

# Procesbeschrijving IAM: Autoriseren

Auteur: 5.1.2.e

Status: Definitief

Versie 1.0

26 september 2017

Rubricering: Groen

## Toelichting voor gebruik van rubricering.

Deze code is verplicht voor ICT documenten.

Deze informatie is naar eigen inzicht te **verwijderen**. (klik in de tabel/plaatje en delete)

Rubricering	Hieronder valt informatie	Toelichting
<b>Politie Intern (GROEN)</b>	<ul style="list-style-type: none"><li>die betrekking heeft op de politie en de door de politie uitgevoerde werkzaamheden</li><li>waarvan toegang door niet-gerechtigden kan en/of zal leiden tot nadeel aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie</li></ul>	Onder nadeel wordt verstaan de schending van privacy van personen, doordat naam, adres en/of andere gevoelige gegevens openbaar worden, danwel het bekend worden van gegevens, waardoor de uitvoering van de politietaak kan worden aangetast en waarvan de gevolgen lastig zijn te herstellen
<b>Politie Zeer Vertrouwelijk (GEEL)</b>	<ul style="list-style-type: none"><li>die betrekking heeft op de politie en door de politie uitgevoerde werkzaamheden</li><li>waarvan toegang door niet-gerechtigden kan en/of zal leiden tot schade aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie.</li><li>waarvan inzage door nietgerechtigden, kan leiden tot schadelijke gevolgen voor onderzoek naar de zware en georganiseerde criminaliteit</li></ul>	Onder schade kan onder meer verstaan worden de openbaarmaking van gegevens, waardoor de uitoefening van de dienstverlening en/of taken van de politie, de ketenpartners en/of in het partnerdomein van de politie zodanig in gevaar komen, dat de gevolgen daarvan nauwelijks herstelbaar zullen zijn
<b>Politie Geheim (ROOD)</b>	<ul style="list-style-type: none"><li>die betrekking heeft op de politie en de door de politie uitgevoerde werkzaamheden en</li><li>waarvan toegang door niet-gerechtigden kan en/of zal leiden tot ernstige schade aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie.</li><li>waarvan inzage door niet gerechtigden kan leiden tot het toebrengen van ernstige schade aan de opsporing van, en de opsporingsmethodieken inzake ernstige inbreuken op de rechtsorde, of ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten</li></ul>	Onder ernstige schade kan onder meer verstaan worden de openbaarmaking van gegevens, waardoor de uitoefening van de taken van de politie zodanig in gevaar komen, dat deze onherstelbaar zullen zijn
<b>Politie Zeer Geheim (PAARS)</b>	<ul style="list-style-type: none"><li>die betrekking heeft op de politie en de door de politie uitgevoerde werkzaamheden en</li><li>waarvan toegang door niet-gerechtigden kan en/of zal leiden tot zeer ernstige schade aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie</li><li>waarvan inzage door niet gerechtigden zeer ernstige schadelijke gevolgen heeft voor het onderzoek naar georganiseerde zware criminaliteit, of zeer ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten.</li></ul>	Onder zeer ernstige schade kan onder meer verstaan worden de openbaarmaking van gegevens, waardoor de uitoefening van de taken van de politie zodanig in gevaar komen, dat deze onherstelbaar zullen zijn en mensenlevens in het geding zijn (infiltranten, informanten en beschermde getuigen).

# 1 Documentinformatie

## Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	07-09-2016	Eerste opzet	
0.2	26-09-2016	Vier ogen principe toegevoegd aan autoriseren via ATL	
0.3	22-11-2016	Proceseigenaar is door MT-DIM benoemd.	
0.4	07-12-2016	Spellingsfouten en stijlfouten gecorrigeerd en begrippenlijst aangevuld	
0.5	10-01-2017	Procesnummering in lijn gebracht nav wijziging in het IAM proces "profielenbeheer".	
0.6	08-6-2017	Diverse spel en stijlfouten fouten gecorrigeerd.	
1.0	26-9-2017	Geaccordeerd door de Proceseigenaar (sectorhoofd Functioneelbeheer) en stuurgroep Autorisatiemodel.	PVO als bijlage toegevoegd

## Distributie

Versie	Verzend datum	Naam	Afdeling / Functie

## Review commentaar

Versie	Wanneer	Wie	Functie

©2017 Politie, all rights reserved.

Niets uit deze uitgave mag worden veeleenvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

# Inhoudsopgave

1 Documentinformatie .....	3
2 Voorwoord .....	5
2.1 Autorisatiebeheerproces onder Identity & Accessmanagement (IAM) .....	5
3 Inleiding .....	7
3.1 Doel van het proces .....	7
3.2 Scope .....	7
3.3 Doelstellingen van het autorisatieproces .....	7
3.4 Toegevoegde waarde van dit proces .....	7
3.5 Eigenaarschap proces: .....	7
4 Het autorisatiebeheer proces .....	8
4.1 Inleiding .....	8
4.2 Uitleg over de werkprocessen binnen Autorisatiebeheer .....	8
1.1.1 IAM13.0 Autoriseren Instroom .....	8
1.1.2 IAM 14.0 Autoriseren Doorstroom .....	11
1.1.3 IAM15.0 Autoriseren uitstroom .....	13
1.1.4 IAM 16.0 Autoriseren met ATL .....	17
1.1.5 IAM17.0 De-autoriseren met ATL .....	19
5 Performance Indicatoren .....	22
6 Begrippenlijst .....	24
7 Bijlage 1: Legenda workflows .....	25
7.1 Legenda .....	25
7.2 Nummering van de processen en activiteiten .....	25

## 2 Voorwoord

### 2.1 Autorisatiebeheerproces onder Identity & Accessmanagement (IAM)

Met het Identity & Access Managementproces (IAM) wordt binnen de Nederlandse Politie de toegang tot ICT applicaties geregeld, evenals de toegang tot mappen en schijven conform de landelijke standaard.

Dit document beschrijft één van de drie werkprocessen die gezamenlijk IAM vormen: het Autorisatiebeheer proces. Dit proces beschrijft de werkzaamheden die benodigd zijn om de autorisaties toe te kennen of in te trekken.

### 2.2 De overige processen onder Identity & Accessmanagement (IAM)

De andere twee processen binnen IAM zijn in andere documenten vastgelegd:

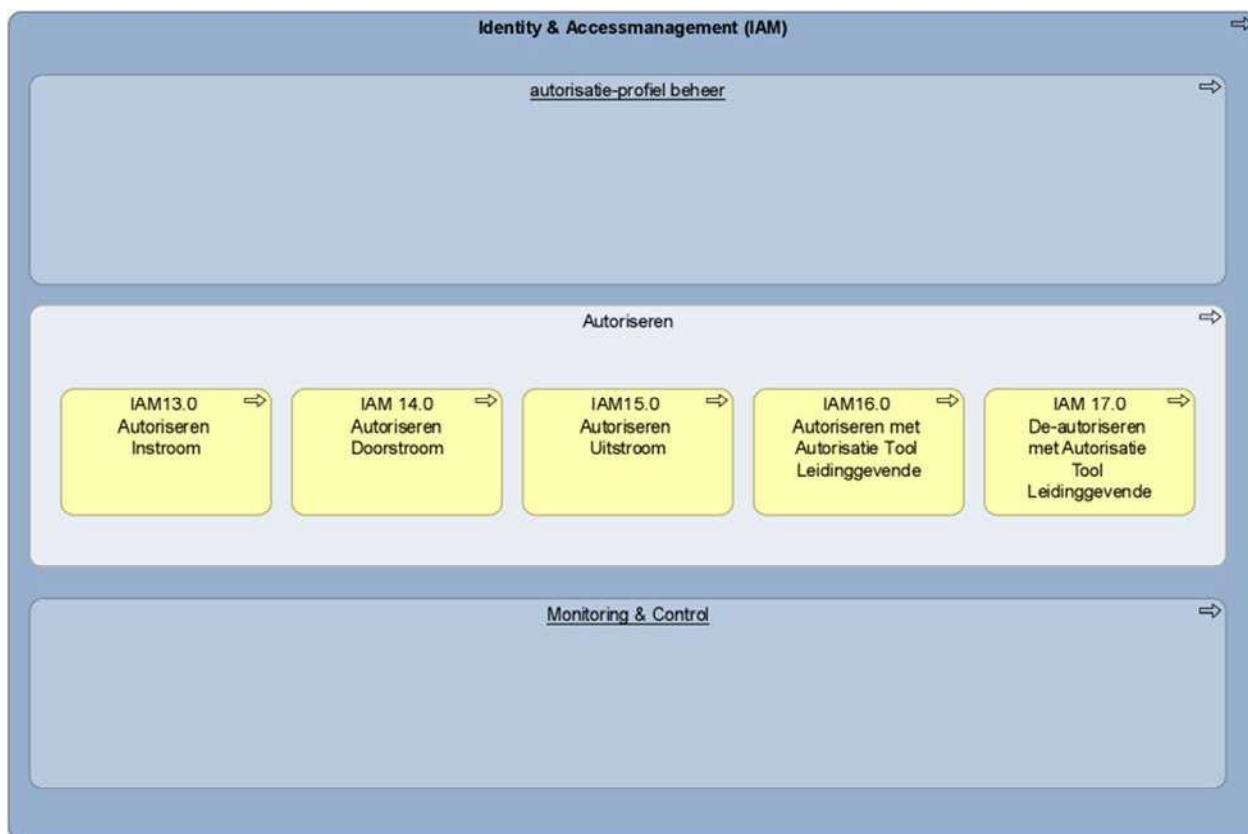
- Autorisatieprofielbeheer: hoe de autorisatieprofielen tot stand komen, wijzigen en geïmplementeerd worden.
- Monitoring & Control: het monitoren op een juiste autorisatie en acteren op afwijkingen (fouten of veranderende factoren, zoals bijvoorbeeld regelgeving).

Het autorisatiebeheer proces is een proces waarin veel handelingen automatisch uitgevoerd worden. Hiervoor wordt gebruik gemaakt van autorisatieprofielen. Hoe deze tot stand komen en toegepast worden, staat beschreven in het autorisatieprofielenbeheer proces.

### 2.3 Scope

Dit document richt zich op het autoriseren, waarbij menselijke interactie nodig is. Voor de geautomatiseerde onderdelen wordt verwezen naar de functionele ontwerpen van de IAM-tool.

Een legenda van de processchema's en de opbouw van de nummering van de werkprocessen en bijbehorende activiteiten zijn in de bijlagen terug te vinden.



**Figuur 1: Autorisatiebeheer gepositioneerd binnen IAM**

# 3 Inleiding

## 3.1 Doel van het proces

Het doel van het autorisatiebeheer proces is het toekennen, aanpassen en stopzetten van toegang tot de politie systemen en -applicaties voor medewerkers en ketenpartners van de politie.

## 3.2 Scope

Deze procesbeschrijving richt zich op:

- Het toekennen en intrekken van autorisaties op basis van de zogenoemde IDU processen:
  - o de instroom van nieuwe medewerkers,
  - o de doorstroom van medewerkers,
  - o de uitstroom van medewerkers.
- Het toekennen en intrekken van autorisaties voor politiemedewerkers die tijdelijk bij een andere afdeling of eenheid worden gedetacheerd.

Buiten de scope van deze procesbeschrijving valt:

- het autorisatiebeheer van de EBO's,
- autorisatie voor het (technisch) systeembeheer van systemen, als routers en servers,
- de processen die HR gebruikt om de personeelsadministratie uit te voeren,
- de werkwijze binnen de afdeling Functioneel beheer (FB), wanneer er handmatige handelingen benodigd zijn,
- Het beschrijven van de geautomatiseerde processen in de IAM-tool. Deze informatie staat in de functioneel ontwerpen van de IAM-tool.

## 3.3 Doelstellingen van het autorisatieproces

1. politiemedewerkers tijdig voorzien van juiste autorisaties,
2. voorkomen dat autorisaties onnodig open blijven staan,
3. bieden van flexibiliteit en snelheid voor de autorisaties voor politiemedewerkers die tijdelijk bij een andere afdeling of eenheid worden ondergebracht.

## 3.4 Toegevoegde waarde van dit proces

1. draagt bij aan het realiseren van het "Delen tenzij" principe,
2. draagt bij aan de administratieve lastenverlichting,
3. geeft inzicht in welke medewerker waarvoor is geautoriseerd.

## 3.5 Eigenaarschap proces:

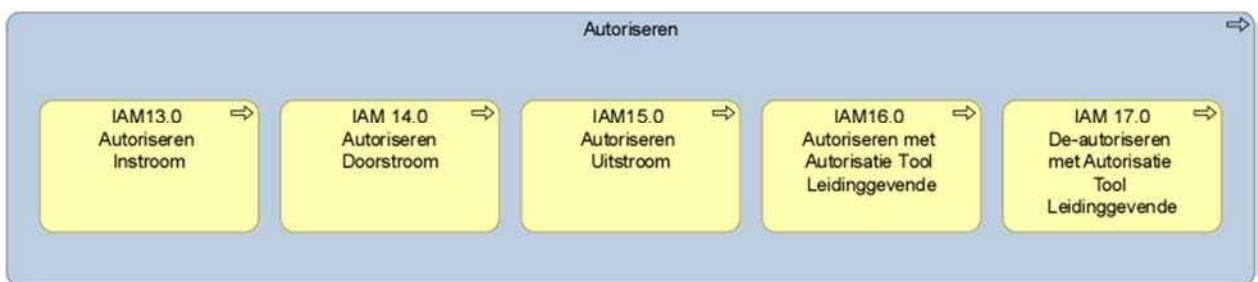
Het eigenaarschap van dit proces ligt bij het Hoofd van de Dienst Informatiemanagement en is gedelegeerd aan het sectorhoofd Functioneel beheer (bron: 5.1.2.e , 5.1.2.e , d.d. 21-11-2016)

## 4 Het autorisatiebeheer proces

### 4.1 Inleiding

Het autorisatiebeheerproces wordt gestart door het IDU proces (Instroom, Doorstroom en Uitstroom) binnen de personeelsadministratie van HRM (HRA: HR Administratie). Daarnaast is er voor de leidinggevende een mogelijkheid om een tijdelijke autorisatie toe te kennen en in te trekken via de autorisatietool leidinggevende (ATL). Dat maakt dat er in totaal vijf werkprocessen binnen het autorisatiebeheer worden toegepast:

1. autoriseren Instroom,
2. autoriseren Doorstroom,
3. autoriseren Uitstroom,
4. autoriseren met ATL,
5. De-autoriseren met ATL.



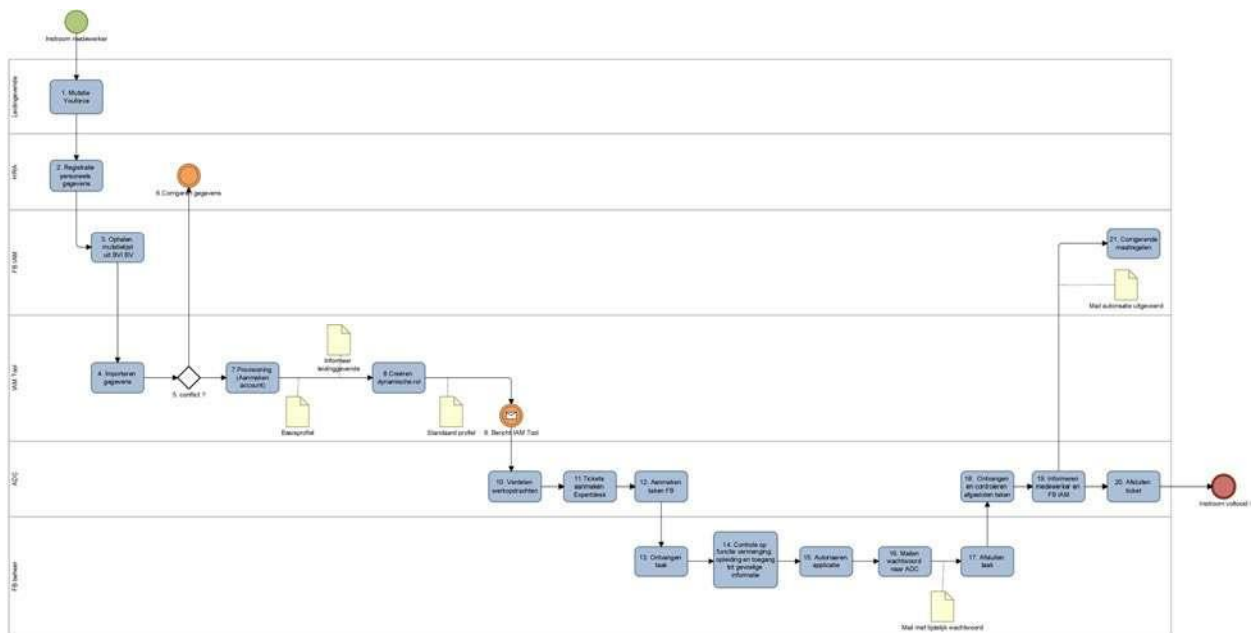
Figuur 2: de werkprocessen binnen het autorisatiebeheer.

### 4.2 Uitleg over de werkprocessen binnen Autorisatiebeheer

*Opmerking: Een legenda betreffende de symbolen in de schema's staat in de bijlage.*

#### 1.1.1 IAM13.0 Autoriseren Instroom

Onder Instroom worden medewerkers verstaan die nieuw binnenkomen bij de politie en een nieuw dienstverband krijgen. Dit geldt ook voor oud-medewerkers die na enige tijd weer bij de politie gaan werken.



Figuur 3: IAM13 - autoriseren instroom

Vanaf stap 13.9 worden de werkzaamheden door de ADC en Functioneel Beheer van de applicatie uitgevoerd. Deze activiteiten worden hier op hoofdlijnen benoemd. De detailuitwerking staan in de werkinstructies voor het ADC en FB.

Processtap	Omschrijving	Responsible	Waarmee
13.1	De leidinggevende registreert de nieuwe medewerker in YouForce.	Leidinggevende	Youforce
13.2	Bij HR wordt de nieuwe medewerker in de personeelsadministratie verwerkt.	HR	Personeelsregistratie systeem (BO4)
13.3	De personeelsgegevens worden automatisch opgehaald uit de BVI-BV. Query's zorgen ervoor dat het resultaat een importsheet oplevert met personeelsgegevens die aan de IAM criteria voldoen.	FB IAM	BVI-BV
13.4	De gegevens worden in de IAM tool geïmporteerd.	FB IAM (automatisch)	IAM-tool
13.5	De import wordt automatisch gecontroleerd op ontbrekende of conflicterende personeelsgegevens op basis van de business rules die in de IAM tool zijn geconfigureerd.	FB IAM (automatisch)	IAM-tool
13.6	Foutieve gegevens gaan retour naar HRM en zij dienen de correcties uit te voeren. De correcties zullen in de volgende run opnieuw worden aangeboden.	FB IAM (automatisch)	IAM-tool
13.7	Voor de nieuwe medewerker gaat er een opdracht uit naar het beheer van de active-directory en wordt een inlogaccount (netwerkaccount)	Beheer AD Leidinggevende	IAM-tool AD

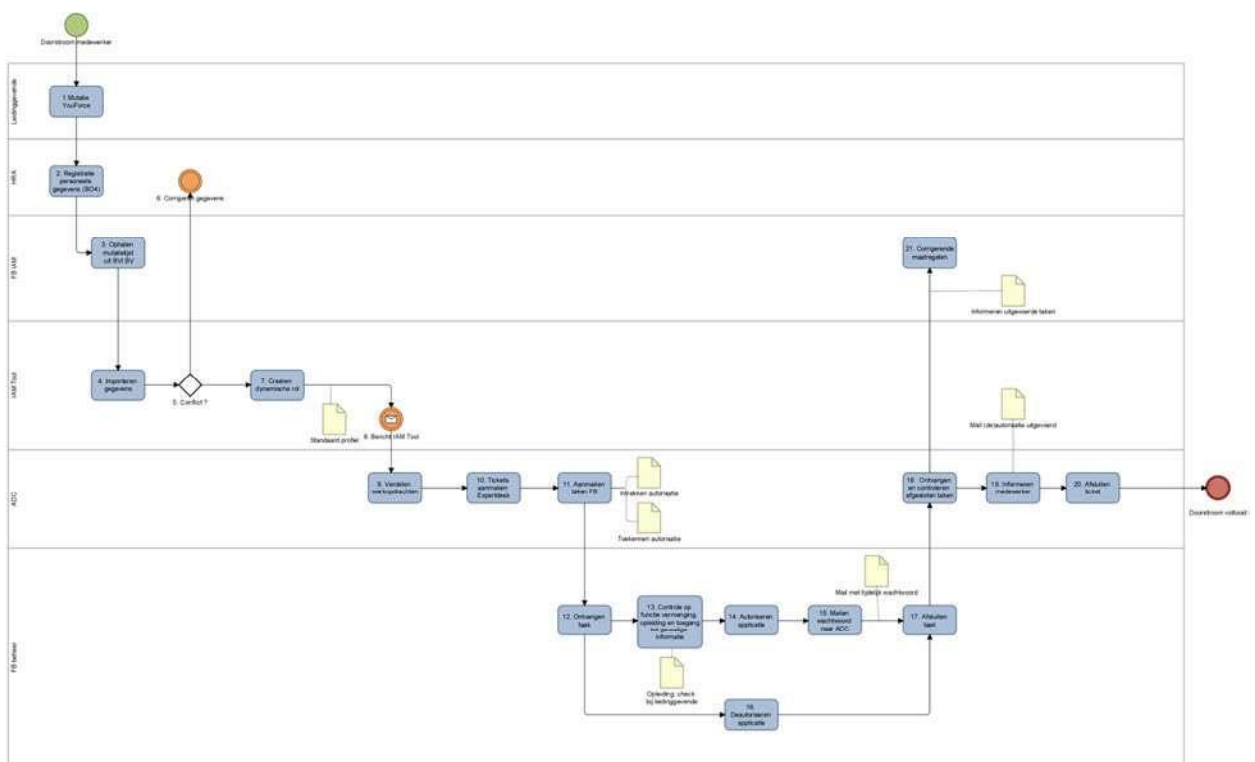
	<p>gecreëerd, waarmee de medewerker kan inloggen op het computersysteem van de politie. Hiermee is het basisprofiel geactiveerd: de medewerker heeft toegang tot het systeem, met Outlook, Office en enkele andere standaard voorzieningen. Dit wordt ook de Functionele Bodem genoemd. Zodra dit gerealiseerd is, wordt de leidinggevende (automatisch, via een e-mail), op de hoogte gebracht (die vervolgens de nieuwe medewerker kan inlichten).</p>		
13.8	<p>Nu het account bekend is, wordt op basis van standaardprofielen en de HR gegevens berekend voor welke applicaties de autorisaties toegekend moeten worden. Dit wordt de dynamische rol genoemd.</p> <p>Er ligt nu een relatie tussen het account en relevante applicaties.</p>	FB IAM (automatisch)	IAM-tool
13.9	De IAM tool levert een concrete opdracht via mail aan de Autorisatiedesk Centraal (ADC)	ADC FB-IAM	IAM-tool Outlook
13.10	Het ADC kijkt welke werkopdrachten nodig zijn voor de verdere verwerking (voor welke beheerders, wat er moet worden geautoriseerd etc.) De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Outlook
13.11	Het ADC maakt een ticket aan in Expertdesk. De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk
13.12	Onder het ticket worden de relevante taken voor de oplosgroepen aangemaakt. De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk
13.13	De oplosgroepen (Functioneel beheer teams) nemen de taak in ontvangst. De verdere uitwerking van deze taak staat in de instructies bij FB).	FB	Expertdesk
13.14	FB voert een check uit ter controle of een verplichte functiescheiding noodzakelijk is (en die door IAM niet kan worden aangeven).	FB	Beheertool van FB
13.15	Toegang tot de applicatie wordt verleend.	FB	Beheertool van FB
13.16	FB mailt het wachtwoord naar het ADC.	FB	Outlook

13.17	FB sluit zijn taak af.	FB	Expertdesk
13.18	ADC ontvangt en controleert de door FB afgesloten taak. FB IAM wordt geïnformeerd over de uitgevoerde opdrachten (zie instructies voor het ADC).	ADC	Expertdesk
13.19	Het ADC informeert de medewerker door het wachtwoord naar hem te sturen.	ADC	Outlook
13.20	Het ticket wordt afgesloten.	ADC	Expertdesk
13.21	Wanneer vanuit de berichtgeving van het ADC blijkt dat er taken zijn die niet zijn uitgevoerd, moet FB IAM herstelacties uitvoeren. Dit betekent een analyse van het niet kunnen uitvoeren van het verzoek en op basis van de uitkomst van de analyse de corrigerende maatregelen nemen.	FB IAM	

### 1.1.2 IAM 14.0 Autoriseren Doorstroom

Onder Doorstroom wordt verstaan:

1. Een medewerker die van eenheid/team verandert,
2. Een medewerker die een nieuwe functie krijgt,
3. Een medewerker die en nieuwe functie krijgt én naar een nieuwe eenheid of team vertrekt.



Figuur 4: IAM14 - autoriseren doorstroom

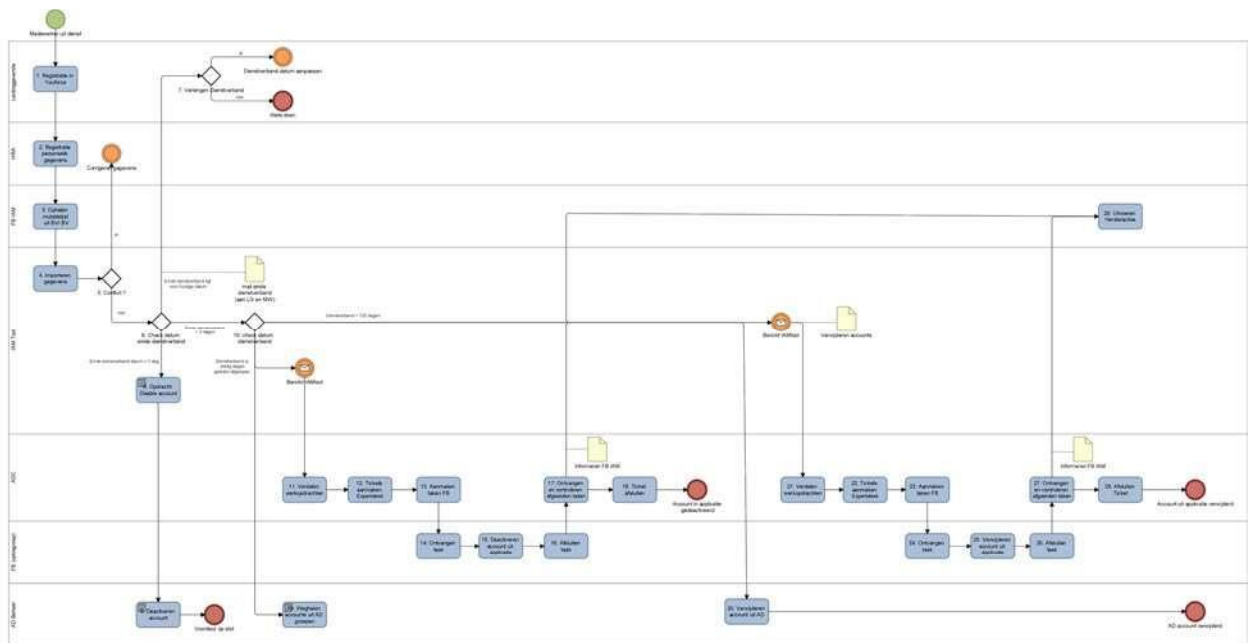
Processtap	Omschrijving	Responsible	Waarmee
------------	--------------	-------------	---------

14.1	De leidinggevende registreert de nieuwe functie of nieuwe eenheid van de medewerker in Youforce.	Leidinggevende	Youforce
14.2	Bij HR worden de gegevens van de medewerker in de personeelsadministratie bijwerkt.	HR	Personeelsregistratie systeem (BO4)
14.3	De personeelsgegevens worden automatisch opgehaald uit de BVI-BV. Query's zorgen ervoor dat het resultaat een importsheet oplevert met personeelsgegevens die aan de IAM criteria voldoen.	FB IAM	BVI-BV
14.4	De gegevens worden in de IAM tool geïmporteerd.	FB IAM (automatisch)	IAM-tool
14.5	De import wordt automatisch gecontroleerd op ontbrekende of conflicterende personeelsgegevens op basis van de business rules die in de IAM tool zijn geconfigureerd.	FB IAM (automatisch)	IAM-tool
14.6	Foutieve gegevens gaan retour naar HRM en zij dienen de correcties uit te voeren. De correcties zullen in de volgende run opnieuw worden aangeboden.	FB IAM (automatisch)	IAM-tool
14.7	Op basis van de standaardprofielen en de aangepaste HR gegevens wordt berekend voor welke applicaties de autorisaties toegekend moeten worden en welke moeten worden verwijderd.	FB IAM (automatisch)	IAM-tool
14.8	De IAM tool levert een concrete opdracht via mail aan de Autorisatiedesk Centraal (ADC) waarin aangegeven staat welke autorisaties nieuw moeten worden toegevoegd voor de gebruiker en welke autorisaties ingetrokken moeten worden.	ADC FB-IAM	IAM-tool Outlook
14.9	Het ADC kijkt welke werkopdrachten nodig zijn voor de verdere verwerking (welke beheerders moeten een opdracht krijgen, wat er moet worden ge(de)autoriseert etc.) De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Outlook
14.10	Het ADC maakt een ticket aan in Expertdesk. De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk
14.11	Aan het ticket worden de relevante taken voor de oplosgroepen aangemaakt. De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk

14.12	De oplosgroepen (Functioneel beheer teams) nemen de taak in ontvangst. De verdere uitwerking van deze taak staat in de instructies bij FB).	FB	Expertdesk
14.13	FB voert een check uit ter controle op mogelijke functiemenging die niet is toegestaan (maar door IAM nog niet kan worden aangeven).	FB	Beheertool van FB
14.14	Toegang tot de applicatie wordt verleend.	FB	Beheertool van FB
14.15	FB mailt het wachtwoord naar het ADC.	FB	Outlook
14.16	Toegang tot niet relevante applicaties wordt afgesloten (applicaties die volgens het profiel niet voor de functionaris zijn bedoeld).	FB	Beheertool van FB
14.17	FB sluit zijn taak af.	FB	Expertdesk
14.18	ADC ontvangt en controleert de door FB afgesloten taak. FB IAM wordt geïnformeerd over de uitgevoerde opdrachten (zie instructies voor het ADC).	ADC	Expertdesk
14.19	Het ADC informeert de medewerker door het wachtwoord naar hem te sturen.	ADC	Outlook
14.20	Het ticket wordt afgesloten.	ADC	Expertdesk
14.21	Wanneer vanuit de berichtgeving van het ADC blijkt dat er taken zijn die niet zijn uitgevoerd, moet FB IAM herstelacties uitvoeren. Dit betekent een analyse van het niet kunnen uitvoeren van het verzoek en op basis van de uitkomst van de analyse de corrigerende maatregelen nemen.	FB IAM	

### 1.1.3 IAM15.0 Autoriseren uitstroom

Onder uitstroom worden de medewerkers verstaan, waarvan de dienstverbanden worden beëindigd.



**Figuur 5: IAM15 - autoriseren uitstroom**

Processtap	Omschrijving	Responsible	Waarmee
15.1	In Youforce geeft de leidinggevende aan dat het dienstverband met de medewerker wordt beëindigd.	Leidinggevende	Youforce
15.2	Bij HR wordt het beëindigen van het dienstverband in de personeelsadministratie verwerkt.	HR	Personeelsregistratie systeem (BO4)
15.3	De personeelsgegevens worden opgehaald uit de BVI-BV. Query's zorgen ervoor dat het resultaat een import oplevert met personeelsgegevens die aan de IAM criteria voldoen.	FB IAM	BVI-BV
15.4	De gegevens worden in de IAM tool geïmporteerd.	FB IAM (automatisch)	IAM-tool
15.5	De import wordt automatisch gecontroleerd op ontbrekende of conflicterende personeelsgegevens. Foutieve gegevens gaan retour naar HRM en zij dienen de correcties uit te voeren. De correcties zullen in de volgende run opnieuw worden aangeboden.	FB IAM (automatisch)	IAM-tool
15.6	Controle op de datum einde dienstverband. Wanneer deze datum in de toekomst ligt, vervolgt het proces via 15.7. Wanneer deze datum in het verleden ligt, gaat het proces verder bij 15.11.	Automatisch	IAM-tool
15.7	De leidinggevende wordt via e-mail op de hoogte gebracht van de naderende datum uitdiensttreding. Wanneer het einde dienstverband toch	Leidinggevende	IAM-tool

	<p>niet wenselijk is. Heeft de leidinggevende de tijd om hierop actie te ondernemen, door de einddatum van het dienstverband in Youforce aan te passen.</p> <p>Wanneer de medewerker daadwerkelijk op die datum de organisatie verlaat, hoeft de leidinggevende niet te doen: Het proces gaat via 15.8 verder.</p>		
15.8	<p>Wanneer het dienstverband is beëindigd, wordt er een opdracht naar de AD gestuurd om het account behorende bij het dienstverband dicht te zetten.</p>	Automatisch	IAM-tool
15.9	<p>Het account wordt in de AD dichtgezet. Via het account kan niet meer op het netwerk worden ingelogd.</p>	Automatisch	Active Directory
15.10	<p>Zodra de datum einde dienstverband is overschreden, wordt een nieuwe datumcheck uitgevoerd. Als de datum van het einde dienstverband met 30 dagen is overschreden worden er acties geïnitieerd om toegang tot de applicaties dicht te zetten. (deze buffer van 30 dagen is ingebakken, mocht onverhoopt de medewerker toch nog blijven bij de politie). Op de dertigste dag gaat het proces verder met 15.11 én 15.19.</p> <p>Zodra de datum van het einde dienstverband de 710 dagen heeft overschreden, gaat het proces verder bij 15.20 én 15.21.</p>	automatisch	IAM-tool
15.11	<p>De IAM tool levert een concrete opdracht via mail aan de Autorisatiedesk Centraal (ADC) waarin aangegeven staat welke autorisaties gedeactiveerd moeten worden. Het ADC kijkt welke opdrachten nodig zijn voor de verdere verwerking (welke beheerders zijn nodig, welke applicaties er moeten worden gedeactiveerd etc.) De verdere uitwerking van deze taak staat in de instructies voor het ADC</p>	ADC	
15.12	<p>Er wordt een ticket, per persoon die moet worden gedeactiveerd, aangemaakt in Expertdesk De verdere uitwerking van deze taak staat in de instructies voor het ADC</p>	ADC	Expertdesk
15.13	<p>Voor iedere betrokken oplosgroep (Functioneel beheer) wordt een taak aangemaakt</p>	ADC	Expertdesk

15.14	De oplosgroep ontvangt de taak via Expertdesk.	FB	Expertdesk
15.15	Het account in de applicatie wordt gedeactiveerd	FB	Beheertool applicatie
15.16	Na uitvoering wordt de taak afgesloten. Wanneer onverhoopt blijkt dat de taak niet kon worden uitgevoerd, dan is de afsluiting voorzien van de reden hiervoor	FB	Expertdesk
15.17	De afgesloten taken worden gecontroleerd en FB IAM wordt geïnformeerd over wat er is uitgevoerd en wat niet.	ADC	Mail
15.18	Het ticket wordt afgesloten	ADC	Expertdesk
15.19	De accounts worden uit de desbetreffende AD groepen gehaald	automatisch	IAM-tool
15.20	Na 720 dagen worden de accounts uit de AD verwijderd	automatisch	IAM-tool
15.21	De IAM tool levert een concrete opdracht via mail aan de Autorisatiedesk Centraal (ADC) waarin aangegeven staat welke autorisaties voor welke applicaties verwijderd moeten worden. Het ADC kijkt welke opdrachten nodig zijn voor de verdere verwerking (welke beheerders en welke applicaties betrokken zijn) De verdere uitwerking van deze taak staat in de instructies voor het ADC	ADC	
15.22	Er wordt een ticket, per persoon die moet worden verwijderd, aangemaakt in Expertdesk De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk
15.23	Voor iedere betrokken oplosgroep (Functioneel Beheer) wordt een taak aangemaakt.	ADC	Expertdesk
15.24	De oplosgroep ontvangt de taak via Expertdesk.	FB	Expertdesk
15.25	Het account in de applicatie wordt verwijderd.	FB	Beheertool applicatie
15.26	Na uitvoering wordt de taak afgesloten. Wanneer onverhoopt blijkt dat de taak niet kon worden uitgevoerd, dan is de afsluiting voorzien van de reden hiervoor.	FB	Expertdesk
15.27	De afgesloten taken worden gecontroleerd en FB IAM wordt geïnformeerd over wat er is uitgevoerd en wat niet.	ADC	Mail
15.28	Het ticket wordt afgesloten.	ADC	Expertdesk
15.29	Wanneer vanuit de berichtgeving van het ADC blijkt dat er taken zijn die niet zijn uitgevoerd, moet FB IAM	FB IAM	

	herstelacties uitvoeren. Dit betekent een analyse van het niet kunnen uitvoeren van het verzoek en op basis van de uitkomst en de corrigerende maatregelen nemen.		
--	---	--	--

### 1.1.4 IAM 16.0 Autoriseren met ATL

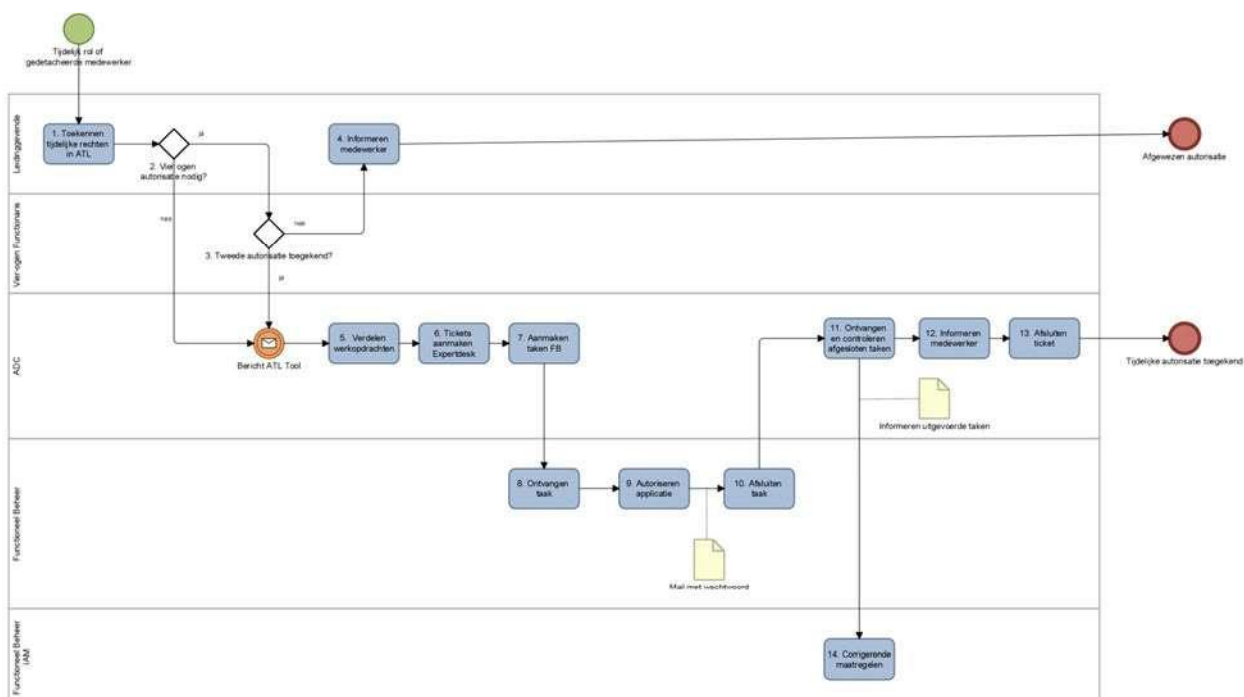
De leidinggevende kan met behulp van de Autorisatietool Leidinggevende (ATL) een medewerker die tijdelijk (korter dan drie maanden) op de afdeling wordt tewerk gesteld (TTW) rechten toekennen.

Dit geldt ook voor medewerkers op de afdeling, die tijdelijk andere taken op die afdeling gaan vervullen.

De ATL kan alleen voor applicaties worden gebruikt die in de profielen zitten die aan dat team zijn toegekend. (waardoor de leidinggevende automatisch is gemandateerd om voor deze applicaties de ATL te gebruiken).

De medewerker behoudt de autorisaties van de applicaties die hij vanuit zijn eigen afdeling kent.

Voor een aantal autorisaties geldt dat deze, wanneer de ATL wordt gebruikt, via het vier ogen principe worden geautoriseerd. De ATL geeft dit aan.



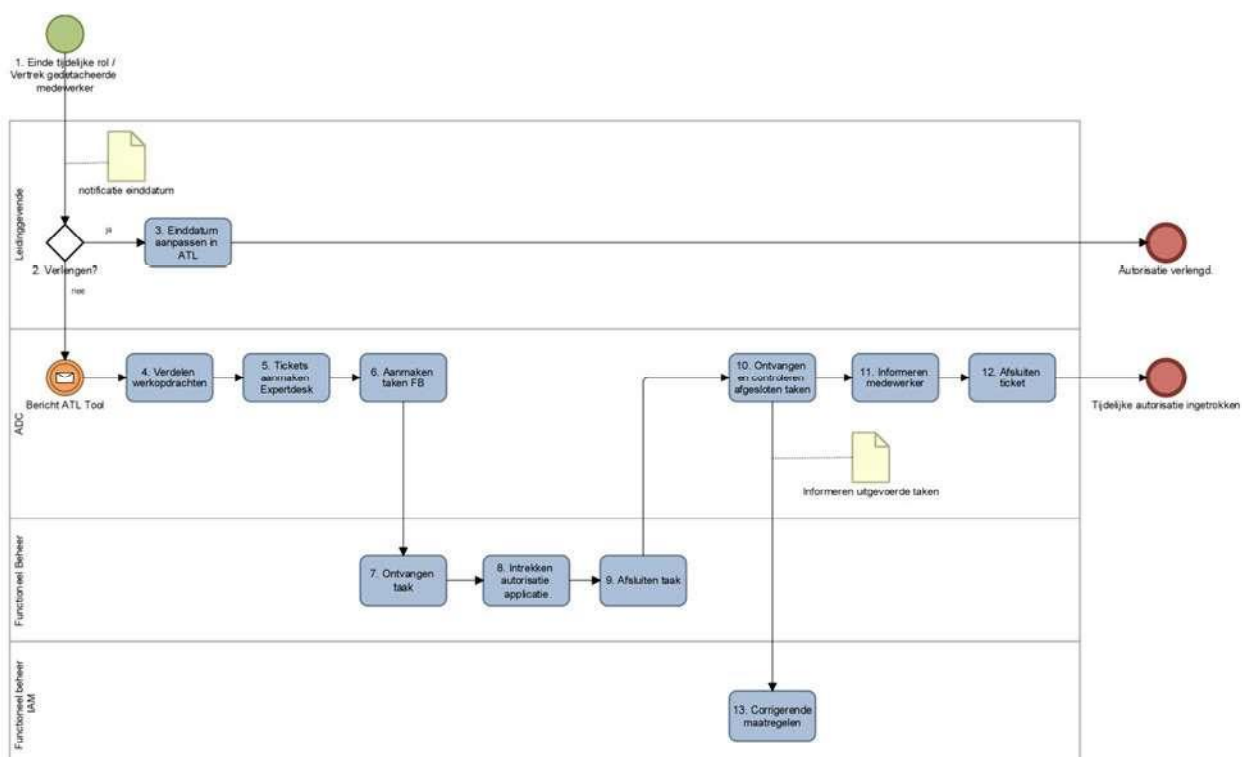
**Figuur 6: IAM16 - autoriseren met ATL**

Processtap	Omschrijving	Responsible	Waarmee
16.1	De leidinggevende van de afdeling waar de medewerker tijdelijk werkzaam wordt (of een medewerker van de afdeling die tijdelijk een andere rol krijgt binnen die afdeling) kent de autorisaties toe via de ATL.	Leidinggevende	ATL

16.2	Staat de applicatie op de lijst van applicaties waarvoor de autorisatie via het vier-ogen principe moet worden goedgekeurd? Nee: ga naar 16.5 Ja: ga naar 16.3	Leidinggevende	ATL
16.3	De autorisatie moet bevestigd worden door de bevoegde functionaris. Indien dit positief is: ga naar 16.5 Indien afgewezen, ga naar 16.4	Bevoegde functionaris	ATL
16.4	Autorisatie wordt afgewezen. De leidinggevende informeert de medewerker dat de autorisatie niet is toegekend.	Leidinggevende	
16.5	Het ADC kijkt welke werkopdrachten nodig zijn voor de verdere verwerking (voor welke beheerders, wat er moet worden geautoriseerd etc.) De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	
16.6	Het ADC maakt een ticket aan in Expertdesk. De verdere uitwerking van deze taak staan in de instructies voor het ADC.	ADC	Expertdesk
16.7	Onder het ticket worden de relevante taken voor de oplosgroepen aangemaakt. De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk
16.8	De oplosgroepen (Functioneel Beheer teams) nemen de taak in ontvangst. De verdere uitwerking van deze taak staan in de instructies bij FB).	FB	Expertdesk
16.9	FB voert een check uit ter controle op mogelijke functiemenging die niet is toegestaan (maar door IAM nog niet kan worden aangegeven).FB mailt het wachtwoord naar het ADC.	FB	Beheertool van de applicatie
16.10	FB sluit zijn taak af.	FB	Expertdesk
16.11	De afgesloten taken worden gecontroleerd en FB IAM wordt geïnformeerd over wat er is uitgevoerd en wat niet.	ADC	mail
16.12	De medewerker wordt geïnformeerd dat de toegang tot de applicatie is geregeld en krijgt zijn wachtwoord (tenzij de applicatie een single sign – on constructie kent, want dan is het wachtwoord niet relevant) )	ADC	
16.13	Het ticket wordt afgesloten.	ADC	Expertdesk

16.14	Wanneer vanuit de berichtgeving van het ADC blijkt dat er taken zijn die niet zijn uitgevoerd, moet FB IAM herstelacties uitvoeren. Dit betekent een analyse van het niet kunnen uitvoeren van het verzoek en op basis van de uitkomst en de corrigerende maatregelen nemen.	FB IAM	
-------	--	--------	--

### 1.1.5 IAM17.0 De-autoriseren met ATL



Figuur 7: IAM17 - de-autoriseren met ATL

Processtap	Omschrijving	Responsible	Waarmee
17.1	De leidinggevende van de afdeling waar de medewerker tijdelijk werkzaam is trekt de autorisaties in via de ATL. Daarnaast kan een autorisatie automatisch worden ingetrokken als de einddatum van de TTW wordt overschreden. <sup>1</sup> In dit laatste geval worden de leidinggevende en applicatiegebruiker vooraf (30 dagen) gewaarschuwd,	Leidinggevende	

<sup>1</sup> De veld einddatum TTW wordt bij het opvoeren van een TTW. Wanneer de leidinggevende dit niet invult, wordt de default waarde van de einddatum op 9 maanden gezet.

	zodat de leidinggevende een eventuele verlenging kan doorvoeren.		
17.2	De leidinggevende besluit of de tijdelijke autorisatie verlengd moet worden.	Leidinggevende	
17.3	Als de tijdelijke autorisatie moet worden verlengd, dan past de leidinggevende de einddatum aan in de ATL. Wanneer de tijdelijke autorisatie niet wordt verlengd, dan hoeft de leidinggevende niets meer te doen. Er wordt dan op de vervaldatum automatisch een mail naar het ADC gestuurd.	Leidinggevende	ATL
17.4	Het ADC kijkt welke werkopdrachten nodig zijn voor de verdere verwerking (voor welke beheerders, wat er moet worden ingetrokken etc.) De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	
17.5	Het ADC maakt een ticket aan in Expertdesk. De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk
17.6	Aan het ticket worden de relevante taken voor de oplosgroepen aangemaakt. De verdere uitwerking van deze taak staat in de instructies voor het ADC.	ADC	Expertdesk
17.7	De oplosgroepen (Functioneel Beheer teams) nemen de taak in ontvangst. De verdere uitwerking van deze taak staat in de instructies bij FB).	FB	Expertdesk
17.8	Toegang tot de applicatie wordt ingetrokken.	FB	Beheertool van de applicatie
17.9	FB sluit de taak af. Wanneer de taak niet uitgevoerd kon worden, dan wordt dit met reden vermeld in de taakafsluiting.	FB	Expertdesk
17.10	De afgesloten taken worden gecontroleerd en FB IAM wordt geïnformeerd over wat er is uitgevoerd en wat niet.	ADC	mail
17.11	De medewerker en leidinggevende wordt geïnformeerd dat de toegang tot de applicatie is ingetrokken.	ADC	
17.12	Het ticket wordt afgesloten.	ADC	Expertdesk
17.13	Wanneer vanuit de berichtgeving van het ADC blijkt dat er taken zijn die niet zijn uitgevoerd, moet FB IAM herstelacties uitvoeren. Dit betekent een analyse van het niet kunnen uitvoeren van het verzoek en op basis	FB IAM	

	van de uitkomst en de corrigerende maatregelen nemen.		

## 5 Performance Indicatoren

Performance indicatoren worden opgesteld door de proceseigenaar en vastgelegd in het Monitoring&Controlplan.

Enkele voorbeelden die het (de)autoriseren steunen:

1. Het aantal uitgevoerde autorisaties in een periode
2. Het aantal niet uitgevoerde autorisaties, gecategoriseerd op oorzaak.
3. De applicaties die via de ATL worden toegekend en bij welk team/eenheid dit voorkomt
4. Aantal accounts zonder dienstverband
5. Aantal accounts die niet zijn toegekend aan een applicatie.
6. Aantal autorisaties binnen afgesproken termijn toegekend
7. Aantal de-autorisaties uitgevoerd in een periode
8. Aantal de-autorisaties binnen afgesproken termijn uitgevoerd
9. Aantal tijdelijk toegekende autorisaties in een periode
10. Aantal ingetrokken tijdelijk toegekende autorisaties in een periode

## 6 Escalatie en navraag

Wanneer er geen terugkoppeling op het autorisatieverzoek richting leidinggevende en/of eindgebruiker is gekomen kan dit verschillende redenen hebben. De coördinatie van het achterhalen van de oorzaak ligt bij de ADC.

De ADC zal eerst Functioneel Beheer van de applicatie benaderen als blijkt dat daar nog tickets openstaan en wat het beletsel is. De meeste vertragingen kunnen op deze manier worden verhelderd en opgelost worden.

Wanneer blijkt dat de opdracht nooit door de ADC is ontvangen (en richting Functioneel Beheer van de applicatie is gestuurd), wordt de profielenbeheerder door de ADC benaderd en gekeken of er een fout in het autorisatieprofiel zit (een verkeerde AD groep, het bericht komt niet aan bij de juiste oplosgroep, of er komt geen bericht bij oplosgroep etc.).

De profielenbeheerder zal met de Functioneelbeheer van de applicatie of met de IV-expert op zoek gaan naar de juiste en actuele workflow informatie. Correcties op het profiel worden door middel van RFC's doorgevoerd.

De ADC is te bereiken via e-mail: [5.1.2.1@politie.nl](mailto:5.1.2.1@politie.nl)

Er is geen direct telefonisch contact mogelijk. Indien gewenst kunnen de coördinatoren van de ADC worden benaderd.

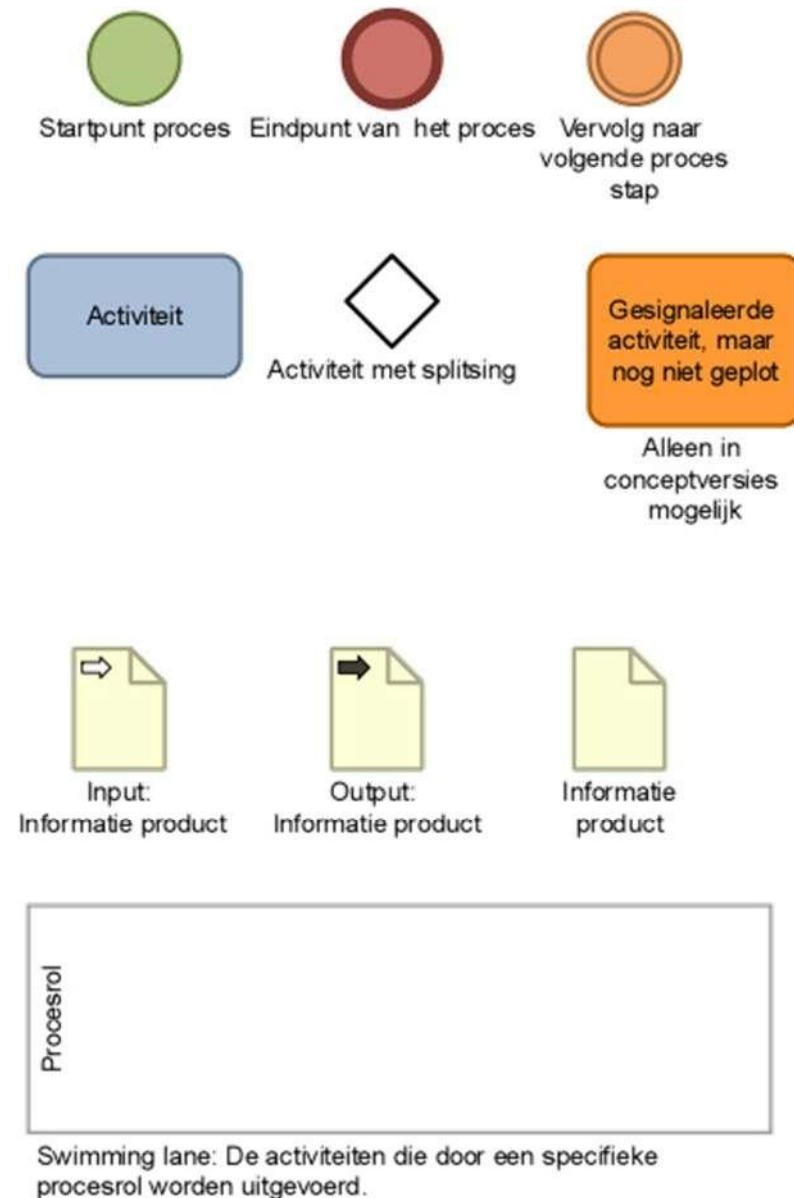
## 7 Begrippenlijst

begrip	Uitleg
AD	Active Directory
ADC	AutorisatieDesk Centraal
ATL	Autorisatie Tool Leidinggevende: het hulpmiddel voor de leidinggevende om extra tijdelijke autorisatie toe te kennen aan (één van) zijn medewerkers.
EBO	Eigen Beheerde Omgeving: Een ICT omgeving die door een eenheid wordt beheerd en niet door de dienst IM en/of dienst ICT. In jargon: een "Shadow IT omgeving", waarvoor de PDC geen zorg draagt.
HRA	HR administratie
IDU	Afkorting voor de instroom van nieuwe medewerkers, de doorstroom van medewerkers (veranderen van functie of team) en de uitstroom van medewerkers bij de politie.

# 8 Bijlage 1: Legenda workflows

## 8.1 Legenda

Hieronder staan de symbolen die worden gebruikt in de schematische weergave van de procesflows in dit document.



## 8.2 Nummering van de processen en activiteiten

IAMx.0 Een 0 betekent dat het hier gaat om een werkproces in zijn geheel: voorbeeld: IAM13.0 is Autoriseren Instroom

IAMx.y De activiteit binnen een werkproces: voorbeeld: IAM13.3 is activiteit 3 (Importeren gegevens), binnen werkproces 13 (Autoriseren Instroom)

## 9 Bijlage 2: Ondertekend Protocol van Oplevering

(klik op het PVO om het document te openen)



### Protocol van Oplevering

0000000000  
Aanvraagnummer  
12345

5.1.2.e

Definitief

Versie 4

Versie datum 7 september 2017

Rubricering Politie INTERN

« waakzaam en dienstbaar »