IAM-Architectuur

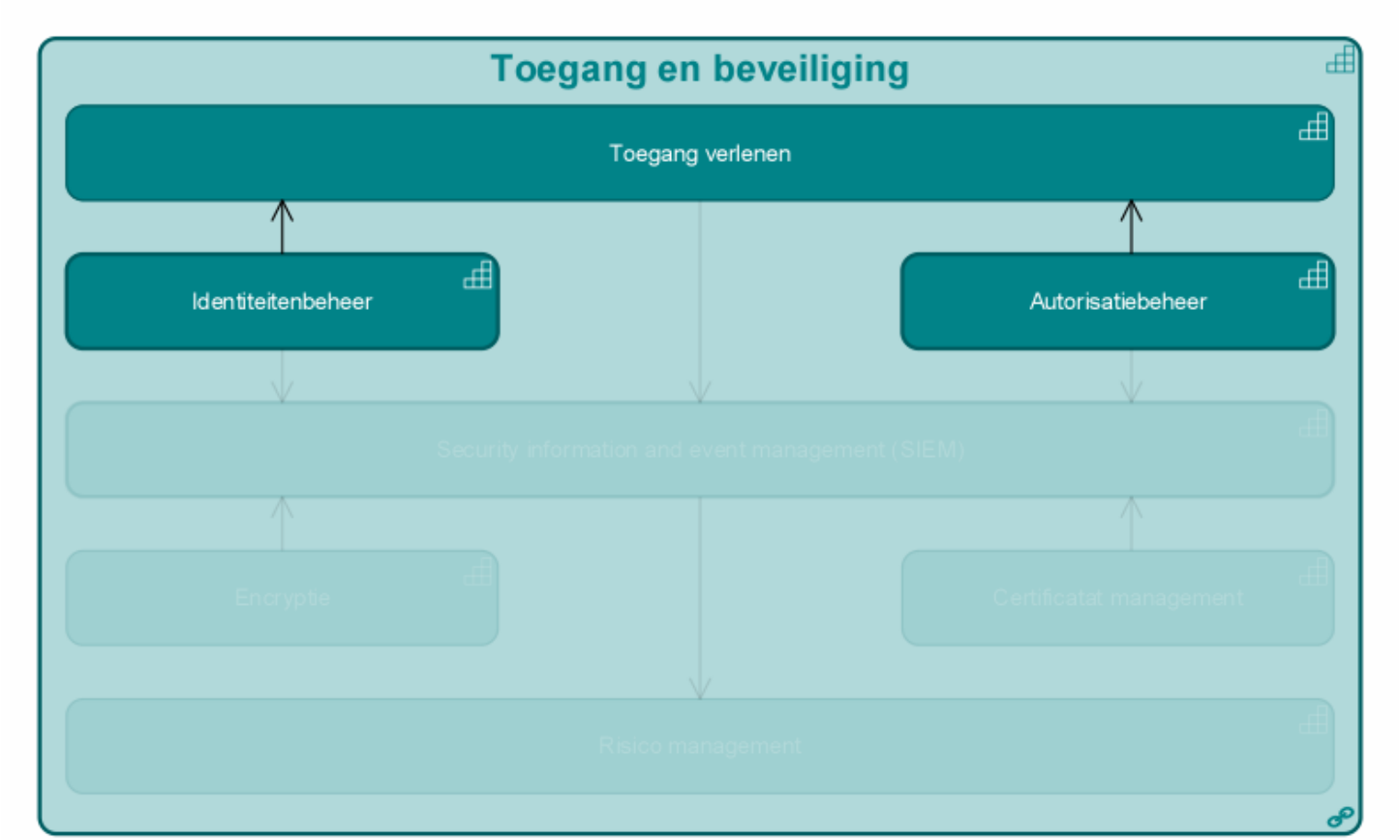
Colofon
Uitgave: Dienst IT en Inkoopcentrum Fontys Hogescholen
Adres: Postbus 347, 5600 AH Eindhoven
Datum: 16 december 2022

Versie: 1.0

Table of contents

01. IAM Scope ... 3
Toegang en beveiliging ... 4
01.1 IAM Concept ... 5
Entiteit ... 6
Resource ... 7
01.2 Level of Assurance ... 8
Attribuut ... 9
02. IAM Bedrijfsfuncties ... 10
Toegang verlenen ... 10
Identiteitenbeheer ... 10
Autorisatiebeheer ... 11
04. IAM Applicatiefuncties ... 12
Toegang verlenen ... 12
Identiteitenbeheer ... 12
Autorisatiebeheer ... 13
04.1 IAM Single Sign On ... 14
Identity Provider (IdP) ... 15
Resource: Toegang verlenen ... 15
Toegang verlenen ... 15
05. Processen ... 16
05.1 Proces Onboarden ... 16
05.2 Proces Offboarden ... 17
05.3 Proces Wijzigen ... 19
05.4 Proces Autorisatieregelbeheer ... 20
05.5 Proces Inrichten SSO ... 21
05.6 Proces Aanvragen toegang ... 22
05.7 Proces Toegang verlenen ... 23
06. IAM niveaus ... 24
07. IAM Doel architectuur ... 25
08. Toegepaste principes ... 26
ISP Principes ... 26
IAM Principes ... 27

01. IAM Scope



Total view 01. IAM Scope

Identity and Access Management (IAM) is vrij vertaald het beheer om ervoor te zorgen dat de juiste "identiteiten" (denk daarbij aan personen of computers), voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste faciliteiten. IAM bestaat uit de volgende onderdelen:

- Toegang verlenen: Het daadwerkelijk toegang geven tot resources door de identiteit vast te stellen, de identiteit te verifiëren (authentiseren) en autorisatie van de identiteit te controleren.

.

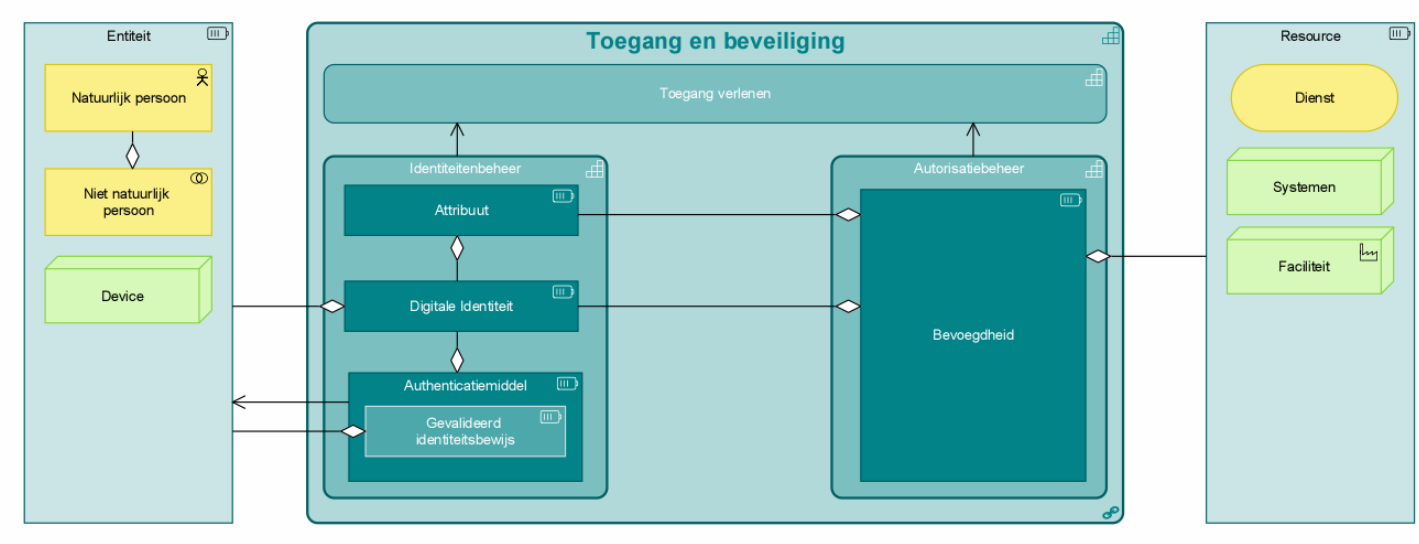
- Identiteitenbeheer: Identiteitenbeheer betreft de "levenscyclus" van identiteiten: vanaf het vaststellen en valideren van de entiteit (persoon, organisatie, apparaat) en initieel creëren van een identiteit tot het uiteindelijk vervallen ervan t, inclusief het gecontroleerd registreren, verstrekken en innemen van authenticatiemiddelen bij een identiteit.

- Autorisatiebeheer: Autorisatiebeheer betreft de “levenscyclus” van bevoegdheden: vanaf het onderkennen (ontstaan en eventueel aanpassen), naar het toekennen aan digitale identiteiten en het verklaren daarvan, tot aan het intrekken (verwijderen) van bevoegdheden. Doorgaans wordt dit ook wel Bevoegdhedenbeheer of Access management genoemd. Uitgangspunt hierbij is, dat met bepaalde “regels” wordt bepaald wat mag (of wat niet mag) en dat op het moment dat ergens toegang tot wordt gevraagd, dat dan wordt gecontroleerd of dat volgens die regels mag.

Toegang en beveiliging

Toegang en beveiliging - Documentation	
Name	**Documentation**
Toegang verlenen	Het daadwerkelijk toegang geven tot resources door de identiteit vast te stellen, de identiteit te verifiëren (authentiseren) en autorisatie van de identiteit te controleren.
Identiteitenbeheer	Identiteitenbeheer betreft de "levenscyclus" van identiteiten: vanaf het vaststellen en valideren van de entiteit (persoon, organisatie, apparaat) en initieel creëren van een identiteit tot het uiteindelijk vervallen ervan, inclusief het gecontroleerd registreren, verstrekken en innemen van authenticatiemiddelen bij een identiteit.
Autorisatiebeheer	Autorisatiebeheer betreft de “levenscyclus” van bevoegdheden: vanaf het onderkennen (ontstaan en eventueel aanpassen), naar het toekennen aan digitale identiteiten en het verklaren daarvan, tot aan het intrekken (verwijderen) van bevoegdheden. Uitgangspunt hierbij is, dat met bepaalde autorisatieregels wordt bepaald wat mag (of wat niet mag) en dat op het moment dat ergens toegang tot wordt gevraagd, dat dan wordt gecontroleerd of dat volgens die regels mag.

01.1 IAM Concept



Total view 01.1 IAM Concept	
Het objectmodel voor IAM identificeert welke concepten uit de reële wereld relevant zijn voor het onderwerp IAM, en het beschrijft de relaties tussen de objecten. De figuur is een architectuur model van de concepten en hun relaties.	
References	NORA: Begrippen IAM

01.1 IAM Concept - Documentation	
Name	**Documentation**
Entiteit	Een herkenbaar en onderscheidbaar iets dat relevant is voor IAM en waarbij een Digitale Identiteit kan behoren. · Een Entiteit kan zowel een fysieke als logische form hebben. Voorbeelden van Entiteiten zijn, een persoon, een organisatie, een fysiek apparaat, een simkaart, een softwaretoepassing en een proces dat draait op een fysiek apparaat. · Er is een onderscheid tussen 3 soorten Entiteiten: Natuurlijke Personen, Niet-Natuurlijke personen en Devices.
Resource	Een fysieke component of een eenheid van informatie waartoe een Entiteit toegang zou kunnen krijgen. Een Resource kan worden gezien als een Entiteit; Resources kunnen dus een Digitale Identiteit hebben.

Entiteit

Entiteit - Documentation	
Name	**Documentation**
Natuurlijk persoon	Een persoon van vlees en bloed die rechten en plichten kan hebben · Er zijn meerdere soorten te onderkennen, een daarvan is het onderscheid tussen personen die ingezetene zijn van Nederland en zij dit dat niet zijn
Niet natuurlijk persoon	Een Niet-Natuurlijk Persoon is een Rechtspersoon of een samenwerkingsverband van Natuurlijk Personen (Natuurlijk persoon). Een Rechtspersoon is een door de wet mogelijk gemaakte entiteit, die drager kan zijn van rechten en plichten. · Een BV, NV, Stichting en vereniging zijn voorbeelden van een Rechtspersoon · Een Maatschap en VOF zijn samenwerkingsverbanden die geen Rechtspersoon zijn. Een functioneel account handelt namens een Niet Natuurlijk Persoon en dient dan ook als zodanig toegepast te worden. De 01.2 Level of Assurance bepaalt de mate waarmee een functioneel accout zich moet kunnen identificeren.
Device	Een fysiek apparaat, software, of de draaiende geautomatiseerde processen. · Voorbeeld van Devices zijn een computer, telefoon, een app op een smartphone of een digitale deurbel met camera functie · Devices hebben een Digitale Identiteit nodig voor Informatiebeveiligingsfuncties.

Identiteitenbeheer

Identiteitenbeheer - Documentation	
Name	**Documentation**
Attribuut	Een enkelvoudig of samengesteld informatie-element dat onderdeel is van een Digitale Identiteit en relevant is voor Bevoegdheid. Voorbeelden van attributen zijn: · Naam, Ingangsdatum identiteit, Expiratiedatum, Geboortedatum, e-mailadres, contactgegevens · Mate van betrouwbaarheid: Identity Assurance Level · Organisatieonderdelen waartoe een Digitale Identiteit behoort; · De rollen van de Digitale Identiteit binnen de organisatie (manager, docent, examinator, surveillant, student); · De studies voor welke een Digitale Identiteit is ingeschreven.
Digitale Identiteit	Een Digitale Identiteit is een verzameling gegevens die een digitale representatie zijn van een Entiteit binnen een bepaald digitaal toepassingsgebied. Een Entiteit kan meerdere Digitale Identiteiten hebben (binnen dezelfde of andere contexten) Een digitale identiteit bevat eigenschappen die als Attribuut worden opgeslagen. Attributen zijn veranderlijk in tegenstelling tot het ID van de digitale identiteit (bijvoorbeeld userid, dit kan na aanmaken niet meer gewijzigd worden (IAM-P01: Interne identiteit is uniek en onveranderlijk).
Authenticatiemiddel	Een fysiek of digitaal middel op grond waarvan authenticatie van een Entiteit kan plaatsvinden; i.e. een drager van een Digitale Identiteit met een vastgesteld betrouwbaarheidsniveau. Een Identiteitsbewijs wordt met een uitgifte proces door een middelenuitgever verstrekt aan de Entiteit. · Het betrouwbaarheidsniveau wordt bepaald door de processen die bij de uitgifte van het middel zijn gevolgd. · Een Identiteitsbewijs bevat een Identifier van de gebruiker, de uitgever van het middel, en optioneel extra attributen. · Certificaten en soft-tokens (bijv. OAuth, SAML of Kerberos) zijn voorbeelden van digitale Identificatiemiddelen. Binnen de HOSA is dit ook bekend als verifieerbare credential.

Authenticatiemiddel

Authenticatiemiddel - Documentation	
Name	**Documentation**
Gevalideerd identiteitsbewijs	Een fysiek of digitaal middel op grond waarvan authenticatie van een gebruiker kan plaatsvinden; i.e. een drager van een Digitale Identiteit met een vastgesteld betrouwbaarheidsniveau. Een Identiteitsbewijsw ordt met een uitgifte proces door een externe middelenuitgever, zoals de overheid, verstrekt aan de Entiteit.

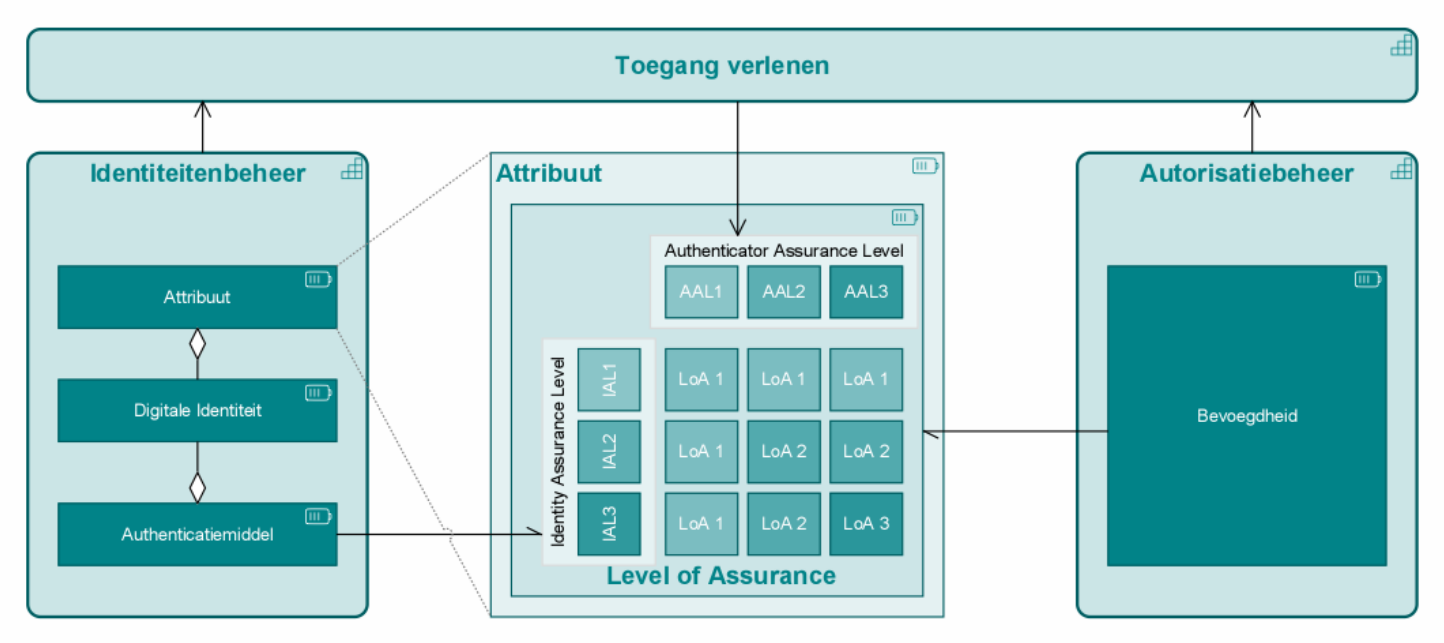
Autorisatiebeheer

Autorisatiebeheer - Documentation	
Name	**Documentation**
Bevoegdheid	Een toestemming van een Entiteit of danwel zelf, danwel als vertegenwoordiger van een belanghebbende, om toegang te krijgen tot een Resource waarbij voorwaarden kunnen worden gedefinieerd op de attributen van de Digitale Identiteit. · Een Autorisatie is randvoorwaardelijk voor het krijgen van toegang, maar niet voldoende. · Autorisaties kunnen als informatie object zijn vastgelegd, maar dat hoeft niet altijd het geval te zijn; bijvoorbeeld als deze bij via autorisatieregels bepaald is.

Resource

Resource - Documentation	
Name	**Documentation**
Systemen	En systeem representeert een digitale of fysieke resources ten behoeve van het faciliteren, verwerken of interacteren met andere digitale of fysieke resources. Dit zijn bijvoorbeeld: · Applicaties · Computers · Infrastructuur · IoT
Faciliteit	Een faciliteit representeert een fysieke structuur of een omgeving. Voorbeelden hiervan zijn: · Gebouwen · Parkeerplaatsen
Dienst	Een dienst is een vooraf afgesproken activiteit die de aanbieder verricht ter ondersteuning en in opdracht van de afnemer.

01.2 Level of Assurance



Total view 01.2 Level of Assurance	
Level of Authentication geeft de mate van zekerheid weer waarmee een claim van een identiteit tijdens het authenticatieproces kan worden vertrouwd als 'echte' identiteit.	
References	NORA: Begrippen IAM

01.2 Level of Assurance - Documentation	
Name	**Documentation**
Toegang verlenen	Het daadwerkelijk toegang geven tot resources door de identiteit vast te stellen, de identiteit te verifiëren (authentiseren) en autorisatie van de identiteit te controleren.
Identiteitenbeheer	Identiteitenbeheer betreft de "levenscyclus" van identiteiten: vanaf het vaststellen en valideren van de entiteit (persoon, organisatie, apparaat) en initieel creëren van een identiteit tot het uiteindelijk vervallen ervan, inclusief het gecontroleerd registreren, verstrekken en innemen van authenticatiemiddelen bij een identiteit.
Attribuut	Een enkelvoudig of samengesteld informatie-element dat onderdeel is van een Digitale Identiteit en relevant is voor Bevoegdheid. Voorbeelden van attributen zijn: · Naam, Ingangsdatum identiteit, Expiratiedatum, Geboortedatum, e-mailadres, contactgegevens · Mate van betrouwbaarheid: Identity Assurance Level · Organisatieonderdelen waartoe een Digitale Identiteit behoort; · De rollen van de Digitale Identiteit binnen de organisatie (manager, docent, examinator, surveillant, student); · De studies voor welke een Digitale Identiteit is ingeschreven.
Autorisatiebeheer	Autorisatiebeheer betreft de “levenscyclus” van bevoegdheden: vanaf het onderkennen (ontstaan en eventueel aanpassen), naar het toekennen aan digitale identiteiten en het verklaren daarvan, tot aan het intrekken (verwijderen) van bevoegdheden. Uitgangspunt hierbij is, dat met bepaalde autorisatieregels wordt bepaald wat mag (of wat niet mag) en dat op het moment dat ergens toegang tot wordt gevraagd, dat dan wordt gecontroleerd of dat volgens die regels mag.

Attribuut

Attribuut - Documentation	
Name	**Documentation**
Level of Assurance	Level of Authentication geeft de mate van zekerheid weer waarmee een claim van een identiteit tijdens het authenticatieproces kan worden vertrouwd als 'echte' identiteit.

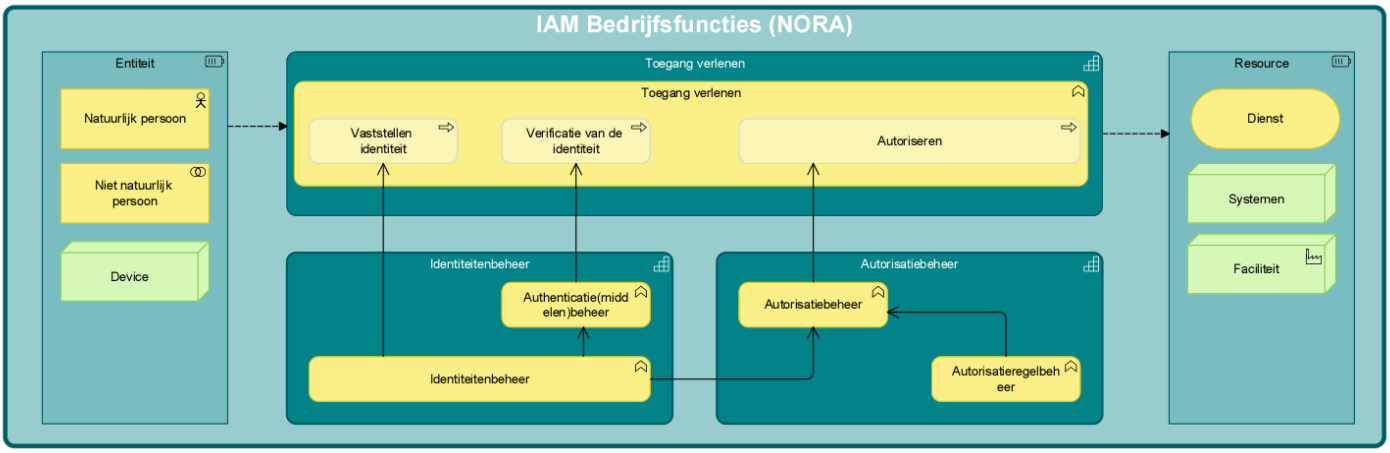
Level of Assurance

Level of Assurance - Documentation	
Name	**Documentation**
Identity Assurance Level	Identity Assurrance Level geeft de mate van vertrouwen weer, waarmee een geclaimde identiteit van een entiteit daadwerkelijk kan worden vastgesteld.
Authenticator Assurance Level	Mate van vertrouwen in het authenticatiemechanisme.
LoA 1	Minimale betrouwbaarheid
LoA 2	Beperkte betrouwbaarheid
LoA 3	Hoge betrouwbaarheid

Authenticator Assurance Level

Authenticator Assurance Level - Documentation	
Name	**Documentation**
AAL1	Enig vertrouwen in het authenticatiemechanisme. Denk hierbij aan een wachtwoord of de foto op de Fontys kaart.
AAL2	Hoog vertrouwen in het authenticatiemechanisme, hierbij is in ieder geval kennis en bezig nodig. Denk hierbij aan de combinatie van Biometrische gegevens en pin, Multi Fact Authentication (MFA) via een App of een SMS.
AAL3	Zeer Hoog vertrouwen in het authenticatiemechanisme.

02. IAM Bedrijfsfuncties



Total view 02. IAM Bedrijfsfuncties	
Binnen Fontys en conform ISP-P06 Standaard beperkte toegang en veilige instellingen moet de toegang tot resources, waaronder informatie, beperkt worden tot personen of systemen die geautoriseerd zijn om de informatie in te zien of te kunnen wijzigen. Daarbij wordt veelal onderscheid gemaakt naar onderwijsdeelnemers, medewerkers (zowel intern als extern), (zaken)partners en individuen in andere rollen. De uitwerking van het IAM-concept is gebaseerd op bedrijfsfuncties en bedrijfsprocessen: · Identiteitenbeheer valt uiteen in een functie Identiteitenbeheer, waarin de identiteiten met de attributen beheerd worden en een functie authenticatie(middelen)beheer waarin middelen zoals tokens en Fontys-pasjes beheerd worden; · Autorisatiebeheer valt uiteen in een functie autorisatieregelbeheer, waarin het beleid van Fontys uitgedrukt is in autorisatieregels en een functie Autorisatiebeheer, waarin de (digitale) identiteit geautoriseerd wordt op basis van autorisatieregels. Dus het toepassen van autorisatie. · Toegang verlenen bestaat uit één functie Toegang verlenen met daarin opgenomen drie processen. Deze processen beschrijven sequentieel het identificatie-, authenticatie en autorisatieproces.	
References	NORA: Begrippen IAM

Toegang verlenen

Toegang verlenen - Documentation	
Name	**Documentation**
Vaststellen identiteit	Het proces om een Entiteit binnen een context te onderscheiden van andere Entiteiten op basis van gepresenteerde of geobserveerde attributen
Verificatie van de identiteit	Het aantonen dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft: ben je het ook echt? Authenticatie noemt men ook wel verificatie van de identiteit.
Autoriseren	Het proces om te beslissen of een Entiteit op grond van een Authenticatiemiddel, Identiteitsverklaring, of een Machtiging toegang krijgt tot een Resource. De beslissing wordt mede gebaseerd op het bij de resource behorende Autorisatieregels en omgevingsfactoren.

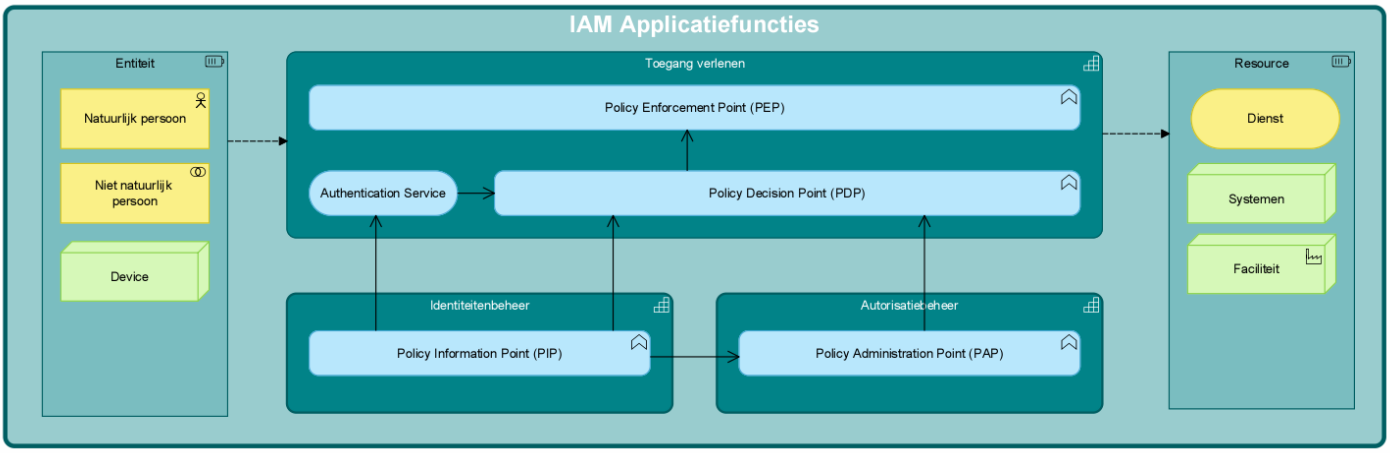
Identiteitenbeheer

Identiteitenbeheer - Documentation	
Name	**Documentation**
Identiteitenbeheer	De functie Identiteitenbeheer brengt Digitale identiteiten tot stand voor Entiteiten (zoals Personen). Het beheer betreft ook de attributen die aan de Digitale entiteit zijn gerelateerd. Wanneer nodig zorgt de functie eveneens voor het actualiseren daarvan.
Authenticatie(middelen) beheer	De functie Authenticatie(middelen)beheer voorziet in Authenticatiemiddelen voor Digitale identiteiten. Voorbeelden van authenticatiemiddelen zijn: · De Fontyskaart · Mobiele telefoon · Een (digitale) token

Autorisatiebeheer

Autorisatiebeheer - Documentation	
Name	**Documentation**
Autorisatiebeheer	De functie Autorisatiebeheer zorgt voor een formele (en actuele) vastlegging van Autorisaties, die vanuit de Digitale identiteit van de Belanghebbende worden toegekend aan de Digitale identiteit van de Vertegenwoordiger. De autorisatie is veelal beperkt tot een Resource/een reeks Resources. De autorisatie kan voor beperkte duur gelden, of gelden totdat die wordt ingetrokken.
Autorisatieregelbeheer	De functie autorisatieregelbeheer formuleert de Autorisatieregels die worden toegepast bij het nemen van Autorisatiebeslissingen voor een Resource.

04. IAM Applicatiefuncties



Total view 04. IAM Applicatiefuncties	
Bij het beschrijven van Identity & Acces Management binnen Fontys worden zeven onderdelen onderscheiden, waarbij het Identificeren en Authentiseren als één applicatiefunctie is gedefinieerd. Deze applicatiefunctie is verder uitgewerkt in Identificeren en Authentiseren (IA). Autorisaties worden beheerd via een Policy Administration Point (PAP). Deze draagt zorg voor het gestructureerd vastleggen van autorisaties op basis van policies én toegekende autorisatie-aanvragen. Identiteiten worden beheerd via de functie en stelt in staat om authenticatiemiddelen uit te geven aan identiteiten. De in IB, AB en PAP geregistreerde informatie wordt geleverd (provisioning) aan één of meerdere geautoriseerde afnemers, Policy Information Point (PIP) genaamd. Een PIP stelt deze informatie beschikbaar bij het verlenen van toegang. Het verlenen van toegang aan een Entiteit tot een Resource verloopt altijd via een Policy Enforcement Point (PEP). De PEP regisseert het verlenen van toegang. Eerst controleert de PEP of en via welke Identity Provider ((idP) de identiteit van de entiteit kan worden vastgesteld en geverifieerd. De idP vult de applicatiefunctie IA uit. Na het vaststellen van de identiteit valideert de PEP het autorisatieverzoek via een Policy Decision Point (PDP). Afhankelijk van het resultaat verleent of weigert de PEP de Entiteit toegang tot de Resource. De PEP fungeert als ware als poortwachter. De applicatiefuncties IA en PDP raadplegen de PIP, waarin de informatie over identiteiten, authenticatiemiddelen, autorisaties en autorisatieregels zijn opgeslagen.	
References	NORA: Begrippen IAM

Toegang verlenen

Toegang verlenen - Documentation	
Name	**Documentation**
Policy Enforcement Point (PEP)	Policy Enforcement Point (PEP) draagt zorg voor het ontvangen van een verzoek van de gebruiker en het bevragen de PDP.
Policy Decision Point (PDP)	Policy Decision Point (PDP) draagt zorg voor het beoordelen van de autorisatie aanvragen op basis van policies.
Authentication Service	Authentication Service is een service die digitale identiteiten opslaat en beheert, en op basis van deze informatie een Entiteit kan authentiseren. Autheication Service maakt een onderdeel uit van een identity provider (IdP)

Identiteitenbeheer

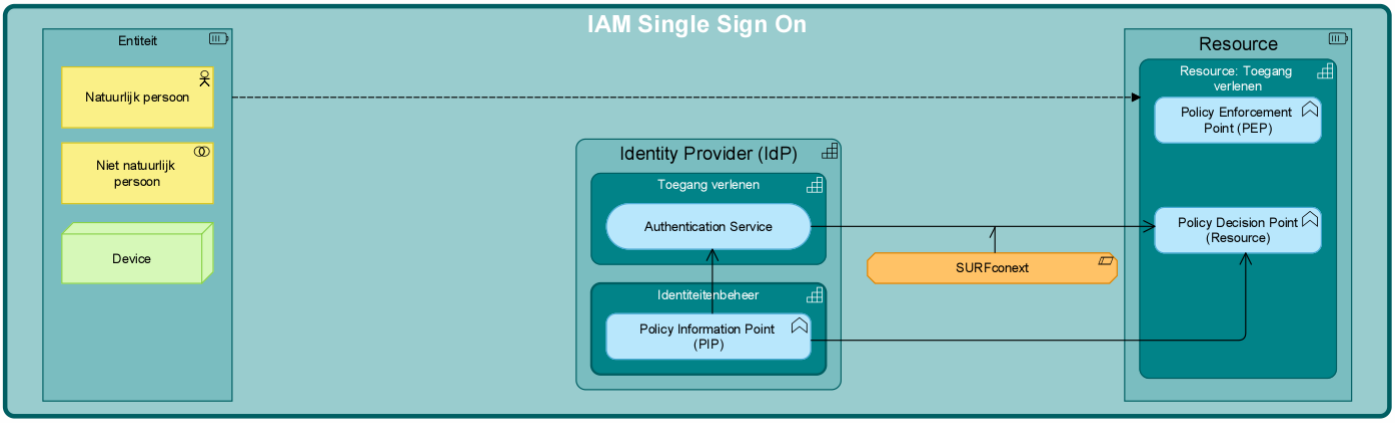
Identiteitenbeheer - Documentation	
Name	**Documentation**
Policy Information Point	Policy Information Point (PIP) draagt zorg voor het elektronisch beheren van de digitale

(PIP)	identiteiten en attributen.

Autorisatiebeheer

Autorisatiebeheer - Documentation	
Name	**Documentation**
Policy Administration Point (PAP)	Policy Administration Point (PAP) draagt zorg voor het administreren van de toegangsrechten in de vorm van policies. Op basis van policies worden autoritatieve bronnen toegang gegeven tot de gevraagde doel systemen/resources.

04.1 IAM Single Sign On



Total view 04. IAM Single Sign On	
In geval van Single Sign On is sprake van externalisering van authenticatie ofwel de Authentication Service, dat wil zeggen dat het door een centrale voorziening wordt uitgevoerd in plaats van door elke applicatie (Resource) afzonderlijk. Deze centrale voorziening wordt ook wel de Identity Provider (IdP) genoemd. De IdP beheert de Digitale Identiteit en valideert deze op verzoek van de Resource. Single Sign On binnen Fontys wordt gerealiseerd door middel van als Onderwijsstandaard. Om als applicatie (Resource) hiervan gebruik te kunnen maken is ondersteuning van de SAML of OpenID standaarde een vereiste. Een deel van de onderwijsapplicaties en CLoudapplicaties zijn geschikt gemaakt voor SURFconext, zie: https://www.surf.nl/welke-diensten-kun-je-met-surfconext-gebruiken?dst=n1724	
References	Patroon voor single sign-on

04. IAM Single Sign On - Documentation	
Name	**Documentation**
Entiteit	Een herkenbaar en onderscheidbaar iets dat relevant is voor IAM en waarbij een Digitale Identiteit kan behoren. · Een Entiteit kan zowel een fysieke als logische form hebben. Voorbeelden van Entiteiten zijn, een persoon, een organisatie, een fysiek apparaat, een simkaart, een softwaretoepassing en een proces dat draait op een fysiek apparaat. · Er is een onderscheid tussen 3 soorten Entiteiten: Natuurlijke Personen, Niet-Natuurlijke personen en Devices.
SURFconext	SURFconext koppelt Fontys als identityprovider met de dienstaanbieders. SURFconext is privacyvriendelijk en wisselt alleen de gegevens uit die echt nodig zijn.
Resource	Een fysieke component of een eenheid van informatie waartoe een Entiteit toegang zou kunnen krijgen. Een Resource kan worden gezien als een Entiteit; Resources kunnen dus een Digitale Identiteit hebben.

Identity Provider (IdP)

Identity Provider (IdP) - Documentation	
Name	**Documentation**
Toegang verlenen	Het daadwerkelijk toegang geven tot resources door de identiteit vast te stellen, de identiteit te verifiëren (authentiseren) en autorisatie van de identiteit te controleren.
Identiteitenbeheer	Identiteitenbeheer betreft de "levenscyclus" van identiteiten: vanaf het vaststellen en valideren van de entiteit (persoon, organisatie, apparaat) en initieel creëren van een identiteit tot het uiteindelijk vervallen ervan, inclusief het gecontroleerd registreren, verstrekken en innemen van authenticatiemiddelen bij een identiteit.

Resource: Toegang verlenen

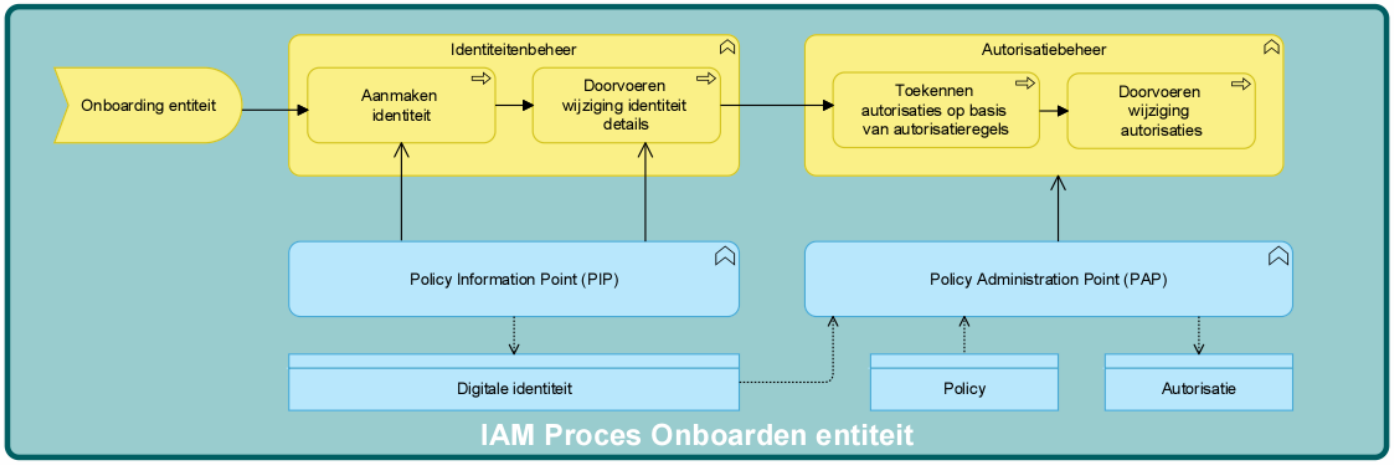
Resource: Toegang verlenen - Documentation	
Name	**Documentation**
Policy Decision Point (Resource)	Policy Decision Point (**Resource**) draagt zorg voor het beoordelen van de autorisatie aanvragen op basis van policies.

Toegang verlenen

Toegang verlenen - Documentation	
Name	**Documentation**
Authentication Service	Een identity provider (IdP) is een service die digitale identiteiten opslaat en beheert, en op basis van deze informatie een Entiteit kan authentiseren.
Policy Decision Point (PDP)	Policy Decision Point (**PDP**) draagt zorg voor het beoordelen van de autorisatie aanvragen op basis van policies.

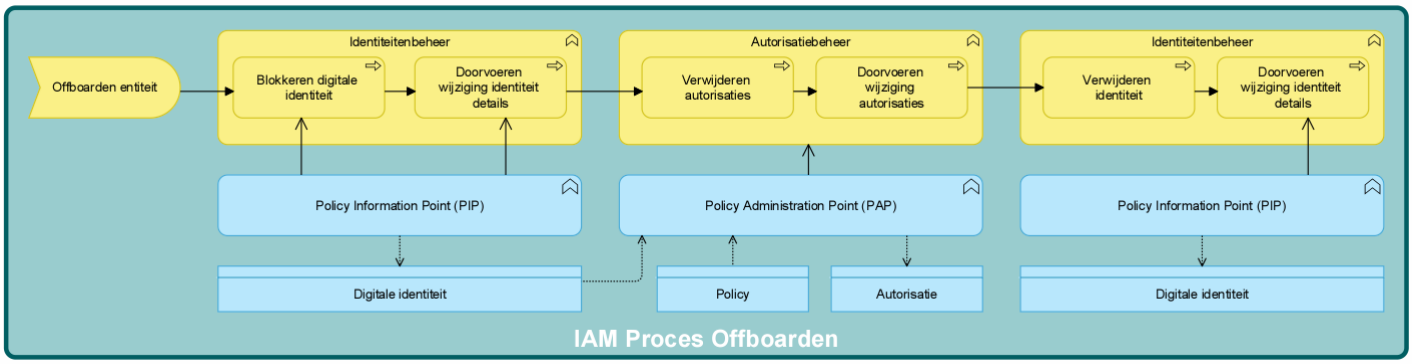
05. Processen

05.1 Proces Onboarden



05.1 Proces Onboarden - Documentation	
Name	**Documentation**
Onboarding entiteit	Het toekennen van een Identiteit, nadat de Fontys-organisatie de entiteit erkend heeft. Dit kan zijn in geval van: · Inschrijven van een onderwijsdeelnemer; · Aanstellen van een medewerker.
Identiteitenbeheer	De functie Identiteitenbeheer brengt Digitale identiteiten tot stand voor Entiteiten (zoals Personen). Het beheer betreft ook de attributen die aan de Digitale entiteit zijn gerelateerd. Wanneer nodig zorgt de functie eveneens voor het actualiseren daarvan.
Policy Information Point (PIP)	Policy Information Point (**PIP**) draagt zorg voor het elektronisch beheren van de digitale identiteiten en attributen.
Digitale identiteit	Een Digitale Identiteit is een verzameling gegevens (Attributen) die een digitale representatie zijn van een Entiteit binnen een bepaald digitaal toepassingsgebied. · Een Entiteit kan meerdere Digitale Identiteiten hebben (binnen hetzelfde of andere contexten) · Digitale Identiteiten kunnen een onderlinge samenhang hebben waarbij enkele attributen in een Afhankelijke Digitale Identiteit een-op-een gelijk zijn aan de overeenkomstige attributen in een Leidende Digitale Identiteit. Het is dan een kwaliteitseis dat deze attributen in de afhankelijke Digitale Identiteit een zekere mate gelijk moeten zijn en gelijk gehouden worden aan die in de Leidende Digitale Identiteit; denk aan verschil tussen registratie in de BRP en de gegevens in een paspoort. · Bij een Digitale Identiteit kan metadata behoren, bijvoorbeeld de organisatie die de Digitale Identiteit heeft vastgesteld en de datum waarop dat is gedaan, en de mate van betrouwbaarheid van attributen.
Autorisatiebeheer	De functie Autorisatiebeheer zorgt voor een formele (en actuele) vastlegging van Autorisaties, die vanuit de Digitale identiteit van de Belanghebbende worden toegekend aan de Digitale identiteit van de Vertegenwoordiger. De autorisatie is veelal beperkt tot een Resource/een reeks Resources. De autorisatie kan voor beperkte duur gelden, of gelden totdat die wordt ingetrokken.
Policy Administration Point (PAP)	Policy Administration Point (**PAP**) draagt zorg voor het administreren van de toegangsrechten in de vorm van policies. Op basis van policies worden autoritatieve bronnen toegang gegeven tot de gevraagde doel systemen/resources.
Autorisatie	Een toestemming van een Entiteit of danwel zelf, danwel als vertegenwoordiger van een belanghebbende, om toegang te krijgen tot een Resource waarbij voorwaarden kunnen worden gedefinieerd op de attributen van de Digitale Identiteit. · Een Autorisatie is randvoorwaardelijk voor het krijgen van toegang, maar niet voldoende. · Autorisaties kunnen als informatie object zijn vastgelegd, maar dat hoeft niet altijd het geval te zijn; bijvoorbeeld als deze bij via autorisatieregels bepaald is.

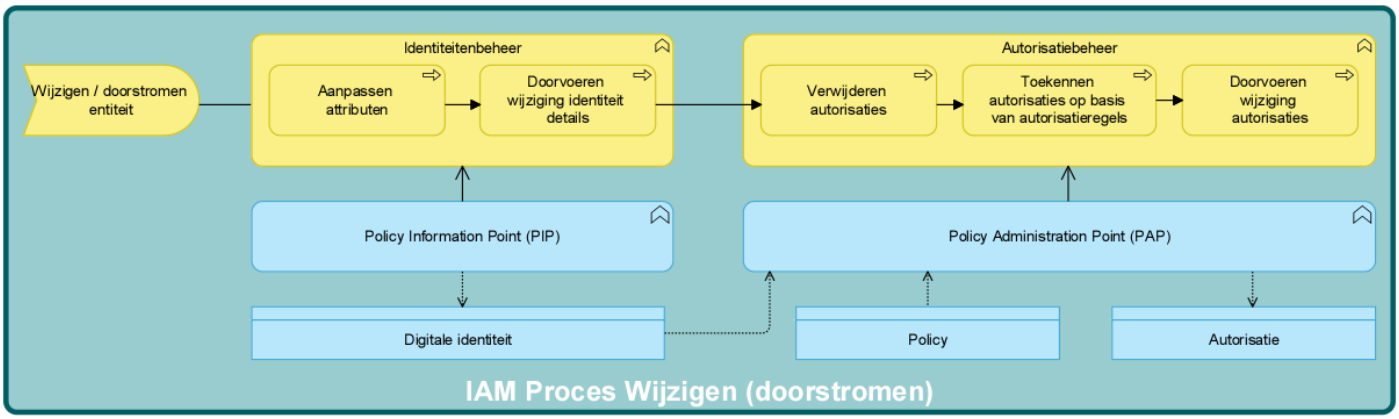
05.2 Proces Offboarden



05.2 Proces Offboarden - Documentation	
Name	**Documentation**
Identiteitenbeheer	De functie Identiteitenbeheer brengt Digitale identiteiten tot stand voor Entiteiten (zoals Personen). Het beheer betreft ook de attributen die aan de Digitale entiteit zijn gerelateerd. Wanneer nodig zorgt de functie eveneens voor het actualiseren daarvan.
Policy Information Point (PIP)	Policy Information Point (**PIP**) draagt zorg voor het elektronisch beheren van de digitale identiteiten en attributen.
Digitale identiteit	Een Digitale Identiteit is een verzameling gegevens (Attributen) die een digitale representatie zijn van een Entiteit binnen een bepaald digitaal toepassingsgebied. · Een Entiteit kan meerdere Digitale Identiteiten hebben (binnen hetzelfde of andere contexten) · Digitale Identiteiten kunnen een onderlinge samenhang hebben waarbij enkele attributen in een Afhankelijke Digitale Identiteit een-op-een gelijk zijn aan de overeenkomstige attributen in een Leidende Digitale Identiteit. Het is dan een kwaliteitseis dat deze attributen in de afhankelijke Digitale Identiteit een zekere mate gelijk moeten zijn en gelijk gehouden worden aan die in de Leidende Digitale Identiteit; denk aan verschil tussen registratie in de BRP en de gegevens in een paspoort. · Bij een Digitale Identiteit kan metadata behoren, bijvoorbeeld de organisatie die de Digitale Identiteit heeft vastgesteld en de datum waarop dat is gedaan, en de mate van betrouwbaarheid van attributen.
Autorisatiebeheer	De functie Autorisatiebeheer zorgt voor een formele (en actuele) vastlegging van Autorisaties, die vanuit de Digitale identiteit van de Belanghebbende worden toegekend aan de Digitale identiteit van de Vertegenwoordiger. De autorisatie is veelal beperkt tot een Resource/een reeks Resources. De autorisatie kan voor beperkte duur gelden, of gelden totdat die wordt ingetrokken.
Policy Administration Point (PAP)	Policy Administration Point (**PAP**) draagt zorg voor het administreren van de toegangsrechten in de vorm van policies. Op basis van policies worden autoritatieve bronnen toegang gegeven tot de gevraagde doel systemen/resources.
Autorisatie	Een toestemming van een Entiteit of danwel zelf, danwel als vertegenwoordiger van een belanghebbende, om toegang te krijgen tot een Resource waarbij voorwaarden kunnen worden gedefinieerd op de attributen van de Digitale Identiteit. · Een Autorisatie is randvoorwaardelijk voor het krijgen van toegang, maar niet voldoende. · Autorisaties kunnen als informatie object zijn vastgelegd, maar dat hoeft niet altijd het geval te zijn; bijvoorbeeld als deze bij via autorisatieregels bepaald is.
Identiteitenbeheer	De functie Identiteitenbeheer brengt Digitale identiteiten tot stand voor Entiteiten (zoals Personen). Het beheer betreft ook de attributen die aan de Digitale entiteit zijn gerelateerd. Wanneer nodig zorgt de functie eveneens voor het actualiseren daarvan.
Policy Information Point (PIP)	Policy Information Point (**PIP**) draagt zorg voor het elektronisch beheren van de digitale identiteiten en attributen.
Digitale identiteit	Een Digitale Identiteit is een verzameling gegevens (Attributen) die een digitale representatie zijn van een Entiteit binnen een bepaald digitaal toepassingsgebied. · Een Entiteit kan meerdere Digitale Identiteiten hebben (binnen hetzelfde of andere contexten) · Digitale Identiteiten kunnen een onderlinge samenhang hebben waarbij enkele attributen

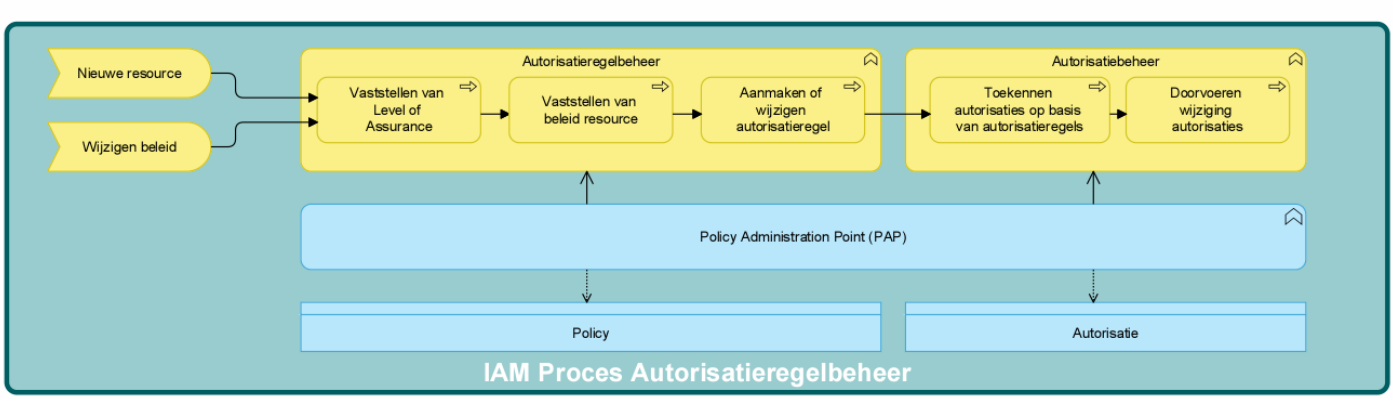
	in een Afhankelijke Digitale Identiteit een-op-een gelijk zijn aan de overeenkomstige attributen in een Leidende Digitale Identiteit. Het is dan een kwaliteitseis dat deze attributen in de afhankelijke Digitale Identiteit een zekere mate gelijk moeten zijn en gelijk gehouden worden aan die in de Leidende Digitale Identiteit; denk aan verschil tussen registratie in de BRP en de gegevens in een paspoort. · Bij een Digitale Identiteit kan metadata behoren, bijvoorbeeld de organisatie die de Digitale Identiteit heeft vastgesteld en de datum waarop dat is gedaan, en de mate van betrouwbaarheid van attributen.

05.3 Proces Wijzigen



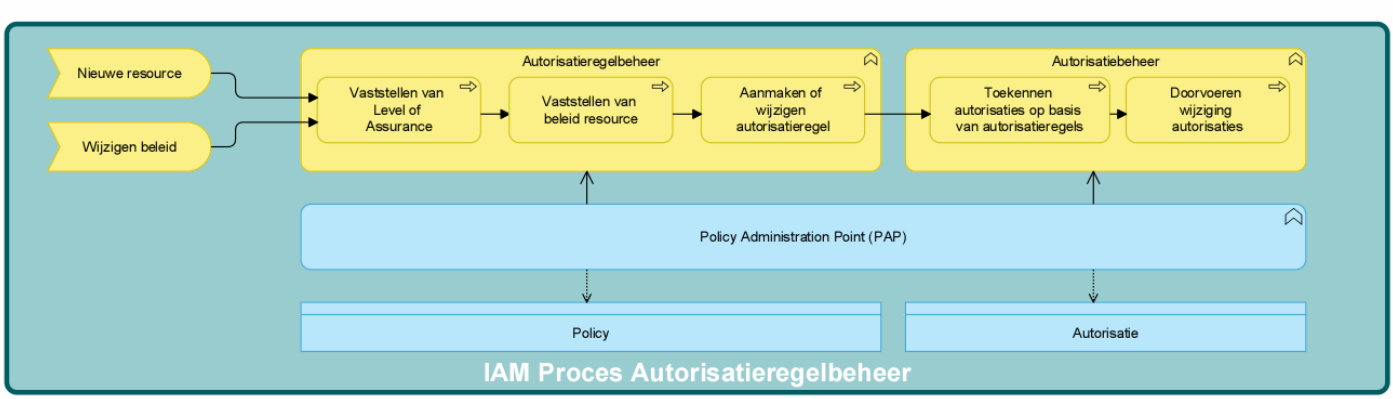
05.3 Proces Wijzigen - Documentation	
Name	**Documentation**
Identiteitenbeheer	De functie Identiteitenbeheer brengt Digitale identiteiten tot stand voor Entiteiten (zoals Personen). Het beheer betreft ook de attributen die aan de Digitale entiteit zijn gerelateerd. Wanneer nodig zorgt de functie eveneens voor het actualiseren daarvan.
Policy Information Point (PIP)	Policy Information Point (**PIP**) draagt zorg voor het elektronisch beheren van de digitale identiteiten en attributen.
Digitale identiteit	Een Digitale Identiteit is een verzameling gegevens (Attributen) die een digitale representatie zijn van een Entiteit binnen een bepaald digitaal toepassingsgebied. · Een Entiteit kan meerdere Digitale Identiteiten hebben (binnen hetzelfde of andere contexten) · Digitale Identiteiten kunnen een onderlinge samenhang hebben waarbij enkele attributen in een Afhankelijke Digitale Identiteit een-op-een gelijk zijn aan de overeenkomstige attributen in een Leidende Digitale Identiteit. Het is dan een kwaliteitseis dat deze attributen in de afhankelijke Digitale Identiteit een zekere mate gelijk moeten zijn en gelijk gehouden worden aan die in de Leidende Digitale Identiteit; denk aan verschil tussen registratie in de BRP en de gegevens in een paspoort. · Bij een Digitale Identiteit kan metadata behoren, bijvoorbeeld de organisatie die de Digitale Identiteit heeft vastgesteld en de datum waarop dat is gedaan, en de mate van betrouwbaarheid van attributen.
Autorisatiebeheer	De functie Autorisatiebeheer zorgt voor een formele (en actuele) vastlegging van Autorisaties, die vanuit de Digitale identiteit van de Belanghebbende worden toegekend aan de Digitale identiteit van de Vertegenwoordiger. De autorisatie is veelal beperkt tot een Resource/een reeks Resources. De autorisatie kan voor beperkte duur gelden, of gelden totdat die wordt ingetrokken.
Policy Administration Point (PAP)	Policy Administration Point (**PAP**) draagt zorg voor het administreren van de toegangsrechten in de vorm van policies. Op basis van policies worden autoritatieve bronnen toegang gegeven tot de gevraagde doel systemen/resources.
Autorisatie	Een toestemming van een Entiteit of danwel zelf, danwel als vertegenwoordiger van een belanghebbende, om toegang te krijgen tot een Resource waarbij voorwaarden kunnen worden gedefinieerd op de attributen van de Digitale Identiteit. · Een Autorisatie is randvoorwaardelijk voor het krijgen van toegang, maar niet voldoende. · Autorisaties kunnen als informatie object zijn vastgelegd, maar dat hoeft niet altijd het geval te zijn; bijvoorbeeld als deze bij via autorisatieregels bepaald is.

05.4 Proces Autorisatieregelbeheer



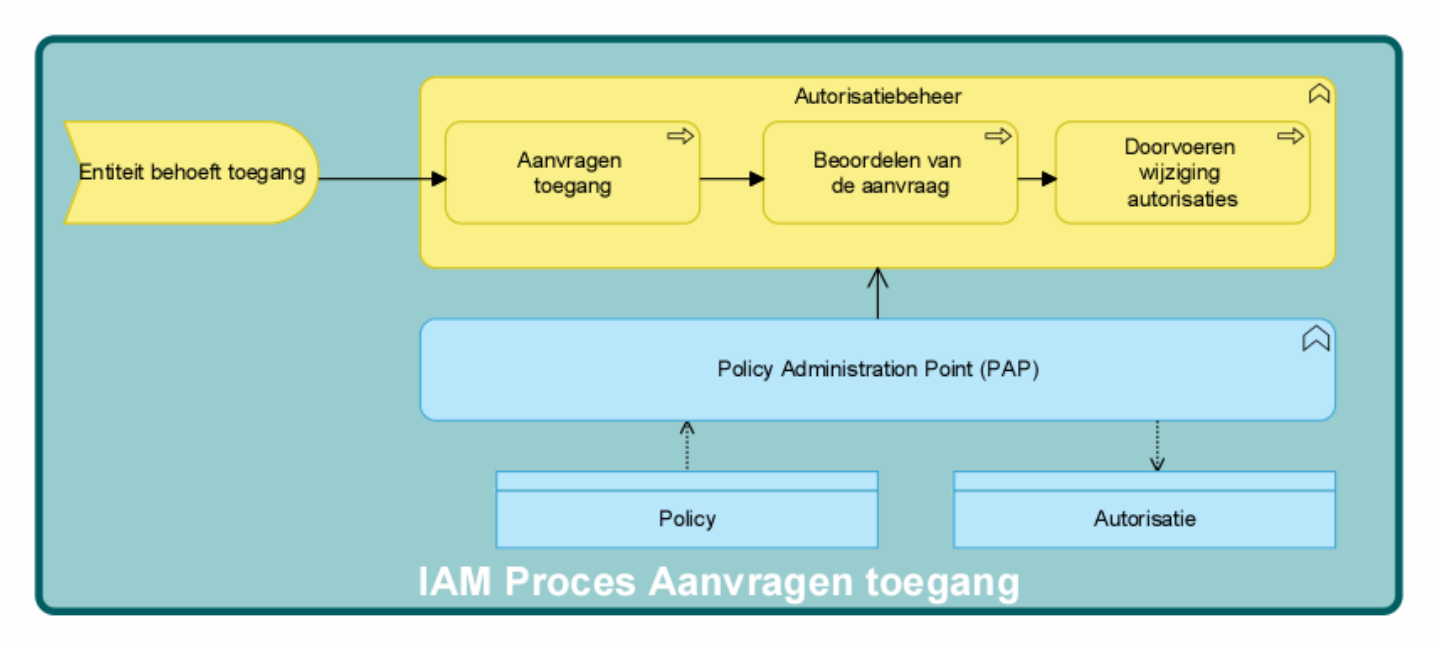
05.4 Proces Autorisatieregelbeheer - Documentation	
Name	**Documentation**
Nieuwe resource	In geval een nieuwe resource opgenomen wordt in de Fontys omgeving, dienen een aantal stappen worden uitgevoerd.
Autorisatieregelbeheer	De functie autorisatieregelbeheer formuleert de Autorisatieregels die worden toegepast bij het nemen van Autorisatiebeslissingen voor een Resource.
Policy Administration Point (PAP)	Policy Administration Point (**PAP**) draagt zorg voor het administreren van de toegangsrechten in de vorm van policies. Op basis van policies worden autoritatieve bronnen toegang gegeven tot de gevraagde doel systemen/resources.
Autorisatiebeheer	De functie Autorisatiebeheer zorgt voor een formele (en actuele) vastlegging van Autorisaties, die vanuit de Digitale identiteit van de Belanghebbende worden toegekend aan de Digitale identiteit van de Vertegenwoordiger. De autorisatie is veelal beperkt tot een Resource/een reeks Resources. De autorisatie kan voor beperkte duur gelden, of gelden totdat die wordt ingetrokken.
Autorisatie	Een toestemming van een Entiteit of danwel zelf, danwel als vertegenwoordiger van een belanghebbende, om toegang te krijgen tot een Resource waarbij voorwaarden kunnen worden gedefinieerd op de attributen van de Digitale Identiteit. · Een Autorisatie is randvoorwaardelijk voor het krijgen van toegang, maar niet voldoende. · Autorisaties kunnen als informatie object zijn vastgelegd, maar dat hoeft niet altijd het geval te zijn; bijvoorbeeld als deze bij via autorisatieregels bepaald is.

05.5 Proces Inrichten SSO



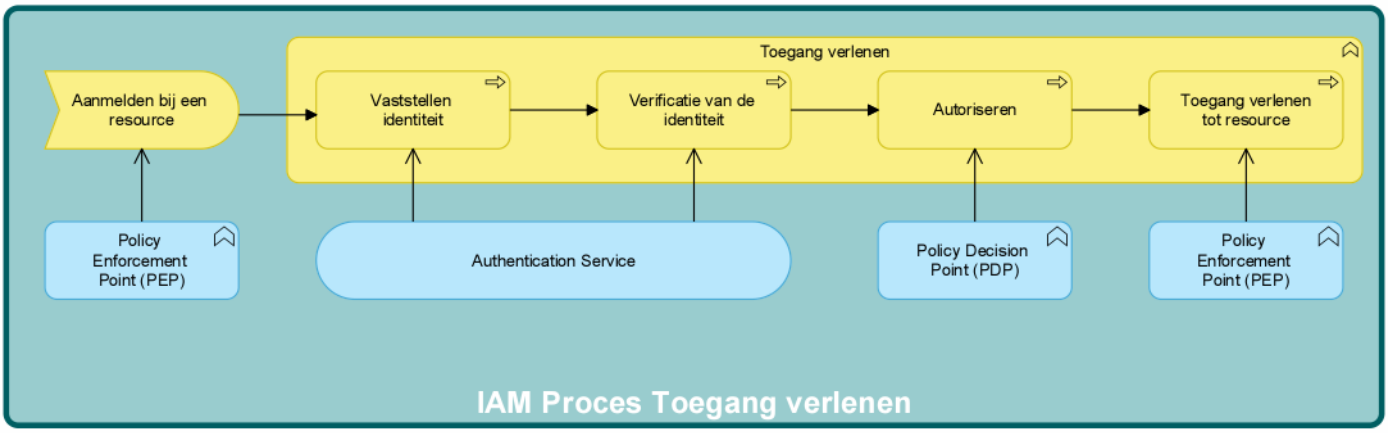
05.5 Proces Inrichten SSO - Documentation	
Name	**Documentation**
Nieuwe resource	In geval een nieuwe resource opgenomen wordt in de Fontys omgeving, dienen een aantal stappen worden uitgevoerd.
Autorisatieregelbeheer	De functie autorisatieregelbeheer formuleert de Autorisatieregels die worden toegepast bij het nemen van Autorisatiebeslissingen voor een Resource.
Policy Administration Point (PAP)	Policy Administration Point (**PAP**) draagt zorg voor het administreren van de toegangsrechten in de vorm van policies. Op basis van policies worden autoritatieve bronnen toegang gegeven tot de gevraagde doel systemen/resources.
Autorisatiebeheer	De functie Autorisatiebeheer zorgt voor een formele (en actuele) vastlegging van Autorisaties, die vanuit de Digitale identiteit van de Belanghebbende worden toegekend aan de Digitale identiteit van de Vertegenwoordiger. De autorisatie is veelal beperkt tot een Resource/een reeks Resources. De autorisatie kan voor beperkte duur gelden, of gelden totdat die wordt ingetrokken.
Autorisatie	Een toestemming van een Entiteit of danwel zelf, danwel als vertegenwoordiger van een belanghebbende, om toegang te krijgen tot een Resource waarbij voorwaarden kunnen worden gedefinieerd op de attributen van de Digitale Identiteit. · Een Autorisatie is randvoorwaardelijk voor het krijgen van toegang, maar niet voldoende. · Autorisaties kunnen als informatie object zijn vastgelegd, maar dat hoeft niet altijd het geval te zijn; bijvoorbeeld als deze bij via autorisatieregels bepaald is.

05.6 Proces Aanvragen toegang



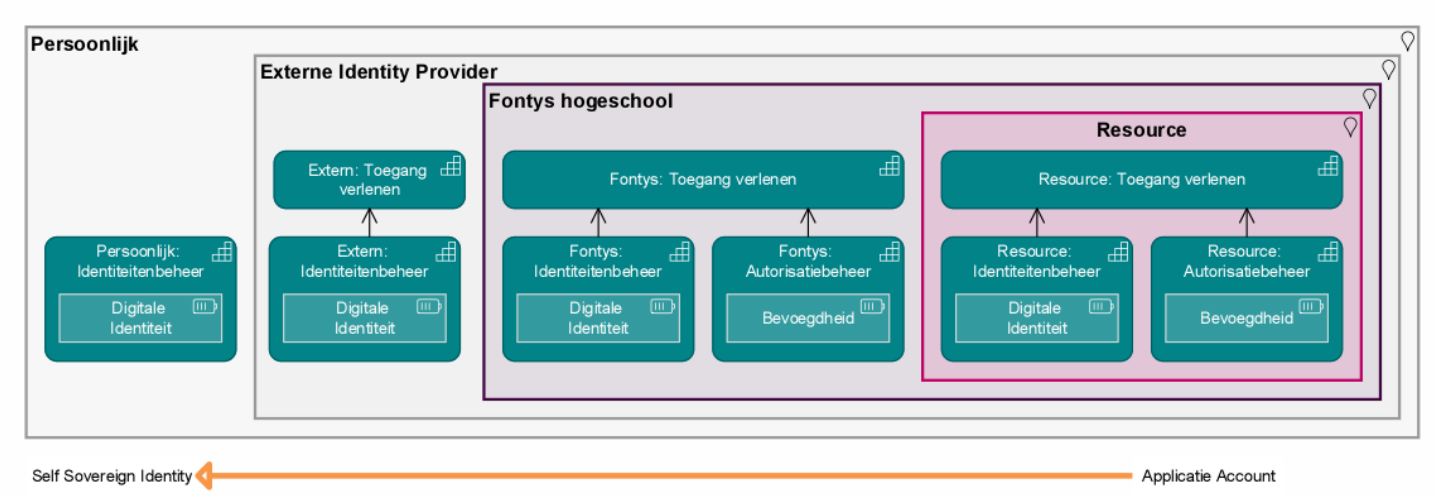
05.6 Proces Aanvragen toegang - Documentation	
Name	**Documentation**
Autorisatiebeheer	De functie Autorisatiebeheer zorgt voor een formele (en actuele) vastlegging van Autorisaties, die vanuit de Digitale identiteit van de Belanghebbende worden toegekend aan de Digitale identiteit van de Vertegenwoordiger. De autorisatie is veelal beperkt tot een Resource/een reeks Resources. De autorisatie kan voor beperkte duur gelden, of gelden totdat die wordt ingetrokken.
Policy Administration Point (PAP)	Policy Administration Point (**PAP**) draagt zorg voor het administreren van de toegangsrechten in de vorm van policies. Op basis van policies worden autoritatieve bronnen toegang gegeven tot de gevraagde doel systemen/resources.
Autorisatie	Een toestemming van een Entiteit of danwel zelf, danwel als vertegenwoordiger van een belanghebbende, om toegang te krijgen tot een Resource waarbij voorwaarden kunnen worden gedefinieerd op de attributen van de Digitale Identiteit. · Een Autorisatie is randvoorwaardelijk voor het krijgen van toegang, maar niet voldoende. · Autorisaties kunnen als informatie object zijn vastgelegd, maar dat hoeft niet altijd het geval te zijn; bijvoorbeeld als deze bij via autorisatieregels bepaald is.

05.7 Proces Toegang verlenen



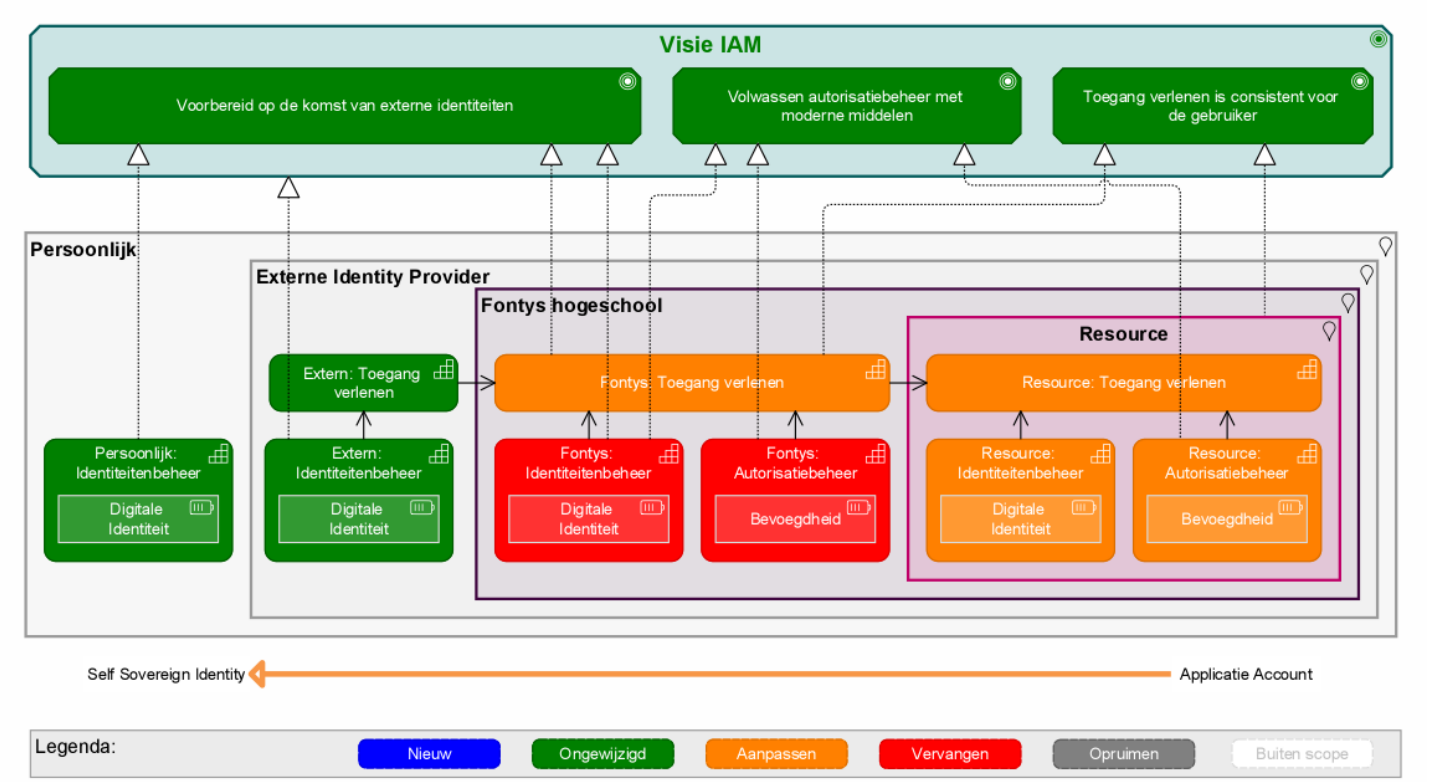
05.7 Proces Toegang verlenen - Documentation	
Name	**Documentation**
Toegang verlenen	**Regisseert het proces met identificatie, authenticatie en autoriseren**
Authentication Service	Een identity provider (IdP) is een service die digitale identiteiten opslaat en beheert, en op basis van deze informatie een Entiteit kan authentiseren.
Policy Decision Point (PDP)	Policy Decision Point (**PDP**) draagt zorg voor het beoordelen van de autorisatie aanvragen op basis van policies.

06. IAM niveaus



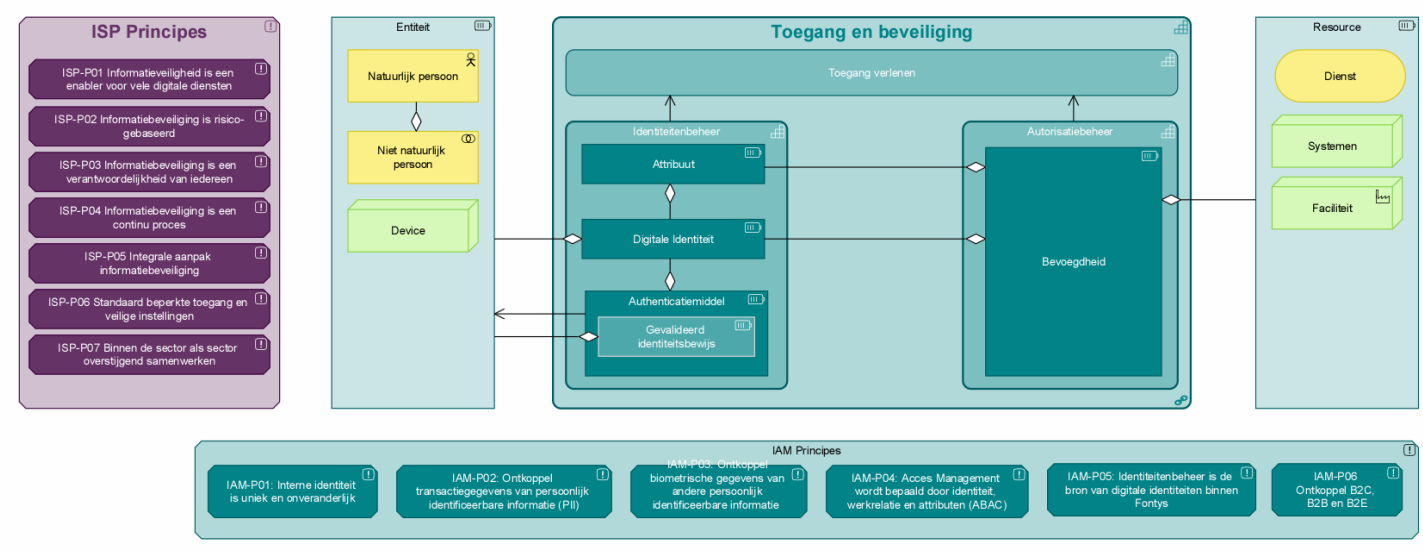
Total view 06. IAM niveaus
Het toegang verlenen, beheren van identiteiten en beheren van autorisaties vinden op verschillende plekken en op verschillende niveaus plaats. Er is spraken van een gelaagdheid. Op het laagste niveau is er een resource, bijvoorbeeld een systeem of applicatie. De applicatie kent identiteiten en autorisaties die beheerd worden en er wordt toegang verleent. Ditzelfde gebeurt ook op het niveau van de organisatie en op federatief niveau (bijvoorbeeld SURF).

07. IAM Doel architectuur



Total view 07. IAM Doel architectuur
De doelarchitectuur kenmerkt zich dat het beheer van identiteiten langzaamaan verschuift van de individuele applicaties naar centraal binnen de organisatie of SURF en uiteindelijk naar de gebruiker zelfs op basis van Self Sovereign Identity (SSI). In deze laatste vorm wordt de (digitale) identiteit beheerd op basis van een collectief (gelijk aan blockchain). Om het inloggen te vergemakkelijken dienen de resources, waaronder ook applicaties, geschikt te zijn om met externe identiteiten om te gaan. Dat betekent dat de resources (applicaties) geschikt gemaakt worden om op basis van OAuth2, OpenID Connect en SAML, waarbij de identificatie en authenticatie belegd is bij een ‘externe’ Identity Provider (IdP). Vanuit een externe IdP worden met de identiteit ook attributen verstrekt. Deze attributen kunnen gebruikt worden voor het autoriseren van de gebruiker (entiteit). Dit betekent dat het meer dan wenselijk is dat de attributen binnen een applicatie gestandaardiseerd dienen worden. Dit vereenvoudigt het provisioning proces. Voor autorisatie wordt er expliciet onderscheidt gemaakt tussen autorisatie binnen een resource (bijvoorbeeld de Canvas applicatie) en de autorisaties binnen de Fontys Organisatie. Voor het beheren van de autorisaties binnen de Fontys organisatie dient een Policy Administration Point (PAP).

08. Toegepaste principes



Total view 08. Toegepaste principes	
Documentation Het objectmodel voor IAM identificeert welke concepten uit de reële wereld relevant zijn voor het onderwerp IAM, en het beschrijft de relaties tussen de objecten. De figuur is een architectuur model van de concepten en hun relaties.	
References	NORA: Begrippen IAM

ISP Principes

ISP Principes - Documentation	
Name	**Documentation**
ISP-P01 Informatieveiligheid is een enabler voor vele digitale diensten	Informatiebeveiliging en privacybescherming bij Fontys dragen bij aan waardecreatie en waardebehoud.
ISP-P02 Informatiebeveiliging is risico-gebaseerd	We baseren maatregelen op de mogelijke risico's voor Fontys; wet- en regelgeving is naast de Fontys Strategiekaart en het cyberdreigingsbeeld in het hoger onderwijs, de basis voor het identificeren van risico's.
ISP-P03 Informatiebeveiliging is een verantwoordelijkheid van iedereen	De verantwoordelijkheid voor informatiebeveiliging en privacybescherming ligt bij iedereen en het management stuurt hierop.
ISP-P04 Informatiebeveiliging is een continu proces	Informatiebeveiliging en privacybescherming zijn cyclische processen die verankerd zijn in exploratie, verandering, exploitatie en beëindiging.
ISP-P05 Integrale aanpak informatiebeveiliging	Fontys verankert informatiebeveiliging en privacybescherming in processen en management in denken en doen.
ISP-P06 Standaard beperkte toegang en veilige instellingen	Toegang tot informatie is afgeschermd en wordt alleen specifiek voor gebruikers opengezet op basis van het 'need to know'-principe ("Gesloten waar nodig en open waar mogelijk").
ISP-P07 Binnen de sector als sector overstijgend samenwerken	Vanuit het perspectief van macrodoelmatigheid kijkt en volgt Fontys wat "sector overstijgend samen" en "sectorspecifiek aanvullend" gedaan kan worden.

IAM Principes

IAM Principes - Documentation	
Name	**Documentation**
IAM-P01: Interne identiteit is uniek en onveranderlijk	In een IAM-omgeving wordt een Entiteit geïdentificeerd op basis Attribuut dit kan bijvoorbeeld een E-mail, gebruikersnaam of een telefoonnummer zijn. Deze attributen zijn aan verandering onderhevig. De administratieve vastlegging van de Digitale Identiteit geschied op basis van een systeem specifieke identificatie, die uniek en onveranderlijk binnen het systeem is.
IAM-P02: Ontkoppel transactiegegevens van persoonlijk identificeerbare informatie (PII)	Persoonlijk Identificeerbare Informatie refereert naar informatie die te herleiden is naar een persoon, zoals een naam, BSN, Onderwijsnummer, geboortedatum, Bakrekening of telefoonnummer. De transactiegegevens die benodigd zijn voor het autheniceren en autoriseren (zoals bedoeld in IAM-P01) zijn ontkoppeld van de PII. Indien in geval van AVG de persoonsgegevens gewist moeten worden, kan volstaan worden door enkel de PII-informatie te verwijderen.
IAM-P03: Ontkoppel biometrische gegevens van andere persoonlijk identificeerbare informatie (PII)	Biometrische gegevens worden gebruikt als bewijs om de entiteit vast te stellen. Om misbruik te voorkomen dienen de biometrische gegevens ontkoppeld worden van de PII-gegevens. Bij het opslaan van Biometrische gegevens mogen geen PII-gegevens opgeslagen worden, wel kan een pseudoniem of een hash toegepast worden van de digitale identiteit. Hiermee wordt voorkomen dat een verkregen biometrisch gegeven gerelateerd kan worden aan de persoon.
IAM-P04: Acces Management wordt bepaald door identiteit, toegangsbeleid en attributen (ABAC)	Het toegang verlenen geschiedt op basis van drie gegevens: De digitale identiteit, het toegangsbeleid dat is vastgelegd als autorisatieregel en de attributen. Voor dit doel dienen de autorisatieregels expliciet vastgelegd te worden in de PAP en losgetrokken te worden van de digitale identiteiten en bijbehorende attributen. De digitale identiteiten en bijbehorende attributen dienen te worden vastgelegd in de PIP. Dit maakt het mogelijk om in geval van een audit het beleid (de autorisatieregels) los van de identiteiten en attributen te valideren.
IAM-P05: Identiteitenbeheer is de bron van digitale identiteiten binnen Fontys	Daar waar digitale identiteiten benodigd zijn is identiteitenbeheer de bron. De benodigde gegevens worden via uitwisselstandaarden gedeeld met andere resources, bij voorkeur gebaseerd op SAML of OAuth2 standaarden.
IAM-P06 Ontkoppel B2C, B2B en B2E	De (juridische) eigenschappen van een klantentiteit is anders dan die van een medewerker of een leverancier. Het is daarom dat essentieel dat de bijbehorende digitale entiteiten behorende bij medewerker, leverancier en klantsegment gescheiden worden van elkaar.