Informatieclassificatie Vlaamse overheid (Vo-ICR)

Identity en access management (IAM)

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen Identity en access management (IAM). Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 2 delen. Eerst worden de minimale maatregelen besproken alvorens in het tweede deel al de nodige aanvullende informatie ter beschikking wordt gesteld.

De organisatie van de maatregelen in het kader van informatieclassificatie wordt beschreven in het document 'Vo informatieclassificatie – Organisatie - Informatieclassificatieraamwerk'.

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

	Datum	Auteur	Opmerkingen
v.0.1	27 november 2017	Wim BROOS	Eerste draft
v.0.2	18 december 2017	Wim BROOS	Eerste review
v.0.3	23 januari 2018	Johan SMEKENS	Review
v.0.4	29 januari 2018	Pieter LENAERTS Johan SMEKENS	Review en aanvullende documentatie
v.0.5	1 februari 2018	Johan SMEKENS	Review workshop feedback
v.0.6	8 februari 2018	Johan SMEKENS	Aanvulling 'autorisatie'
v.0.7	13 februari 2018	Johan SMEKENS	Voorbereiding 1ste publieke review
v.1.0	25 juni 2020	Beau JANSSEN	Toevoeging maatregelen en context "Integriteit" Tekstuele aanpassingen
v.1.1	13 juli 2020	Beau JANSSEN	Herwerking input Kristel Van Aken
v.1.2	27 augustus 2020	Beau JANSSEN	Toevoegingen na Taakgroep van 27/08/2020
v.1.3	13 juli 2021	Beau JANSSEN	Toevoeging maatregelen en context "Beschikbaarheid"
v.2.0	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
V.2.1	17 oktober 2023	Nele Lowet	Update KSZ

Bronnen en verwijzingen

De inhoud van dit document werd samengesteld op basis van een workshops en gesprekken met het HFB IDM/ACM team en het BOSA[2].

Documentverwijzingen:

- Vo Informatieclassificatie – Organisatie Informatieveiligheid (PDF)
- Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk (PDF)
- FAS/CSAM als identity provider
- ItsMe als identity provider
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eID.AS)

Inhoudsopgave

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	〉 Identificatie: Geen identificatie vereist 〉 Authenticatie: Geen authenticatie vereist 〉 Autorisatie: Geen autorisatie vereist 〉 Beschrijf de Soll/Ist van je toepassing

	Alle maatregelen van Klasse 1 +
	
	〉 Identificatie: Zwakke identificatie
	〉 Authenticatie:
	  〉 eIDAS LAAG
	  〉 Beheer van status van account
	  〉 Bescherming van het paswoord in opslag en in transit. Bij federatie van de authenticatie, het verzekeren van gelijkaardige controles bij de derde partij
	〉 Autorisatie: Autorisatie op basis van technische of organisatorische criteria
	  〉 Technisch: **Geauthentiseerde** gebruikers, zonder lidmaatschap tot een autorisatie rol.
	  〉 Organisatorisch: Geauthentiseerde gebruikers, met toekenning tot autorisatie rol op basis van lidmaatschap binnen de organisatie (of een deel ervan). Dit doe je middels een Soll/Ist-beschrijving.
	〉 Bescherming van identificatiegegevens die toegang geven tot toepassingen. De identificatiegegevens zelf zijn klasse 3 voor Vertrouwelijkheid en 4 voor Integriteit en moet je beschermen met cryptografische controles

	Alle maatregelen van Klasse 1 + Klasse 2 +
	
	〉 Identificatie: Sterke identificatie
	〉 Authenticatie maatregelen: eIDAS SUBSTANTIEEL
	〉 Autorisatie:
	  〉 Autorisatie registratie via toegangsbeheerproces (IDM)
	  〉 Autorisatie op basis van functionele groep, deze functionele groep mag gedeeld worden door meerdere (deel-) applicaties
	  〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie.

	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 + 〉 Sterke identificatie via de federale overheid 〉 Authenticatie maatregelen:

	〉 eIDAS SUBSTANTIEEL 〉 SSO via ACM voor gebruikers Vlaamse Overheid. 〉 Autorisatie: 〉 Autorisatie registratie via toegangsbeheerproces (IDM) 〉 Autorisatie op basis van functionele groep, deze functionele groep mag **niet gedeeld** worden door meerdere (deel-)applicaties 〉 Autorisatie validatie: 〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie 〉 Validatie met goedkeuring van een door de organisatie geautoriseerd tweede persoon. 〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp of de toepassingsbeheerder. 〉 Jaarlijkse periodieke herziening van de toegangen.<
	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 + Klasse 4 + 〉 Sterke identificatie via de federale overheid 〉 Authenticatie maatregelen: 〉 eIDAS SUBSTANTIEEL 〉 SSO via ACM voor gebruikers Vlaamse Overheid. 〉 Autorisatie: 〉 Autorisatie registratie via toegangsbeheerproces (IDM) 〉 Autorisatie op basis van functionele groep, deze functionele groep mag **niet gedeeld** worden door meerdere (deel-)applicaties 〉 Autorisatie validatie: 〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie 〉 Validatie met goedkeuring van door twee door de organisatie geautoriseerde personen, waarvan minimaal één zonder hiërarchische of functionele relatie met het onderwerp. 〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp of de toepassingsbeheerder, waarna de veiligheidscoördinator de finale validatie bevestigd. 〉 Jaarlijkse periodieke herziening van de toegangen

Integriteit

IC klasse	Minimale maatregelen
	〉 Identificatie: Geen identificatie vereist 〉 Authenticatie: Geen authenticatie vereist 〉 Autorisatie: Geen autorisatie vereist

	〉 Beschrijf de Soll/Ist van je toepassing

	Alle maatregelen van Klasse 1 +
	
	〉 Identificatie: Zwakke identificatie
	〉 Authenticatie:
	  〉 eIDAS LAAG
	  〉 Beheer van status van account
	  〉 Bescherming van het paswoord in opslag en in transit. Bij federatie van de authenticatie, het verzekeren van gelijkaardige controles bij de derde partij
	〉 Autorisatie: Autorisatie op basis van technische of organisatorische criteria
	  〉 Technisch: **Geauthentiseerde** gebruikers, zonder lidmaatschap tot een autorisatie rol.
	  〉 Organisatorisch: Geauthentiseerde gebruikers, met toekenning tot autorisatie rol op basis van lidmaatschap binnen de organisatie (of een deel ervan). Dit doe je middels een Soll/Ist-beschrijving.
	〉 Bescherming van identificatiegegevens die toegang geven tot toepassingen. De identificatiegegevens zelf zijn klasse 3 voor Vertrouwelijkheid en 4 voor Integriteit en moet je beschermen met cryptografische controles

	Alle maatregelen van Klasse 1 + Klasse 2 +
	
	〉 Identificatie: Sterke identificatie
	〉 Authenticatie maatregelen: eIDAS SUBSTANTIEEL
	〉 Autorisatie:
	  〉 Autorisatie registratie via toegangsbeheerproces (IDM)
	  〉 Autorisatie op basis van functionele groep, deze functionele groep mag gedeeld worden door meerdere (deel-) applicaties
	  〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie.

	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3
	
	〉 Sterke identificatie via de federale overheid
	〉 Authenticatie maatregelen:
	  〉 eIDAS SUBSTANTIEEL
	  〉 SSO via ACM voor gebruikers Vlaamse Overheid.
	〉 Autorisatie:
	  〉 Autorisatie registratie via toegangsbeheerproces (IDM)
	  〉 Autorisatie op basis van functionele groep, deze functionele groep mag **niet gedeeld** worden door meerdere (deel-)applicaties
	〉 Autorisatie validatie:
	  〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie
	  〉 Validatie met goedkeuring van een door de organisatie geautoriseerd tweede persoon.

	〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp of de toepassingsbeheerder 〉 Jaarlijkse periodieke herziening van de toegangen
	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 + Klasse 4 + 〉 Sterke identificatie via de federale overheid 〉 Authenticatie maatregelen: 〉 eIDAS SUBSTANTIEEL 〉 SSO via ACM voor gebruikers Vlaamse Overheid. 〉 Autorisatie: 〉 Autorisatie registratie via toegangsbeheerproces (IDM) 〉 Autorisatie op basis van functionele groep, deze functionele groep mag **niet gedeeld** worden door meerdere (deel-)applicaties 〉 Autorisatie validatie: 〉 Onderwerp mag niet deelnemen aan de validatie van de betrokken autorisatie 〉 Validatie met goedkeuring van door twee door de organisatie geautoriseerde personen, waarvan minimaal één zonder hiërarchische of functionele relatie met het onderwerp. 〉 Voorbeeld: Lokale beheerder doet de registratie en deze wordt gevalideerd door de leidinggevende van het onderwerp of de toepassingsbeheerder, waarna de veiligheidscoördinator de finale validatie bevestigd. 〉 Jaarlijkse periodieke herziening van de toegangen

Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 De processen om een gebruiker te identificeren, authenticeren en te autoriseren moeten even beschikbaar zijn als de toepassing waartoe toegang verleend wordt.

1.2 Minimale specifieke (GDPR) maatregelen

De minimale algemene maatregelen voor IAM moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing (zie hoofdstuk 'minimale algemene maatregelen').

Er zijn geen specifieke GDPR maatregelen voor IAM.

1.3 Minimale specifieke (NISII) maatregelen

In afwachting van de goedkeuringen omtrent NISII is er in dit document alvast de nodige ruimte voorzien voor toekomstige minimale specifieke NISII maatregelen.

1.4 Minimale specifieke (KSZ) maatregelen

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van IAM toegepast worden:

Beschikbaarheid, Integriteit & vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Elke organisatie moet de toegang tot de gegevens nodig voor de toepassing en de uitvoering van de sociale zekerheid beveiligen door middel van een identificatie-, authenticatie- en autorisatiesysteem. (Ref. KSZ 5.6.3). 〉 Elke organisatie moet de toegang van informatiebeheerders tot informaticasystemen beperken door identificatie, authenticatie, en autorisatie (Ref. KSZ 5.6.5). 〉 Elke organisatie moet de gepaste maatregelen treffen opdat iedere persoon slechts toegang zou hebben tot de diensten waarvoor hij uitdrukkelijk een autorisatie heeft verkregen (Ref. KSZ 5.6.6).

1.5 Overzicht en integratie van de maatregelen

Onderstaande tabellen geven overzicht van de integratie van de verschillende maatregelen. De maatregelen moet je combineren. Elke toepassing heeft én een klasse voor Vertrouwelijkheid én een klasse voor Integriteit. Je moet de controles voor beide kwaliteitskenmerken implementeren.

Gerelateerd aan Vertrouwelijkheid

	Type data	Afscherming	Minimaal identificatieniveau	Minimaal authenticatie niveau	Minimaal autorisatie niveau	Frequentie review Soll	Frequentie review Ist
1	Publiek	Permissief [1]	**Geen**	**Geen**	**Niet van toepassing**	Jaarlijks	Minstens 1 keer per jaar
2			**Zwak**	**Zwak**	**Geauthentiseerd**		
3	Functioneel		**Sterk**	**Substantieel**	**Functioneel** [3]		Minstens 2 keer per jaar
4		Restrictief [2]	**Sterk**	**Substantieel**	**Strikt functioneel** [4]		
5			**Sterk**	**Substantieel**	**Hoofdelijk** [5]		**Minstens 4 keer per jaar**

Gerelateerd aan Integriteit

	Toegangsniveaus in toepassing	Soort identificatie	Uitwisselen van identificatie-gegevens	Beveiliging van paswoord	Frequentie review Soll	Frequentie review Ist	Validatie van autorisatie
1	Optioneel	Zwak	Optioneel	Verplicht	Jaarlijks	Minstens 1 keer per jaar	Optioneel
2							
3	Verplicht	Sterk	Verplicht			Minstens 2 keer per jaar	Verplicht
4							
5						**Minstens 4 keer per jaar**	

Gerelateerd aan Beschikbaarheid

	Toegangsniveaus in toepassing	Soort identificatie	Uitwisselen van identificatie-gegevens	Beveiliging van paswoord	Frequentie review Soll	Frequentie review Ist	Validatie van autorisatie
1	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing	Jaarlijks	Minstens 1 keer per jaar	Niet van toepassing
2						Minstens 2 keer per jaar	
3							
4						**Minstens 4 keer per jaar**	
5							

Afscherming van informatie

We gebruiken de onderstaande basisprincipes

[1] Permissief: Er worden geen specifieke maatregelen genomen om toegang tot informatie af te schermen of te controleren voor geprivilegieerde accounts. Het *least access* principe blijft altijd gerespecteerd.

[2] Restrictief: Er worden steeds maatregelen genomen om toegang tot informatie af te schermen voor niet geautoriseerde toegangen. (ACL-hygiëne) Voor geprivilegieerde toegangen worden een aantal bijkomende maatregelen geïmplementeerd, waaronder encryptie maatregelen, en controlemaatregelen zoals PAM, Audit trailing, …

Het least access principe is altijd bevestigd in de risicoanalyse.

Minimaal identificatie niveau

Zie identificatie

Minimaal authenticatie niveau

Zie eIDAS

Minimaal autorisatie niveau

We gebruiken lidmaatschap van organisatie (incl. technische organisatorische maatregelen) als basis voor toegang tot publieke informatie.

Bij alle andere informatietypes groeperen we het criteria onder de term ‘functioneel’. Deze behoefte (criteria) is niet alleen een beveiligingsmaatregel, gekend als het *least access* principe, maar het is ook expliciet opgelegd door de toepasbare regelgeving

Functionele relatie met de informatie, zie criteria GDPR Art. 5

[3] Functioneel: De gebruiker motiveert zijn toegang tot informatie op basis van een functionele behoefte met betrekking tot verwerking van de betrokken informatie.

[4] Strikt functioneel: De gebruiker motiveert zijn tijdelijke toegang tot informatie op basis van een functionele behoefte met betrekking tot verwerking van de betrokken informatie en deze behoefte wordt bevestigd door minimaal één geïdentificeerde en geautoriseerde individu. De betrokken eindgebruiker is uitgesloten in het validatie proces.

Het beperken van de duur van de toegangen wordt sterk geadviseerd om het *least access* principe te versterken. Toegangen worden minimaal jaarlijks herzien

[5] Hoofdelijk: De gebruiker motiveert zijn tijdelijke toegang tot informatie op basis van een functionele behoefte met betrekking tot verwerking van de betrokken informatie en deze behoefte wordt bevestigd door minimaal twee geïdentificeerde en geautoriseerde individuen. De betrokken eindgebruiker is uitgesloten in het validatie proces.

De duur van de toegangen worden beperkt tot de functionele behoefte en worden minimaal jaarlijks herzien

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Identificatie als maatregel

2.1.1. Verwachtingen rond de kenmerken van de identificatiemaatregelen

Identificatieprocessen kunnen we opsplitsen in zwakke versus sterke identificatie. Beide hebben implicaties rond vertrouwelijkheid en integriteit.

Zwakke identificatie

Zwakke identificatie: Validatie van de identiteit van een fysiek persoon op basis van een identiteitsattribuut dat niet onder controle valt van een door de overheid geregistreerde of gecertifieerde bron:

De gebruikte identiteit attributen komen voor het identificatie- of registratieproces van een al dan niet commerciële organisatie.
De identiteit is niet geverifieerd via een door de Belgische federale overheid erkende procedure.

- De verificatieprocedure biedt minimale waarborg.

Opmerking: De Vlaamse overheid beschouwt elke bron als commercieel, ook als de gerelateerde dienst 'gratis' wordt aangeboden.

- Identificatie gebeurt op basis van (Niet-gelimiteerde voorbeelden)

  Een e-mailadres
  Een telefoonnummer
  Een (roep)naam

Bv: Sociale media, online winkelplatform, intekenen nieuwsbrief, ...

Opmerking: Hoewel er bij zwakke identificatie minder zekerheid is over de exacte identiteit van de gebruiker dan bij een sterke identificatie, spreken we hier wel degelijk over persoonsgegevens. Zwakke identificatie impliceert niet dat er minder controles nodig zijn om de vertrouwelijkheid en integriteit van deze persoonsgegevens te verzekeren.

Sterke identificatie

Sterke identificatie: Identificatie op basis van een door de Belgische federale overheid geregistreerde of gecertifieerde bron (Identity provider).

De Vlaamse overheid gebruikt als **Identity provider** het identificatieproces van de Belgische federale overheid. Dit geeft aan dat (vandaag) enkel de Federale overheid een sterke validatie van een identiteit kan uitvoeren om te voldoen aan de kenmerken van een sterke identificatie.

De unieke identificatie labels van een **identiteit** (Fysiek persoon) zijn:

- Rijksregisternummer (Ook gekend als RRN)
- Rijksregister-BIS nummer (Ook gekend als BIS-Nummer)

Opmerking: *Binnen de Vlaamse overheid gebeurt de registratie van identiteiten voor fysieke personen, binnen onze access managementprocessen, steeds op basis van het RRN of BIS-Nummer.*

Beperkingen voor buitenlandse identiteiten in gebruik bij de Vlaamse overheid

Volgende situatie is van toepassing op alle individuen met een identiteit die de federale overheid erkent.

- De uitwisselbaarheid van identiteiten van buitenlandse individuen, ook binnen de EU is opgevangen door de registratie van het individu in het RijksRegister-BIS
- Dit bisnummer wordt overgenomen als unieke bron voor een identiteit binnen de Vlaamse overheid

Naar de toekomst toe zullen alle EU *identity providers* de mogelijkheid bieden om identiteiten én de validatie ervan onderling uit te wisselen. Deze integratie zal worden gerealiseerd door de Belgische federale overheid in Europese context (zie bronnen).

Erkende afgeleide bronnen voor sterke identificatie

Een aantal erkende afgeleide bronnen worden gebruikt binnen:

De Belgische federale overheid

- INSZ: Identificatienummer van de sociale zekerheid, gedefinieerd door het sectoraal comité van de sociale zekerheid.
- ItsMe® identificatie validatie

ItsMe® *De veiligheid van het ItsMe®-platform en bijhorende toepassing werd beoordeeld op basis van een controle raamwerk welke FOD BOSA in het leven heeft geroepen, voor de evaluatie van identificatiemiddelen onder het Koninklijk besluit van 08/11/2017 tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor overheidstoepassingen. Zie link naar de publicatie in het staatsblad.*

De Vlaamse overheid

Deze van de federale overheid (zie boven)
VoID: Uniek identiteitslabel, toegepast op zowel RRN als BIS-Nummer identiteiten, binnen de access management processen bij de Vlaamse overheid.

2.1.2. Kwaliteitskenmerken van het identificatieproces

De gegevens die we in het identificatieproces gebruiken, zijn persoonsgegevens en hebben altijd een bepaalde graad van vertrouwelijkheid, integriteit en beschikbaarheid, ongeacht of we zwakke of sterke identificatie gebruiken. Dit moet ervoor zorgen dat tijdens het identificatieproces er voldoende controles in gebruik zijn om beide kwaliteitskenmerken te borgen. Concreet betekent dat deze gegevens volgende klasse toebedeeld krijgen:

- Informatieklasse 3 voor Vertrouwelijkheid

- Informatieklasse 4 voor Integriteit
- De informatieklasse voor Beschikbaarheid is gealigneerd met de classificatie van de toepassing waarvoor de identificatie dient. De maatregelen die je inricht moeten deze beschikbaarheid kunnen garanderen

2.1.3. Integriteit van het identificatieproces

Toegangsniveaus binnen toepassingen, of infrastructuur

Bij het registreren van de identiteit van een gebruiker, houdt de beheerder rekening met de mogelijkheid dat de gebruiker normale gegevens (normale gebruiker) of zelfs systeemeigenschappen (beheerder) zal kunnen passen. Het gaat dus verder dan de vraag tot welke gegevens de gebruiker toegang zal hebben.

Je moet hiermee logica rekening houden in de opzet en toekenning van de rollen binnen de toepassing en haar beheer. Hierbij is het van belang dat de toegang die in de rollen vervat zit, altijd tweedelig is: de vertrouwelijkheids- en integriteitseisen gaan bepalen wie waartoe toegang zal kunnen krijgen.

ACM *Het opzetten van rollen binnen een toepassing en het juist toewijzen van deze rollen aan gebruikers kun je met de Veiligheidsbouwsteen Toegangsbeheer (ACM). Deze bouwsteen houdt in haar ontwerp rekening met alle noodzakelijke controles die het ICR oplegt.*

Relatie van de kwaliteitskenmerken met zwakke, resp. sterke identificatie

Hoe hoger de informatieklasse, hoe hoger de nood tot een sterke identificatie. Dit geldt voor alle drie kwaliteitskenmerken:

- Hoe groter de impact van informatie die (onvrijwillig) publiek vrijkomt, hoe zekerder we moeten zijn dat enkel de meest noodzakelijke personen toegang hebben tot die informatie
- Hoe groter de impact van foutieve informatie kan zijn, hoe zekerder we moeten zijn dat enkel de gemachtigde gebruikers ze kunnen wijzigen
- Hoe groter de impact van de onbeschikbaarheid van een toepassing of proces, hoe zekerder we moeten zijn van een correcte toegangsverlening

De exacte *requirements* hiervoor staan opgelijst in het Overzicht en integratie van de maatregelen.

Combinatie van Vertrouwelijkheid, Integriteit en Beschikbaarheid

Belangrijk hierbij is dat de controles per klasse gecombineerd werken. Staat een controle bij meerdere kwaliteitskenmerken beschreven, dan implementeer je de strengste van beide criteria. Bijvoorbeeld: je moet voor Vertrouwelijkheid 3 en voor Integriteit 4 data encrypteren, maar voor I4 moet je een zwaardere sleutel gebruiken dan voor C3. Dan moet je voor deze data de strengste sleutel van de twee gebruiken. Komt een controle maar in een van de twee categorieën voor, dan moet je die uiteraard ook nog steeds implementeren.

2.1.4. Integriteit van de gegevens betrokken in het identificatieproces

Beveiliging van de uitgewisselde data

Tijdens het identificatieproces, wisselen systemen heel wat data uit. Hierbij ook persoonsgegevens[3] van de persoon die ze identificeren. Hierbij hou je ook rekening met de informatieklasse wat betreft integriteit. De controles die je hierbij zeker moet implementeren, staan beschreven in het Organisatiedocument.

Dit geldt heel specifiek ook voor gegevens die systemen uitwisselen om een persoon te identificeren. Dit is informatie van klasse 3 voor Vertrouwelijkheid en klasse 4 voor Integriteit, met alle noodzakelijke controles die hiermee gepaard gaan.

In de praktijk komt dit neer op het versleutelen van informatie. Meer details hierover vind je in het Beleidsdocument “Cryptografie”.

De exacte controles op het gebied van versleuteling staan beschreven in het Beleidsdocument Cryptografie.

Key Management as a Service

Voor het versleutelen van informatie kun je ook gebruik maken van de centraal aangeboden Veiligheidsbouwsteen Key Management as a Service. Deze zorgt ervoor dat je encryptiesleutels correct en veilig bewaard blijven en dat derden er geen toegang toe hebben.

Beveiliging van de opgeslagen identiteiten

De personen die toegang kunnen krijgen tot een toepassing of een systeem, moet je ook ergens opslaan. De database waar deze informatie opgeslagen is, moet je adequaat beschermen.

De informatie van welke identiteiten er bestaan en waartoe deze toegang hebben in een bepaalde toepassing, is informatie van klasse 3 voor Vertrouwelijkheid en klasse 4 voor Integriteit. De maatregelen die hierop van toepassing zijn, staan beschreven in het Organisatiedocument.

Deze informatieklasse geldt voor zowel de Vertrouwelijkheid als de Integriteit. Hiermee moet je garanderen dat de gebruikerslijst vertrouwelijk en integer blijft. Dit helpt om eventuele cyberaanvallen tegen specifieke profielen of gebruikers tegen te gaan.

Identity Management

Om de gebruikte identiteiten correct te beheren, kun je bijvoorbeeld gebruik maken van de centrale Veiligheidsbouwsteen Identiteitsbeheer (IDM). Deze zorgt ervoor dat je altijd weet welk individu achter een gebruiker zit. Je kunt deze makkelijk linken aan het Toegangsbeheer (ACM) zodat je er zeker van bent van welke toegang een gebruiker heeft.

Alternatieve methodes

Je mag alternatieve methodes gebruiken om een persoon te identificeren. Je moet je er wel van vergewissen dat dit even veilig verloopt als de hierboven beschreven methodes.

Dit verifieer je met de verantwoordelijke voor Informatieveiligheid van je entiteit die dit overlegt met de CISO. Als er aan deze methodes (rest)risico's verbonden zijn, moet het topmanagement deze ook in de mate van het mogelijke mitigeren of accepteren.

De normen waaraan je moet voldoen komen, zoals hierboven beschreven, overeen met klasse 3 voor vertrouwelijkheid en klasse 4 voor integriteit.

2.1.5. Beschikbaarheid van de gegevens betrokken in het identificatieproces

Link met informatieklasse van de toepassing/het proces

De gegevens die gelinkt zijn aan het identificatieproces moeten even beschikbaar zijn als de toepassing of het proces waarvoor ze dienen. Om de toegang tot een toepassing te kunnen garanderen, moeten deze gegevens leesbaar en verwerkbaar zijn tijdens de operationele werking van de toepassing.

Hou hier ook zeker rekening met piekmomenten, zowel qua gebruik als qua tijdsgevoeligheid. Het Organisatiedocument

Als je gebruik maakt van een identificatieproces onafhankelijk van je eigen toepassing, moet dat uiteraard ook aan deze voorwaarden voldoen.

2.2. Authenticatie als maatregel

2.2.1. Van identiteit tot Account

Authenticatie is het deelproces waarbij een individu zijn identiteit bewijst.

Om dit te doen heb je in de eerste plaats een authentieke bron nodig, een gecontroleerd en betrouwbaar identiteitsregistratieproces dat toelaat de identiteit van een individu te registreren. (Zie Identificatie)

Identiteiten worden gecentraliseerd in het rijksregister en rijksregister-BIS van de Belgische federale overheid maar deze identiteiten zijn niet rechtstreeks bruikbaar als authenticatiemiddel. Een gebruiker kan niet simpelweg verwijzen naar dit registratieproces om zijn identiteit te bewijzen. Daarom krijgt het individu een 'middel', dat door iedereen en elke organisatie, op zich erkent wordt als identiteitsreferentie.

Identiteitsbewijzen (inclusief paspoorten, geboortebewijzen, …)

De Belgische identiteitskaart (eID) is het referentiemiddel voor de burger.

Het is echter beperkt inzetbaar als authenticatie bij
Interactieve identificatie tussen fysieke personen
Toepassingen op basis van een authenticatie integratie met de federale CSAM-diensten

Om de beperkingen in gebruik van ons identiteitsbewijs weg te werken gebruikt de Vlaamse overheid een toegangsbeheer systeem, dat toelaat om aangepaste authenticatie middelen aan een identiteit te koppelen, zodat de gebruiker op een aangepaste manier toegang kan krijgen tot applicaties en diensten. Dit authenticatiemiddel noemt men een **account**.

2.2.2. Vorm van het account

De vorm waaronder een account zich voordoet is volledig afhankelijk van de gebruikte technologie.

Fysieke authenticatie vereist het gebruik van een fysiek middel. (Authenticatie tussen personen)
Authenticatie naar een informatie verwerkingssysteem vereist een elektronisch middel

Merk op: *Sommige accountvormen zijn in staat om beide authenticatievereisten samen te brengen. Het Belgische eID ondersteunt zowel fysieke als elektronische authenticatievormen.*

Het aanmaken of ter beschikking stellen van een account gebeurt via het toegangsbeheer.

Het gebruik (proces) van een account om zich kenbaar te maken (= identiteit van de persoon te bewijzen) heet **authenticatie**.
Een account laat enkel toe een gebruiker te identificeren naar een toepassing of dienst. Het moet echter uitgebreid worden met de toestemming om de toepassing of dienst op een bepaalde wijze te gebruiken (zie **autorisatie**)
Een **account** kan verschillende vormen aannemen afhankelijk van de (technische) toepassing.

Enkele voorbeelden:

De **toegangsbadge** (Account) voor de Vo gebouwen, laat toe om de gebruiker (het individu) te identificeren aan de toegangspoort (Authenticatie).

De referentie die de toegangspoort hiervoor gebruikt is een **lijst van accounts** in een database verbonden aan de toepassing: Toegangsbeheer gebouwen

De **Windows gebruiker ID** (Account) laat toe om de gebruiker (het individu) te identificeren bij het aanloggen (Authenticatie) op je werkplek.

De referentie die je werkstation hiervoor gebruikt is een lijst van accounts in een database verbonden aan het werkstation

Windows domain computers:

- Active Directory: ALFA/GID
- Local host
- Windows stand-alone (Gelijkaardig voor andere systemen)
- Local host

Een **applicatie gebruiker** (Account) laat toe om de gebruiker (het individu) te identificeren bij het aanloggen (Authenticatie) op een toepassing.

De referentie die de toepassing gebruikt komt uit een centrale database (LDAP/cLDAP of ACM)

2.2.3. Betrouwbaarheid van het accountbeheerproces

De betrouwbaarheid van een account is rechtstreeks afhankelijk van de kwaliteit van het gebruikte identiteitsbeheersproces. Men kan geen sterke authenticatie garanderen als men geen sterk identificatieproces gebruikt, dat in de eerste plaats de identiteit van de gebruiker, aan wie men een account toekent, kan garanderen.

Account lifecycle

Een *lifecycle* beschrijft alle processen, criteria en doelstellingen van het betrokken object, in dit geval het account object.

Aanmaak van accounts

Het deelproces **aanmaken van een account** wordt bepaald op basis van de aanwezige motivatie van een individu om toegang te krijgen.

Hieruit volgt dat personen die niet geacht worden toegang te hebben tot diensten of informatie geen beschikking mogen hebben tot een (actief) account dat de gebruiker potentieel de mogelijkheid biedt.

Tal van toepassingen baseren zich op enkel geauthentiseerde accounts om toegang toe te staan.

Het account heeft steeds een relatie met een identiteit van een fysiek persoon.

Gebruik steeds, waar mogelijk een sterke identificatie van de fysieke persoon. Vanaf informatieverwerking **[klasse 3]** is het gebruik van een sterke identificatie verplicht.

Een niet gemotiveerde toegang beschouwt men als niet geautoriseerde toegang.

Categorieën, types en status van accounts

Elk van de onderstaande account categorieën en types zijn volledige gedocumenteerd in:

Policy documenten (vb. gebruiks- en paswoord policies)
Gebruikers documentatie

Account categorieën

Gebruikersaccount(s) zijn accounts die gebruikt worden voor reguliere eindgebruikerstoegangen voor informatieverwerking tot en met **[KLASSE 4]**

Geprivilegieerd(e) account(s) zijn accounts waaraan met potentieel geprivilegieerde toegangen worden verleend. Een geprivilegieerde toegang is een toegang die de gebruiker (van het account) de mogelijkheid geeft om

Informatie van **[Klasse 5]** (minimaal) in te kijken
De beschikbaarheid en/of gedrag van de gegevensverwerking te beïnvloeden.

Account types

Persoonlijk(e) account(s) zijn accounts met een rechtstreekse relatie tot één individu.

- Vb. Reguliere gebruikersaccounts

Gedeeld(e) account(s) zijn accounts die gedeeld kunnen worden onder verschillende individuen. Deze accounts hebben ALTIJD een relatie tot een uniek individu via een rol: Toepassingsbeheerder.

Toepassingsaccount(s) zijn accounts gebruikt worden als authenticatie voor toepassingen onderling. Deze accounts hebben ALTIJD een relatie tot een uniek individu via een rol: Toepassingsbeheerder.

Systeemaccount(s) zijn accounts die deel uitmaken van het resultaat van installatie van het betrokken systeem. Deze accounts zijn ook gekend als **built-in account(s)**

Status van een account

Een account is actief wanneer het technisch de mogelijkheid biedt om gebruikt te worden als authenticatiemiddel

De criteria om een actief account te beschouwen zijn afhankelijk van de vorm waarin het account werd aangeleverd

Een account is inactief wanneer het op basis van de criteria uitgesloten werd als actief account. Een account kan bvb tijdelijk geblokkeerd (*disabled*) of slechts gebruikt tijdens bepaalde uren (bvb kantooruren).

Controlemaatregel

Inventarisatie van alle bestaande accounts, inclusief het type en bijhorende categorie met volgende indicatoren. Op basis hiervan kunnen bijkomende maatregelen worden ingevuld:

Slapend(e) account(s): Het account is niet meer gemotiveerd indien het niet werd gebruikt in de laatste 13 maand. De status actief, of inactief heeft geen invloed op de status

Ongemotiveerd(e) account(s): Het account is niet gekoppeld aan een gevalideerd identiteit van een fysiek persoon

Systemen kunnen technisch gezien ook gebruikt worden als identiteiten. In IAM-context koppelen we accounts steeds aan een fysiek persoon

Het is toegestaan koppeling te maken via een toepassing, waarachter onrechtstreeks gekoppeld een fysiek persoon, onder vorm van een 'toepassingsbeheerder'. Deze koppeling kan dan geregistreerd worden via de CMDB

Inactief(ve) account(s): De accounts zijn technisch niet in staat deel te nemen aan een authenticatie proces.

Ongecontroleerd(e) account(s): Het account voldoet niet aan de minimale technische vereisten van de paswoordpolicy die werd toegekend aan de account categorie of –type:

- Leeftijd van het paswoord
- Complexiteit van het paswoord
- Omkeerbare encryptie van het paswoord
- Geen paswoord
- …

Provisioning

Provisioning is het deelproces dat wordt gebruikt voor alle activiteiten die leiden tot het verstrekken van een account aan een geïdentificeerd persoon. Afhankelijk van de implementatie van het proces worden accounts actief of inactief aangeleverd aan de rechtmatige persoon. Bij de aanlevering van inactieve accounts zorgt het provisioning proces voor een geautoriseerd en gedocumenteerd activatie (sub)proces.

Provisioning van actieve accounts is toegelaten tot en met informatie **[klasse 2]**

Account factoren worden gescheiden aangeleverd aan de rechtmatige gebruiker

De-provisioning

De-provisioning is het deelproces dat ervoor zorgt dat een account niet langer ter beschikking voor een eindgebruiker als bruikbaar authenticatiemiddel.

Afhankelijk van de vorm van het authenticatiemiddel en/of de-provisioning methodiek spreekt men van verwijderen, deactiveren (blokkeren), *revoke* (weigering), …

De-provisioning kan in een of meerdere stappen worden uitgevoerd. Gefaseerde de-provisioning processen wordt steeds ondersteund door geïdentificeerde behoeften aan het account *lifecycle* proces.

Een account al dan niet tijdelijk deactiveren, vooraleer effectief te verwijderen is afhankelijk van de behoefte om dit account op een later tijdstip te heractiveren.

Indien accounts op basis van geïdentificeerde regelgeving niet effectief verwijderd mogen worden zal deze behoefte expliciet opgenomen zijn in de beschrijvende procesdocumentatie

2.2.4. Betrouwbaarheid van het authenticatieproces

De maatregelen genomen in het account registratie proces worden verder uitgebreid met een aantal technische maatregelen die het dupliceren en oneigenlijk gebruik van een account moeten voorkomen. Men spreekt over de vertrouwelijkheidsgraden van de authenticatie.

eID.AS Authenticatie vertrouwelijkheidsgraden

Op Europees vlak werden een aantal afspraken gemaakt in verband met deze authenticatie vertrouwelijkheidsgraden. Op deze manier kunnen de authenticatieplatformen van de individuele

Europese lidstaten op een uniforme, gestandaardiseerde manier aangeven welke kwaliteitseisen ze stellen aan de vertrouwelijkheid van een authenticatie verzoek.

- eID.AS: EU-verordening voor elektronische identificatie tussen burgers, bedrijven en overheden
  - Deze standaard in opgebouwd op basis van authenticatie vertrouwelijkheidsschalen

Zowel de Belgische federale overheid, als de Vlaamse overheid gebruiken deze uniforme schalen

De eID.AS LoA4 schalen

Deze vertrouwelijkheidsgraden worden onderverdeeld in 3 eID.AS LoA schalen

High	Hoge vertrouwelijkheid van het authenticatieproces, of **sterke authenticatie**
Substantial	Substantiële vertrouwelijkheid van het authenticatieproces, of **betrouwbare authenticatie**
Low	Lage vertrouwelijkheid van het authenticatieproces, of **zwakke authenticatie**

Opmerking: *De authenticatieschalen worden bepaald door de Belgische federale overheid in context van de FAS/CSAM diensten. De Vlaamse overheid neemt deze integraal over en vult deze aan met een aantal authenticatieprocessen voor gebruik binnen de Vlaamse overheid. Deze 'Vo authenticatie processen' kunnen enkel gebruikt worden voor toepassingen en diensten die gericht zijn op intern gebruik.*

De eID.AS LoA schalen in detail

De vertrouwelijkheid van het (technische) authenticatieproces binnen eenzelfde **eID.AS schaal** aangegeven is door een referentiecijfer. Hoe hoger dit cijfer, hoe hoger de vertrouwelijkheid.

eID.AS schaal	*LOA*	*AUTN technologie*	*Identificatie Proces*	*Beschikbaar voor niet-eID houders*
High	500	eID	Sterk	
High	500	MyDigipass	Sterk	
High	450	Erkende partner (eID.AS High)	Sterk	✓
High	450	ItsMe	Sterk	✓
High	450	Vo ACM in scope Vo toepassingen (Incl.SSO)	Sterk	(via RRN-BIS)
Substantial	400	User/pasw + mobiele applicatie of SMS (TOTP)	Sterk	✓
Substantial	400	Erkende partner (eID.AS Substancial)	Sterk	✓
Substantial	400	User/pasw + Qualified certificate (X509)	Sterk	✓
Substantial	TBD	OTP SMTP	Sterk	✓
Low	300	User/pasw + (paper) token	Zwak	✓
Low	200	Alle single factor authenticatie	Sterk	✓
Low	100	Alle single factor authenticatie	Zwak	✓

Gelieve de brondocumentatie van FOD BOSA te gebruiken voor meer detailinformatie.

(Multi)factor-authenticatie

Bij zowel de Belgische federale als bij de Vlaamse overheid ligt de focus op (multi)factor-authenticatie, terwijl we regelmatig ook geconfronteerd worden met terminologie zoals tweefactor-authenticatie

en tweetraps-authenticatie. Ze worden gemakkelijk door elkaar gehaald gezien ze alle drie baseren op dezelfde beginselen. Maar de verschillen zitten hem in de details.

Zoals reeds aangegeven ligt het identificatieproces aan de basis van een succesvolle implementatie van een betrouwbare authenticatie: Om toegang te verlenen tot een toepassing, dienst of netwerk, moet het achterliggende systeem weten dat de persoon die zich aanmeldt ook daadwerkelijk degene is die als wie hij zich voordoet.

Gezien in de meeste implementaties van multifactor-authenticatie men refereert naar 2 factoren is het niet ongewoon om het synoniem tweefactor-authenticatie te gebruiken.

Wat verstaat men onder factoren?

Onderstaande eenvoudige richtlijnen kunnen hierbij meer duidelijkheid brengen.

Een factor is een van onderstaande:

Iets wat je kent, een wachtwoord of pincode
Iets wat je hebt, bijvoorbeeld een pinpas of smartcard
Iets wat je bent, verwijzend naar biometrische gegevens, zoals je vingerafdruk

Single factor authenticatie

In zijn meest eenvoudige vorm gebruiken we éénfactor-authenticatie vrijwel elke dag onder vorm van een toegangsbadge tot onze gebouwen, maar ook onder een veiliger vorm: onze toegang tot het werkstation door gebruik te maken van een gebruikersID met bijhorend wachtwoord.

Éénfactor-authenticatie verwijst naar de unieke wijze op basis van waarop de identiteit gevalideerd kan worden:

Voor de validatie tot toegang voor een gebouw zal het toegangscontrole systeem de toegang enkel valideren op iets dat in het bezit is van de gebruiker
Bij de toegang tot het werkstation door middel van een gebruiker ID en paswoord zal de controle enkel gevalideerd worden op basis van iets wat de gebruiker weet

Merk op: *In bovenstaande voorbeelden is er geen enkele garantie dat de gebruiker effectief ook de identiteit is, waaraan de toegang werd toegekend. Dit onderstreept het belang voor de organisatie dat gebruikers op de hoogte worden gebracht, hoe deze authenticatiemiddelen correct worden gebruikt.*

Eén-factor authenticatie en de paswoord problematiek

Het probleem bij het gebruik van enkelvoudige factoren, is dat deze niet altijd voldoende garantie biedt om een identiteit te verifiëren. Als derden deze factor weten te misbruiken (het wachtwoord achterhalen of de badge ontvreemden), dan kan deze zich als de persoon, gekoppeld aan het authenticatiemiddel (account) voordoen en zich onrechtmatig toegang verlenen.

Bij de factorauthenticatie op basis van wat je bent (biometrische authenticatie) is misbruik minder evident, maar niet ondenkbaar. Bovendien is de beschikbare technologie niet altijd in staat om de identiteit gegarandeerd vast te stellen (misleiding gezichtsherkenning d.m.v. foto).

Om een betere garantie te geven bij het afschermen van informatie is het sterk geadviseerd om minimaal bijkomende maatregelen te nemen die het risico op misbruik kan verminderen. Bij sommige informatieklassen worden deze bijkomende maatregelen onvoldoende geacht en vraagt men expliciet om een identiteit te valideren op basis bijkomende authenticatie maatregelen op basis van meerdere factoren.

Multifactor-authenticatie

Multifactor baseert zich bij de validatie van een identiteit op meerdere factoren door deze te combineren in het authenticatieproces. Het bekendste voorbeeld van het toepassen van een multifactor-authenticatie is de creditcard (iets wat je hebt) en de bijhorende pincode (iets wat je kent). Het authenticatie proces gebruikt daarbij twee factoren om de identiteit van een gebruiker vast te stellen.

Merk op: *Gebruiker ID en paswoord bevinden zich beide in dezelfde factor klasse (iets dat je weet) en worden dus niet beschouwd als multifactor.*

Tweetraps met één factor

Een belangrijk concept hierbij is dat multifactor uitgaat van twee los van elkaar bestaande factoren. Een toegangscode op bijvoorbeeld een smartphone (App en SMS) naast een reguliere wachtwoordtoegang, is volgens de definitie geen 'echte' multifactor-authenticatie, omdat er gebruik wordt gemaakt van één factor: iets wat je kent.

Het verschil zit hem in de details wanneer men spreekt over tweefactor-authenticatie of tweetraps-authenticatie.

Tweefactor-authenticatie gaat uit van meerdere factoren.
Tweetraps-authenticatie baseert zich op twee uit te voeren stappen met een gelijkwaardige factor (bvb 2x iets wat je kent).

Tweefactor-authenticatie is dus altijd tweetraps-authenticatie (want gaat over twee stappen), maar andersom is tweetraps-authenticatie niet altijd tweefactor-authenticatie (want er kan ook één factor worden gebruikt)

Basisprincipe: Bij multifactor gaat men uit van meerdere authenticatiemiddelen.

2.2.5. Integriteit van de gegevens betrokken in het authenticatieproces

Status van het account

De beheerder beheert de status van de bestaande gebruikers en maakt hiervoor gebruik van de hierboven beschreven categorieën. Dit belet niet enkel onrechtmatige toegang tot data (kwaliteitskenmerk vertrouwelijkheid), het verhindert ook onrechtmatige aanpassingen aan data (kwaliteitskenmerk integriteit).

Hiervoor richt je een proces met de nodige verificatiestappen in om ervoor te zorgen dat de status van de gebruiker te allen tijde correct is. Dit is de enige manier om de Vertrouwelijkheid en Integriteit van de data te borgen.

Meer details over hoe je dit kunt doen, lichten we toe in de beschrijving van de Soll/Ist-methodiek, waarbij de concepten Identiteit, Authenticatie en Autorisatie samenkomen.

Wijzigingen in de status van een gebruiker gebeuren enkel in functie van de SOll/Ist. Het proces van het wijzigen van een toegangsrecht, moet je beschrijven en moet auditeerbaar zijn. Dit doe je door middel van logging van aanvragen en de verwerking ervan.

Tegelijkertijd is het nuttig om dit proces (automatisch) te linken aan het provisioning proces, om er zeker van te zijn dat de status van een account altijd de juiste is.

Beveiliging van het paswoord

Er zijn heel wat controles die je kunt toepassen op paswoorden. Hier focussen we op het uitwisselen van credentials[5] bij het aanmelden, en de veilige opslag van de gebruikersnaam en het paswoord door de toepassing of het systeem.

Bij het verzenden van *credentials* tijdens het aanmelden stuur je enkel de *hash* van het wachtwoord Bij het opslaan van het paswoord, is het belangrijk om ervoor te zorgen dat de toegang ertoe strikt afgezonderd is tot beheerders en dat zij enkel toegang krijgen tot gehashte wachtwoorden. *Salting* is een extra techniek die je toepast om nooit het reële paswoord kenbaar te maken.

> Een alternatief hiervoor is werken met federatie, waarbij je de identificatie en authenticatie aan een derde partij toevertrouwt. Dit wil vooral zeggen dat je de data die hiermee gepaard gaat niet zelf beheert. Als je dit doet, moet je er wel zeker van zijn dat die derde partij alle noodzakelijke controles in plaats heeft gezet om de data te beschermen. Dit dek je idealiter ook contractueel af.

Voorbeelden *Bekende voorbeelden van deze techniek is om aan te melden met een account van een social media platform, bijvoorbeeld Facebook.*

Dit zijn slechts enkele voorbeelden van maatregelen die je kunt nemen om paswoorden te beveiligen. Je mag er uiteraard andere en meer nemen. Doe dit in overleg met de verantwoordelijke over Informatieveiligheid binnen je entiteit.

2.2.6. Beschikbaarheid van de gegevens betrokken in het authenticatieproces

Status van account moet beschikbaar zijn

Hier is de link met de informatieklasse van de toepassing of het proces evenzeer belangrijk. De authenticatie moet kunnen gebeuren terwijl de toepassing functioneel is. Welke controles hiervoor kunnen gelden, staat beschreven in het Beleidsdocument Toegangsbeheer.

Als je gebruik maakt van een authenticatieproces onafhankelijk van je eigen toepassing, moet dat uiteraard ook aan deze voorwaarden voldoen.

Logbestanden bijhouden

De logbestanden voor de gebeurde authenticaties moet beschikbaar zijn in lijn met de termijnen van het bijhouden van de operationele logs van de toepassing. De geldende legale termijn moet je hierbij ook respecteren. Deze zijn uiteraard sterk afhankelijk van de operationele context. De langste termijn is bepalend.

2.3. Autorisatie als maatregel

Toestemming tot gebruik van een dienst of applicatie door een bevoegd persoon noemt men **autorisatie.** Men maakt onderscheid tussen twee specifieke aspecten:

Toegangsbeheer (Het proces) als organisatorische maatregel.
Toegangscontrole (De techniek) als technische maatregel.

2.3.1. Toegangsbeheer als maatregel

Toegangsbeheer is een organisatorische maatregel die steunt op een toegangsbeleid. Dit proces legt uit, hoe en onder welke omstandigheden een individu toegang krijgt tot de organisatiemiddelen.

Om dit te realiseren zijn er in de eerste plaats af te dwingen maatregelen nodig. Deze maatregelen zijn gekend als toegangsbeleidslijnen (*access policies*) en omschrijven onder welke omstandigheden een toegang gevalideerd kan worden op basis van de classificatie van de informatie waarop de validatie van toepassing is.

Daarnaast, maakt men op basis van de behoeften gespecifieerd in deze toegangsbeleidslijnen (*access policies*) een set van (workflow) processen die de organisatie gebruikt om het toegangsbeheer operationeel uit te baten. Deze workflow processen kunnen worden geautomatiseerd (Voorbeeld: Vo webIDM)

Volgende elementen zijn noodzakelijk in het toegangsbeheer vanaf informatieklasse 2 voor Vertrouwelijkheid en Integriteit of afhankelijk van de klassen van de verwerkte informatie binnen de doeltoepassing of dienst.

Opmerking: Toegangsbeheer voor beheersactiviteiten, verschillend van reguliere toegangen voor eindgebruikers worden apart behandeld in het Privileged access management of PAM proces. Deze omvatten de beheerstoegangen tot achterliggende infrastructuur, platform of softwarecomponenten

Attributen van het toegangsbeheer

Volgende attributen zijn aanwezig in het toegangsbeheer om een auditeerbaar proces te garanderen:

Beschikbare informatie bij de verwerking van een toegang

Basis attributen van het verzoek tot toegang (Datum, tijd, aanvrager, volgnummer, …)
Onderwerp, als referentie naar het individu die de toegang wenst te gebruiken.
Motivatie van het verzoek
Bevestiging van motivatie
Basis attributen van de validatie van de toegang (Datum, tijd, …)
Identiteit van de persoon die de goedkeuring(en) geeft.
(Optioneel: bijkomende opmerkingen)
Vervaldag van het toegangsrecht, afhankelijk van de klasse van de verwerkte informatie binnen de dienst of toepassing
Periodiek herhaalde (her)validatie van een recht, afhankelijk van de klasse van de verwerkte informatie binnen de dienst of toepassing

Opmerking(en):

*Motivatie op basis van organisatie lidmaatschap is beperkt tot informatie **[klasse 2]**. Deze motivatie bevat geen expliciete individuele bevestiging van de functionele behoefte door een toegangsbeheerder of hiërarchisch verantwoordelijke van het onderwerp. De toegang is bij deze voorgaand geautoriseerd door de toepassingsverantwoordelijke en gedelegeerd aan het toegangsbeheerproces.*

Vanaf informatieklasse 3 voor Vertrouwelijkheid of Integriteit is er behoefte aan motivatie op basis van de functionele relatie tussen het onderwerp en toegang tot de verwerkte informatie.

Actoren(rollen) bij de verwerking van een toegang

Onderwerp: Identiteit van het individu die toegang tot de verwerking wenst te gebruiken.

Validator: Identiteit van een individu die de voorwaarden tot de gevraagde toegang bevestigen (valideren) tijdens het verwerkingsproces

De verwerking van autorisaties voor zichzelf is hierbij uitgesloten

De autorisatie voor actoren die deze rol opnemen is opgenomen in het toegangsbeheersysteem en gevalideerd door de organisatie

Hiërarchisch leidinggevende

Functioneel leidinggevende

Functioneel verantwoordelijke

Toepassingsbeheerder

Security Officer

Toegangsbeheerder: Identiteit van het individu die de toegangsverzoeken operationeel verwerkt

Elke erkende gebruiker van het toegangsbeheer proces

Self-service baseert zich steeds op een sterke authenticatie

Identiteit van een individu die het toegangsbeheerproces voor anderen administratief verwerken.

De verwerking van toegangen voor zichzelf is hierbij uitgesloten

De autorisatie voor actoren die deze rol opnemen is opgenomen in het toegangsbeheersysteem en gevalideerd door de organisatie.

Auditor: Identiteit van een individu die controle uitvoert op alle aspecten van het verwerkingsproces.

Alle verwerkingsinformatie van het toegangsbeheer (Audit trails) zijn beschikbaar en zijn enkel in te kijken door het individu

De autorisatie voor actoren die deze rol opnemen is opgenomen in het toegangsbeheersysteem en gevalideerd door de organisatie.

2.3.2. Toegangscontrole als maatregel

Toegangscontrole is een set van technische maatregelen die steunen op de technische specificaties van de toegepaste technologie.

Bij het aanmelden aan een toepassing of dienst zal de identiteit (authenticatie) gevalideerd worden, waarbij de technische afhandeling van het validatieverzoek afhankelijk is van de gebruikte technologie. (Zie eID.AS)

Afhankelijk van de gebruikte methode zal datzelfde authenticatieplatform bepalen welke autorisaties er aan het betrokken individu (op basis van zijn account of gekoppeld recht) worden toegekend.

Voorbeeld: Microsoft geïntegreerde authenticatie valideert niet enkel het aangeboden account, maar ook de toegangen. Het authenticatie ticket bevat ook het lidmaatschap van alle

groepen (Dit is geldig voor zowel lokale groepen op een Windows host als Active Directory groepen

Andere authenticatieplatformen handelen enkel de authenticatie van het account af. De autorisatie gebeurt dan binnen de toepassing of op (sub) systeemniveau.

Voorbeeld(en):

LDAP-authenticatie valideert enkel het account. Een toepassing zal, via code, steeds een bijkomende validatie af handelen om groep lidmaatschap te valideren.
Een ACL (Access Control List) op een bestand, folder of disk zal gevalideerd worden door het disk subsysteem op basis van de ACE (Access Control Entry) op het betrokken object.

Beide benaderingen hebben behoefte aan een aangepast controlemechanisme om aan de vereiste technische maatregelen te voldoen.

Voor de toegangen die toegestaan worden op basis van een centrale referentietabel (ook directory genoemd) gebruiken we het toegangsbeheer en zijn onderliggende processen en controles.
Voor toepassingen die deze referentietabel gebruiken om autorisaties te valideren gebruiken een combinatie van volgende processen:
Configuratie beheer garandeert een beveiligde systeem context voor de toepassing.
Secure coding en safe source (**software assurance**) leveren een correcte basis voor een veilige ontsluiting en implementatie van de toepassing.
Voor de toegangen die toegestaan worden op basis van een referentietabel die rechtstreeks gelinkt is aan het middel (ACL op de resource of asset) gebruiken we het proces configuratie beheer (niet in scope van dit document)

Het is belangrijk te noteren dat toegangscontrolemaatregel in lijn moeten zijn met de toegangsbehoefte van de rol tot de verwerkte informatie. Hierbij houden we vast aan het *least access privilege* principe en scheiden we eindgebruikerstoegangen strikt van de beheerstoegangen.

2.3.3. Integriteit van het authenticatieproces

Soll/Ist [6]

Met Soll/Ist bedoelen we twee processen:

- Soll is de documentatie van de gewenste staat van gebruikers. Het biedt een overzicht van welke rollen toegang zouden moeten hebben tot welke functionaliteiten of welke stappen in een deelproces in de toepassing, of het systeem. De Soll is de beschrijving van de ideale situatie en kan vrij gedetailleerd zijn, afhankelijk ook van de complexiteit van de toepassing of het systeem.
- Ist is de beschrijving van de reële toegangen binnen een toepassing of een systeem, los van wat de ideale situatie is. Deze oefening legt meestal inconsistenties bloot en leidt tot acties om toegangen op te ruimen en te aligneren met de Soll.

De Soll-oefening doe je in principe een eerste keer grondig, waardoor je daarna enkel minimale updates moet doen. Een keer je hem gedaan hebt, is een jaarlijkse review voldoende.
De Ist-oefening herhaal je best regelmatig om eventuele tekortkomingen in je user life cycle of provisioning-proces op te sporen en recht te trekken.
Hoe hoger de informatieklasse van je toepassing, hoe vaker je deze oefening best doet. Dit kan gelden voor Vertrouwelijkheid, Integriteit en Beschikbaarheid – de strengste wint.

Informatieklasse	Frequentie review Soll	Frequentie review Ist
	Jaarlijks	Minstens 1 keer per jaar
	Jaarlijks	Minstens 1 keer per jaar
	Jaarlijks	Minstens 2 keer per jaar
	Jaarlijks	Minstens 2 keer per jaar
	Jaarlijks	Minstens 4 keer per jaar

Beide oefeningen laat je valideren door de toepassingseigenaar.

Voorbeeld:

Eén manier om dit in te richten is met de Identiteitsbeheer-bouwsteen (IDM). Dat proces verloopt voorlopig deels automatisch. IDM legt je als tool geen frequentie op, die heb je dus wel zelf onder controle.

Ist-proces vs. De-provisioning

Het Ist-proces is een recurrent proces: je voert het op gestelde momenten uit om te controleren dat de reële situatie beantwoordt aan de ideale. Het is het moment om bepaalde fouten recht te zetten.
Het de-provisioning-proces is een ad hoc proces dat je uitvoert telkens een medewerker van functie verandert, of de organisatie verlaat. Het Ist-proces stelt, als alles goed is, vast dat het de-provisioning-proces goed verlopen is.

Een rol toekennen

Je gebruikt de Soll-matrix als leidraad en kent enkel een rol toe aan een geïdentificeerd persoon.

Als blijkt dat een aanvraag tot toegang niet strookt met de bestaande Soll en de aanvraag gerechtvaardigd is, pas je de Soll aan en laat je hem opnieuw valideren door de toepassingseigenaar.

Afhankelijk van de informatieklasse van de data, zowel qua Vertrouwelijkheid als qua Integriteit, moet de identificatie van de persoon strenger zijn. Dit staat beschreven in het hoofdstuk Identificatie als maatregel.

2.3.4. Integriteit van de gegevens betrokken in het authenticatieproces

Validatie

Het is belangrijk om in de hierboven beschreven processen voldoende controles te voorzien om de integriteit van de gebruikte gegevens te borgen. Dat gaat dan om:

- De controle van de identiteit van de persoon
- De mate waarin die gerechtigd is om een aanvraag in te dienen
- De inhoud van de aanvraag zelf

Voor dat laatste kun je uiteraard teruggrijpen naar de Soll om te verifiëren of de gebruiker recht heeft op een bepaalde rol, en indien ja, dewelke.

Afhankelijk van de informatieklasse, ga je ook strenger moeten zijn. De details over welke controles wanneer nodig zijn staan beschreven in het Overzicht en integratie van de maatregelen. Belangrijk is daarbij te beseffen dat de strengste maatregel de bepalende is. Is je informatie Klasse 2 voor Vertrouwelijkheid en Klasse 4 voor Integriteit, dan moet je de controle implementeren voor Klasse 4.

2.3.5. Beschikbaarheid van het autorisatieproces

Link met de informatieklasse

Het autorisatieproces om een gebruiker te autoriseren moet even beschikbaar zijn als de toepassing waartoe deze gebruiker zich wil laten autoriseren.

Als je gebruik maakt van een autorisatiesysteem onafhankelijk van je eigen toepassing, moet dat uiteraard ook aan deze voorwaarden voldoen.