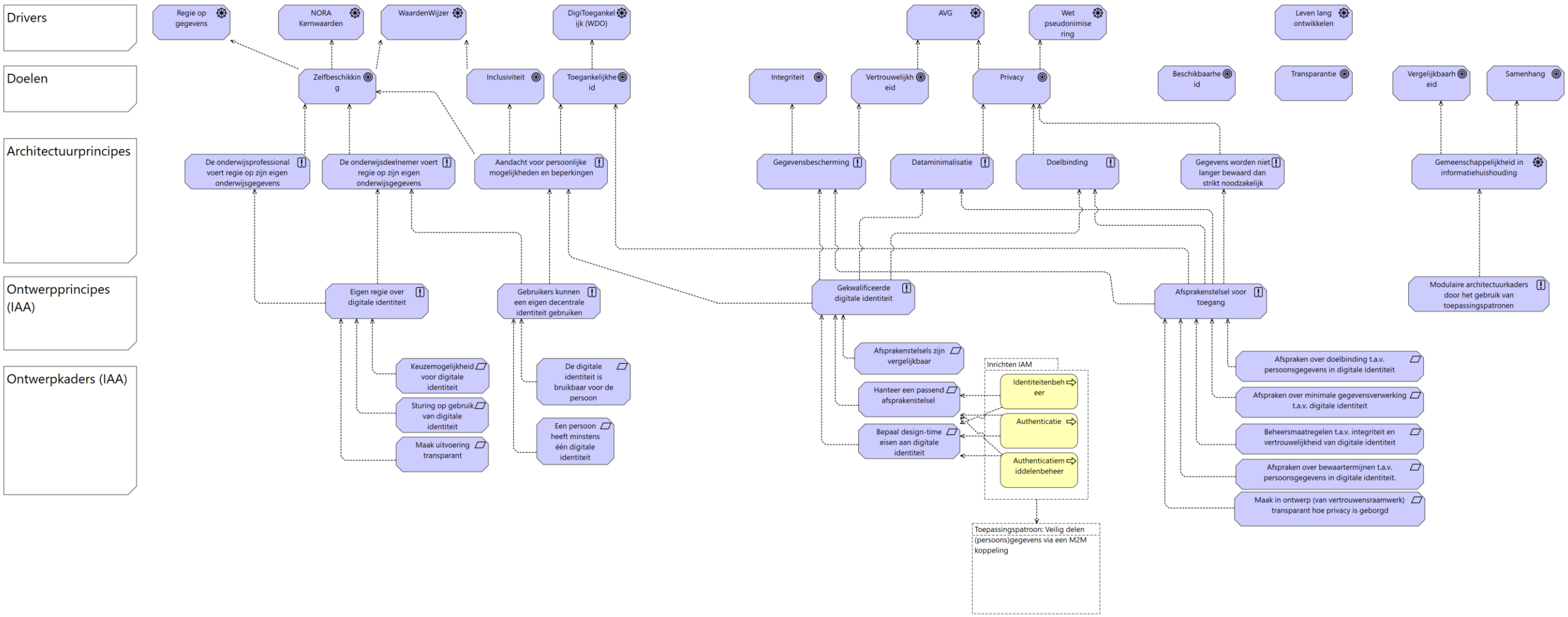
Aanvullende ontwerpkaders

Principe	Gekwalificeerde digitale identiteit[3]
Omschrijving	Elke entiteit die betrokken is bij toegang heeft (tenminste) een (gekwalificeerde) identiteit. Met gekwalificeerd wordt bedoeld dat wordt voldaan aan de eisen die het afsprakenstelsel stelt. Het kan een digitale identiteit van een natuurlijk persoon, rechtspersoon of vestiging betreffen. Voor een natuurlijk persoon kan dit een identifier en/of attribuut zijn, maar kan ook een digitaal paspoort (elektronische attestering van een attribuut) of machtiging zijn. De gekwalificeerde digitale identiteit moet gebruikt kunnen worden voor elektronische attestering van een attribuut of machtiging.
Rationale	Nodig voor ketenbrede toegankelijkheid
Implicaties	• Om (runtime) te besluiten of de digitale identiteit op een geldige (valide) manier kan worden verwerkt tot een resultaat, moet de dienstverlener (design-time) de eisen aan de digitale identiteit vaststellen, bijvoorbeeld op basis van een risicoanalyse. • De eisen aan de digitale identiteit zijn randvoorwaarden bij de keuze voor een passend afsprakenstelsel. • Het kan zijn dat de dienstverlening niet uniform is en niet alle contexten door één afsprakenstelsel ondersteund kan worden. Er kunnen dus meerdere afsprakenstelsels zijn. • Het bestaan van meerdere afsprakenstelsels voor digitale identiteiten vereist dat de dienstverlening gebruik kan maken van een uniform selectieproces en criteria.

- Ontwerpkaders:
  - Bepaal design-time eisen aan de digitale identiteit
  - Afsprakenstelsels zijn vergelijkbaar
  - Hanteer een passend afsprakenstelsel

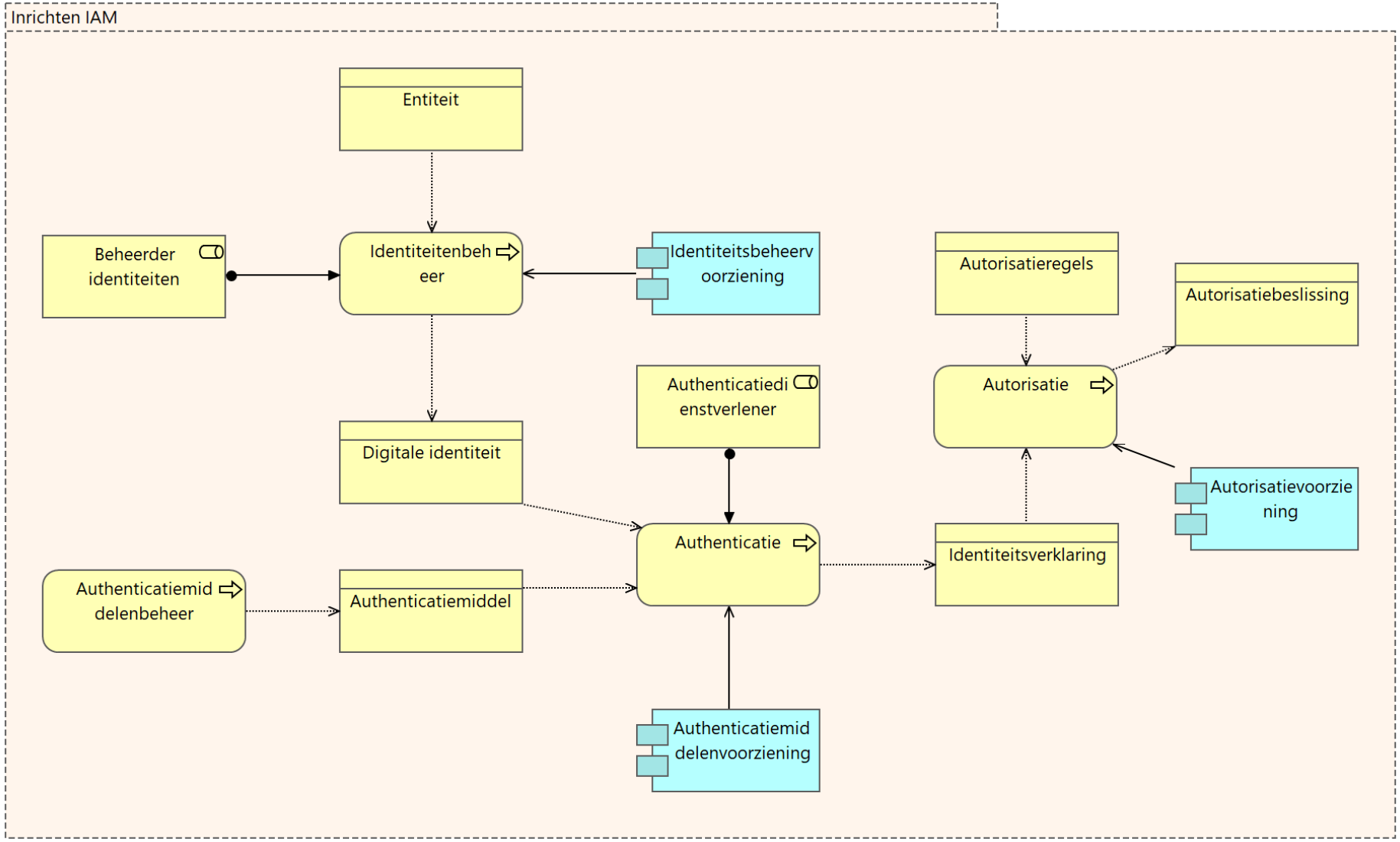
edustandaard

Ontwerpgebied IAA (obv Principes en ontwerpkaders Toegang v0.82)



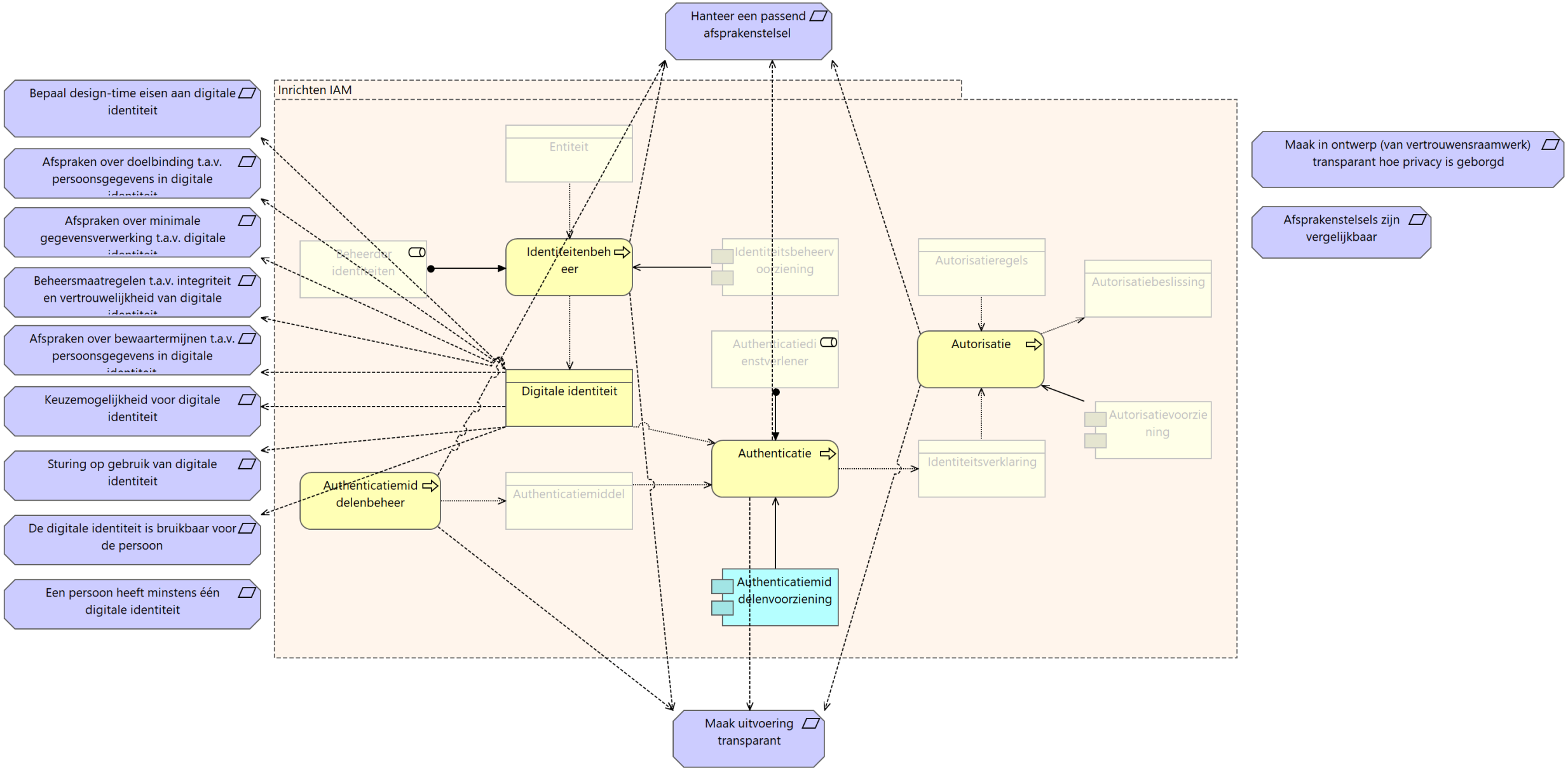
edustandaard

IV-domein Inrichten IAM

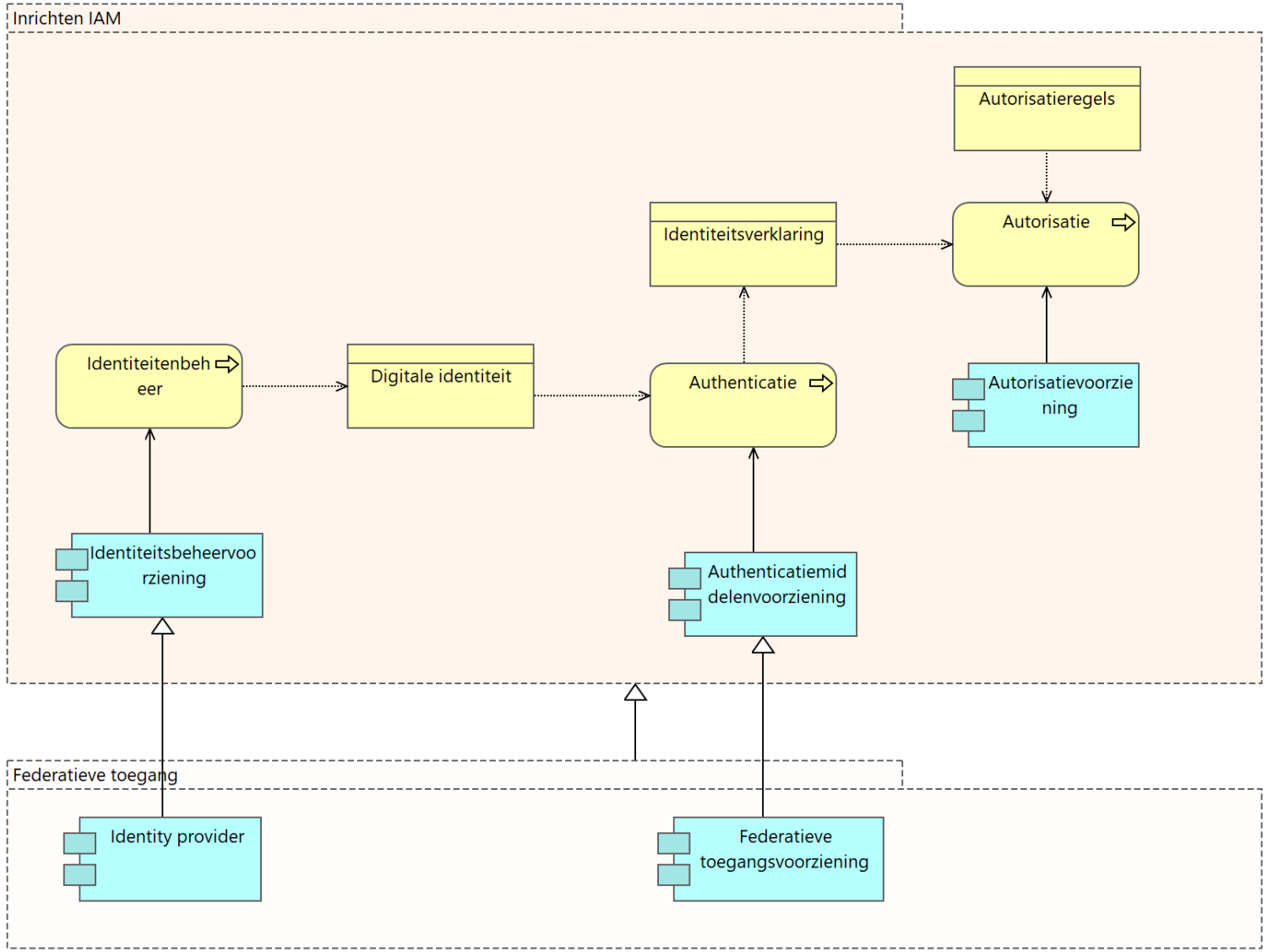


edustandaard

IV-domein Inrichten IAM



Toepassingspatronen (voorbeeld)



edustandaard