

EA2023047 Identity & Access Management: Bijlage F - Programma van Eisen (functionals)

Nummer	Categorie	Omschrijving
EF-01	Attestatie	De Oplossing is in staat om identiteitskenmerken zoals HR-gegevens en risicoprofielen (zoals opgebouwd in de IAM-applicatie) te gebruiken om automatisch gebruikerspopulaties te definiëren voor de Attestatie.
EF-02	Attestatie	Tijdens het Attestatie-proces kan de Oplossing gebruikersaccounts met hogere rechten en andere risicovolle accounts (bijv. serviceaccounts, bots) signaleren of kenmerken.
EF-03	Attestatie	De Oplossing beschikt over een signaleringsfunctie van tegenstrijdige rollen/rechten (segregation of duties).
EF-04	Attestatie	De Oplossing biedt zicht op High Privileged Accounts in de aangesloten Doelsystemen (bijv. hoog mandaat, hoge gebruikersrechten, etc.) tijdens de Attestatie.
EF-05	Attestatie	Tijdens de Attestatie moet de Oplossing inzicht bieden via welke rol de Medewerkers toegang hebben tot welke systemen en met welke rechten.
EF-06	Attestatie	De Oplossing maakt het mogelijk om een totale attestatie of de Attestatie van een of meerdere Medewerkers te delegeren naar een andere attesteerder.
EF-07	Attestatie	De Oplossing maakt het mogelijk om specifieke regels of items in een Attestatie te selecteren om te worden gedelegeerd naar een andere Attesteerder voor beoordeling. Bijvoorbeeld autorisaties als gevolg van deelname in een project die door iemand anders geattesteerd wil laten worden.
EF-08	Attestatie	De Oplossing kan beleidsschendingen beoordelen tijdens de Attestatie.
EF-09	Attestatie	De Oplossing kan een attestatie starten en deze eerst in een "test-modus" activeren (in de productie-omgeving) voordat de attestatie live gezet wordt om te verifiëren of de attestatie correct geconfigureerd is, alvorens te activeren voor Eindgebruikers.
EF-10	Attestatie	De Oplossing kan out-of-the-box (standaard aanwezig) verschillende type Attestatie use cases ondersteunen voor verschillende Eindgebruikers. Bijvoorbeeld Beheerders Attestatie, applicatie-eigenaar Attestatie, gegevens eigenaren, selectie van Leidinggevende/eigenaren.
EF-11	Attestatie	De Oplossing maakt het mogelijk om Attestaties voor gebruikerstoegang, inclusief de criteria tot het samenstellen van de populatie van de Attestatie-deelnemers, automatisch in te stellen om op een periodieke cyclus te starten. Minimaal maandelijks/kwartaal/tertaal/jaarlijks.
EF-12	Attestatie	De Oplossing kan automatisch een Attestatie genereren op basis van gedetecteerde wijzigingen in de toegang van een Identiteit (bijv. verandering van afdelingen, functies, leidinggevende, etc).
EF-13	Attestatie	De Oplossing kan Attestatie-kenmerken definiëren en beheren via de Gebruikersinterface, zoals duur, einddatum, reminder, escalatie, etc.
EF-14	Attestatie	Tijdens de beoordeling van de toegangsrechten van een Medewerker kunnen Attesteerders goedkeuring geven of intrekken of excepties (met toelichting en met of zonder einddatum) toestaan.

Nummer	Categorie	Omschrijving
EF-15	Attestatie	De Oplossing is biedt Attesteerders de mogelijkheid om toegangsrechten van een Medewerker te beoordelen en te kunnen goedkeuren, intrekken of excepties (met toelichting en met of zonder einddatum) toestaan.
EF-16	Attestatie	De Oplossing biedt een administratief Dashboard en een out-of-the-box (standaard aanwezig)rapportagetool om geaggregeerde attestatiestatistieken bij te houden van Attestatie-campagnes.
EF-17	Attestatie	De Oplossing is in staat om zicht te bieden op Attestatie-activiteiten (bijv. voltooiingsstatus) op het Dashboard van een Eindgebruiker.
EF-18	Attestatie	De Oplossing is in staat zijn om de actuele stand van Accounts en Autorisaties uit te lezen uit gekoppelde Doelsystemen en om aan te bieden in de Attestatie.
EF-19	Attestatie	De Oplossing is in staat om de CMDB uit te lezen zodat alle Doelsysteem en Doelsysteem-eigenaren actueel blijven ten behoeve van de Attestatie, zodat ook wijzigingen (van Doelsysteem en eigenaren) in de CMDB altijd up-to date zijn in de Oplossing.
EF-20	Compliance	De Oplossing stelt de SVB in staat om voortdurend te voldoen aan regelgeving van BIO en AVG.
EF-21	Configuratie & beheer	De Oplossing biedt een separate test-en acceptatie omgeving, met geanonimiseerd data waarin rapportages of functionele aanpassingen en nieuw Koppelingen getest kunnen worden voordat deze in productie worden genomen.
EF-22	Configuratie & beheer	De test-en-acceptatie omgeving is een kopie van de productie-omgeving, met dezelfde functionaliteiten en Koppelingen. Minimaal is naast de productie-omgeving een test of acceptatie omgeving aanwezig (minimaal 2 omgevingen).
EF-23	Configuratie & beheer	De Oplossing is zo geconfigureerd dat het de autoratieve bron wordt voor alle Identiteiten en toegang door - per Identiteit - de gewenste (goedgekeurde) status af te dwingen (dus IAM is leidend voor alle Doelsystemen).
EF-24	Configuratie & beheer	De Oplossing ondersteunt minimaal de volgende standaarden rond de interoperabiliteit van identiteitsbeheer: SPML, SCIM(v2), OpenID, CSV-based.
EF-25	Configuratie & beheer	De Oplossing ondersteunt de definitie van gebruikersrollen en toewijzing van toegangsrechten op basis van rollen, en dat het interne Autorisatie-model kan worden aangepast om deze te kunnen inzetten bij het verlenen van toegangsrechten voor Medewerkers.
EF-26	Configuratie & beheer	De Oplossing logt en toont alle acties die zijn uitgevoerd, door de Oplossing ongeacht of deze succesvol zijn geweest of niet (failures). Minimaal, en niet gelimiteerd tot alle activiteiten, met betrekking tot provisioning, identiteitenwijzigingen, account/autorisatie wijzigingen, autorisatie/account aanvragen, voor controle(audit)doeleinden.
EF-27	Configuratie & beheer	De Oplossing neemt eventuele geïmplementeerde aanpassingen en configuraties automatisch en probleemloos meenemen bij een upgrade van de Oplossing.
EF-28	Configuratie & beheer	De Oplossing kan alle acties/taken die worden uitgevoerd door beheerders en eindgebruikers loggen en tonen en controleren om de onweerlegbaarheid van de acties aan te tonen. De granulariteit van de auditcapaciteit moet worden ondersteund met een voorbeeld (tijdens verificatie/PoC).

Nummer	Categorie	Omschrijving
EF-29	Configuratie & beheer	De Oplossing geeft alle acties, zowel van het systeem als van gebruikers, een tijdstempel voor logging en auditing doeleinden.
EF-30	Configuratie & beheer	De Oplossing maakt onderscheid in verschillende Identiteits-typen, zoals Medewerker-intern, Medewerker-extern, functioneel, test, systeem, leveranciers, partners, contractanten, bots, enzovoort. Identiteiten kunnen zowel handmatig en automatisch worden gelabeld.
EF-31	Configuratie & beheer	De Oplossing maakt onderscheid in verschillende Account-typen, zoals Medewerkersaccount, functioneel account, testaccount, serviceaccount, Beheerdersaccount, enzovoort. Accounts kunnen zowel handmatig en automatisch worden gelabeld.
EF-32	Configuratie & Beheer	De Oplossing kan (tijdelijk) extra organisatie-eenheden toekennen aan Medewerkers. Hierbij dient een tweede Active Directory account met bijbehorende tweede mailbox en tweede mailadres (handmatig) aangemaakt te kunnen worden. Rollen kunnen onafhankelijk aan beide Accounts toegekend of ingetrokken worden.
EF-33	Configuratie & Beheer	De Oplossing voorkomt dat unieke eenmaal uitgegeven Identiteits- en Accountgegevens herbruikt kunnen worden door andere Identiteiten nadat de oorspronkelijke Identiteit uit dienst is gegaan (of is verwijderd). Dit geldt voor tenminste het emailadres en samaccountname. In het geval van een herintreder moet dit overruled kunnen worden. Toelichting: Unieke, eenmaal uitgegeven Identiteit- en Account gegevens mogen niet herbruikt worden. De SVB heeft een uniek waarden register voor deze Attributen.
EF-34	Configuratie & Beheer	Het bewaarbeleid van Identiteit-gegevens en bijbehorende gegevens zijn configureerbaar.
EF-35	Configuratie & Beheer	De Oplossing kan niet-gebruikte (slapende) Accounts na een instelbare periode blokkeren.
EF-36	Configuratie & Beheer	De Oplossing kan een kommagescheiden CSV bestand (of ander marktconform importformat) inlezen m.b.t. (onder andere) het doorvoeren van mutaties identiteiten uit het Bronsysteem (nieuw, wijziging en verwijderen) en het inlezen van uitgegeven autorisaties (IST) uit Doelsystemen. Minimaal, maar niet gelimiteerd tot; CSV, XML, platte bestanden (ongestructureerd).
EF-37	Data Aggregatie & Correlatie	De Oplossing ondersteunt fijnmazige modellering van machtigingen/rechten, zoals specifieke rechten op databasetabellen, bestandshares, Teams-kanalen, enzovoort.
EF-38	Data Aggregatie & Correlatie	De Oplossing ondersteunt het verzamelen en beheren van Identiteits- en Autorisatie-gegevens uit SaaS-applicaties en/of IAAS platformen(minimaal het, maar niet gelimiteerd tot, Bronsysteem, Office365, Google applicaties/Cloud, AWS) via een standaard Koppeling.
EF-39	Data Aggregatie & Correlatie	De Oplossing ondersteunt meerdere autoratieve bronnen voor Identiteits-gegevens (kenmerken), bijvoorbeeld persoonlijke gegevens (naam, begin/einddata, enz.) uit het Bronsysteem, e-mailadres uit Exchange, sam accountname uit AD, enzovoort.
EF-40	Data Aggregatie & Correlatie	De Oplossing bevat een gecentraliseerde catalogus van alle rechten van gekoppelde Doelsystemen.

Nummer	Categorie	Omschrijving
EF-41	Data Aggregatie & Correlatie	De Oplossing ondersteunt het importeren en koppelen van betekenisvolle beschrijvingen en andere metadata aan IT-rechten uit de gekoppelde Doelsysteem.
EF-42	Data Aggregatie & Correlatie	De Oplossing ondersteunt de mogelijkheid om de Medewerker-Leidinggevende relatie te abstraheren van het aangesloten Bronsysteem: op basis van informatie uit het Bronsysteem via een koppeling op basis van een API of bestand(extract) is duidelijk wie de Leidinggevende(n) is/zijn van een Medewerker.
EF-43	Data Aggregatie & Correlatie	De Oplossing creëert een enkele weergave van elke Eindgebruiker binnen de SVB en de bijbehorende Account- en toegangsrechten.
EF-44	Data Aggregatie & Correlatie	De Oplossing toont alle gebruikersrechten, rollen, beleidsinformatie en activiteitsgegevens binnen de context van een Identiteit: alle gebruikersrechten, beleidsinformatie en activiteitsgegevens.
EF-45	Extra functionaliteit	De Oplossing heeft functionaliteit om een functioneel account aan te kunnen maken waar automatisch een fictief personeelsnummer aan wordt toegekend.
EF-46	Extra functionaliteit	De Oplossing heeft functionaliteit om een functioneel mailbox aan te kunnen maken waar automatisch een fictief personeelsnummer aan wordt toegekend.
EF-47	Extra functionaliteit	De Oplossing heeft functionaliteit om een leveranciersaccount aan te kunnen maken waar automatisch een fictief personeelsnummer aan wordt toegekend.
EF-48	Extra functionaliteit	De Oplossing kan een overzicht tonen met locaties en afdelingen, met daaraan gekoppeld de volgende attributen; code locatie, code afdeling, manager afdeling, accountcontainer.
EF-49	Extra functionaliteit	De Oplossing heeft functionaliteit om afdelingen waar geen medewerkers aan gekoppeld zijn weg te filteren.
EF-50	Extra functionaliteit	De Oplossing toont in het overzicht met locaties en afdelingen welke nieuw zijn toegevoegd zodat IAM-coördinatoren weten dat er rollen aan gehangen moeten worden. Dit houdt niet in dat er een 1-op-1 koppeling is tussen locaties/afdelingen en rollen. Mogelijk kunnen er meer HR groeperingen zijn (bijv. functies).
EF-51	Extra functionaliteit	De Oplossing toont in het overzicht van autorisaties bij een identiteit welke automatisch (o.b.v. RBAC/ABAC) of handmatig (door wie en wanneer) zijn toegekend.
EF-52	Extra functionaliteit	De Oplossing moet in het overzicht van accounts kunnen tonen dat een medewerker niet meer in het HR-systeem bestaat en daarmee het account beëindigd zou moeten worden. De beheerder kan vervolgens zelf bepalen of dat daadwerkelijk moet gebeuren of niet, al dan niet na een zelf ingestelde periode.
EF-53	Extra functionaliteit	De Oplossing toont een overzicht met alle accounts waarvan de medewerker uitdienst is maar nog actief is in overeenstemming met de norm (nu 30 dagen) en de mogelijkheid geeft aan de beheerder om deze eerder te beëindigen of te verlengen.
EF-54	Extra functionaliteit	De Oplossing toont een overzicht met alle functionele mailboxen en de verantwoordelijke hiervoor en markeert deze (bijvoorbeeld met een kleur) als er geen verantwoordelijke aan toegekend is (t.b.v. controle of functionele mailbox nog nodig is).

Nummer	Categorie	Omschrijving
EF-55	Extra functionaliteit	De Oplossing toont welke foutmelding is opgetreden als identiteiten hun wachtwoord wijzigen maar dit niet succesvol plaatsvindt (t.b.v. troubleshooting).
EF-56	Extra functionaliteit	De Oplossing toont in het autorisatiemodel welke rollen uitdeelbaar zijn en door wie en kan hier een rapportage van uitdraaien.
EF-57	Extra functionaliteit	De Oplossing heeft functionaliteit om uitgevoerde acties ook ongedaan te kunnen maken.
EF-58	Extra functionaliteit	De Oplossing heeft een overzicht van autorisaties die handmatig zijn toegevoegd in systemen maar geen koppeling hebben met de Oplossing. Toelichting: Het kan voorkomen dat binnen de Oplossing de gewenste account/rechten situatie is vastgelegd voor een Doelsysteem, maar dat er geen Koppeling is naar het Doelsysteem (of dat er zelfs geen gewenste situatie is vastgelegd). Door (periodiek) de werkelijke accounts/rechten vanuit een Doelsysteem in te lezen kan de Oplossing het genoemde overzicht bieden.
EF-59	IT & Security Intergrations	De Oplossing ondersteunt integraties met Doelsystemen en/of resources met ongestructureerde gegevens, zoals netwerkschijven, SharePoint, Teams, om zichtbaar te maken wie wat kan op welk moment met deze resources en deze zichtbaar te maken in een Attestatie.
EF-60	IT & Security Intergrations	De Oplossing is geïntegreerd met de PAM Applicatie CyberArk via een standaard Koppeling. De SVB verwacht dat de Oplossing een out-of-the-box connector ofwel een standaard aanwezige Koppeling biedt, waarmee de interface tussen Oplossing en Cyberark functioneert, zodat dat de SVB altijd in control is op de juistheid en rechtmatigheid van via de Oplossing uitgegeven Accounts, Autorisaties en rechten in Cyberark.
EF-61	IT & Security Intergrations	De Oplossing kan out-of-the-box (standaard aanwezig) integreren met SIEM Applicatie (Splunk) via een standaard Koppeling. En informatie uitwisselen die onderdeel is van een melding in SIEM.
EF-62	IT & Security Intergrations	De oplossing kan out-of-the box koppelen of heeft standaard de mogelijkheid om Privileged Identity Management (PIM) te kunnen doen. Waarbij Just-in-time toegang mogelijk moet zijn.
EF-63	LifeCycle Management	De Oplossing bepaalt automatisch of het nodig is om nieuwe Accounts te maken die zijn gekoppeld aan het toevoegen van rechten en rollen. Met andere woorden, een Autorisatie-verzoek kan leiden tot het maken van een Account als de Eindgebruiker het Account nog niet heeft.
EF-64	LifeCycle Management	De Oplossing kan levenscyclusgebeurtenissen (instroom, doorstroom en uitstroom) per Identiteits-type (Medewerker/Leverancier) configureren vanuit de Gebruikersinterface.
EF-65	Password Management	De Oplossing ondersteunt het resetten van wachtwoorden door de Servicedesk rechtstreeks vanuit een Gebruikersinterface van de Oplossing.
EF-66	Password Management	De Oplossing kan wachtwoordwijzigingen over meerdere Doelsystemen, minimaal maar niet gelimiteerd tot Active directory en RACF, direct synchroniseren.
EF-67	Password Management	De Oplossing ondersteunt het opslaan van een wachtwoord in "one way hash".

Nummer	Categorie	Omschrijving
EF-68	Password Management	De Oplossing kan de Eindgebruiker tijdig op de hoogte stellen, middels meldingen via e-mail aan de Eindgebruiker, wanneer zijn/haar wachtwoord verloopt. Deze meldingen moeten inhoudelijk aanpasbaar zijn.
EF-69	Platform & Architecture	De Oplossing heeft een API die kan worden gebruikt om een Koppeling met Bron- en Doelsystemen te maken. En deze moet beschreven worden via Open API Specificatie (OAS). OAS is op dit moment een door Forum Standaardisatie verplichte standaard binnen de overheid. Eventueel mag specificatie in Postman Collections en API Blueprint ook.
EF-70	Platform & Architecture	De Oplossing kan Oauth 2.0 informatie uit te wisselen doormiddel van JWT. Het gaat hier specifiek om REST API's
EF-71	Platform & Architecture	De Oplossing ondersteunt het NTLM protocol voor legacy applicaties (NTLMv2).
EF-72	Platform & Architecture	De Oplossing is zowel via IPv4 als IPv6 te benaderen en ondersteunt beide protocollen.
EF-73	Platform & Architecture	De Oplossing kan koppelen met RADIUS. Radius wordt gebruikt in de Clearpass (netwerktogang) omgeving van de SVB.
EF-74	Provisioning & Connectivity	De Oplossing ondersteunt het opnieuw proberen van een transactie als deze mislukt.
EF-75	Provisioning & Connectivity	De Oplossing biedt functionaliteit voor het maken van configureerbare Koppelingen. Toelichting: De SVB bedoelt hiermee dat connectoren (standaard - out of the box koppelingen) om nieuwe applicaties (Doelsystemen) te integreren configureerbaar zijn, dus parameter gedreven in plaats van maatwerk.
EF-76	Provisioning & Connectivity	De Oplossing kan tijdens het laden van data, de validatie en transformatie van gegevens toepassen.
EF-77	Provisioning & Connectivity	De Oplossing biedt kant-en-klare Koppelingen of integratiemodules voor de volgende categorieën van systemen: Enterprise-systemen, Database, Directory's, Enterprise/Verticale toepassingen, Communicatie-, samenwerkings- en productiviteitstools, Platforms, andere systemen.
EF-78	Provisioning & Connectivity	De Oplossing kan Account- en toegangswijzigingsverzoeken Provisionen naar Doelsystemen.
EF-79	Provisioning & Connectivity	De Oplossing kan Account- en toegangswijzigingsverzoeken real-time Provisionen ('just-in-time provisioning') naar Doelsystemen op basis van Autorisatie-profielen én verschillende Identiteit- en sessiekenmerken.
EF-80	Provisioning & Connectivity	De Oplossing biedt integratie met een Provisioning Doelsysteem, minimaal, maar niet gelimiteerd tot Azure, AWS, RACF van derden voor bulk-re-Provisioning van gebruikers op basis van rolmodelveranderingen.
EF-81	Provisioning & Connectivity	De Oplossing ondersteunt 'closed-loop' validatie van wijzigingsverzoeken (met terugkoppeling dat het verwerkt is) door integratie met een Provisioning-systeem (bijv. Azure) van een derde partij. Toelichting: Er zijn situaties denkbaar waar de Oplossing een andere provisioning engine (zoals Azure, AWS, RACF) moet gebruiken. De Oplossing is hierin leidend. Bijvoorbeeld: via de Oplossing krijgt een Identiteit een (AD) groepslidmaatschap. Via dit lidmaatschap krijgt iemand vervolgens toegang tot 1 of meerdere Doelsystemen.

Nummer	Categorie	Omschrijving
EF-82	Provisioning & Connectivity	De Oplossing integreert met niet geautomatiseerde Provisioning Doelsystemen (Applicaties die niet direct gekoppeld zijn en waarmee geen geautomatiseerde uitwisseling mogelijk is). Bijvoorbeeld het IRN netwerk, InternetResearchNetwork (anoniem internetten). (zie toelichting EF-81)
EF-83	Provisioning & Connectivity	De Oplossing ondersteunt het automatisch genereren van 'tickets' via ITSM/ESM Doelsystemen.
EF-84	Provisioning & Connectivity	De Oplossing kan updates over de ticketstatus ontvangen en deze informatie tonen aan Eindgebruikers bij het volgen van Incidenten. De oplossing kan de informatie van de ticketstatus verwerken.
EF-85	Provisioning & Connectivity	De Oplossing biedt diverse Directory-functionaliteiten, minimaal, maar niet gelimiteerd tot, onpremise Active Directory, Azure, LDAP en RACF groepsanalyse en administratie. Hierbij worden minimaal, maar niet gelimiteerd tot, geneste groepen, distributielijsten, lidmaatschappen en groepsbeheer, ondersteund en zichtbaar gemaakt in de Oplossing.
EF-86	Provisioning & Connectivity	De Oplossing kan wachtwoordwijzigingen in Doelsystemen beheren, tenminste voor Active Directory, Azure AD, LDAP en RACF.
EF-87	Provisioning & Connectivity	De Oplossing biedt een webgebaseerde Gebruikersinterface voor het beheer en de configuratie van de Koppelingen, zowel voor Koppelingen met Doelsystemen onpremise, private-cloud als public cloud (SaaS).
EF-88	Provisioning & Connectivity	De Oplossing ondersteunt het beheer van meerdere Accounts, al dan niet in hetzelfde Doelsysteem, die behoren bij één Identiteit.
EF-89	Provisioning & Connectivity	De Oplossing beschikt over een functie voor Identiteit-management, inclusief bijbehorende rechten conform het rechtenmodel, waardoor leveranciers toegang kunnen krijgen tot Doelsystemen zonder dat zij als Medewerker zijn opgenomen in het Bronssteem. Deze functie kan ook Identiteiten en rechten van partners, zoals catering, beveiliging en huurders, registreren.
EF-90	Provisioning & Connectivity	De Oplossing kan handmatig dan wel geautomatiseerd de indiensttreding van Medewerkers afhandelen. Hierbij dienen Autorisaties en Accounts aangemaakt te worden met een definieerbare periode voorafgaand aan de indiensttreding.
EF-91	Provisioning & Connectivity	De Oplossing kan handmatig dan wel geautomatiseerd de uitdiensttreding van Medewerkers afhandelen en automatisch taken uitvoeren zoals inname van bedrijfseigendommen en het versturen van meldingen naar Medewerkers en Leidinggevenden (op basis van parameters). Op de einddatum worden alle Autorisaties en Accounts ingetrokken, eventueel met een door de Leidinggevende instelbare grace periode (op basis van reden).
EF-92	Provisioning & Connectivity	De Oplossing kan handmatig dan wel geautomatiseerd de definitieve overplaatsing van Medewerkers naar andere locaties afhandelen. Hierbij worden toegangsrechten en Accounts die horen bij de oude locatie ingetrokken, eventueel met instelbare overgangsperiode, en worden rechten en Accounts van de nieuwe locatie toegekend per mutatiedatum.

Nummer	Categorie	Omschrijving
EF-93	Provisioning & Connectivity	De Oplossing kan handmatig dan wel geautomatiseerd de overplaatsing van Medewerkers naar andere functies afhandelen. Hierbij worden rechten en accounts die horen de oude functie ingetrokken, eventueel met instelbare overgangsperiode, en worden toegangsrechten en Accounts van de nieuwe functie toegekend te worden per mutatedatum.
EF-94	Provisioning & Connectivity	De Oplossing biedt een knop aan Beheerders en Leidinggevendenden, waarmee zij direct toegang van een Identiteit (en dus voor alle daaraan gekoppelde Accounts en Autorisaties) kunnen blokkeren.
EF-95	Provisioning & Connectivity	De Oplossing kan een ist-soll vergelijking uitvoeren voor ieder object, om handmatige (of anderszins) mutaties te identificeren in Doelsystemen die niet getriggerd zijn door de Oplossing, of mutaties te identificeren die nog niet zijn doorgevoerd in de Doelsysteem in geval van geen closed-loop koppeling. Dit moet het signaleren van onterecht, of nog niet (dus niet conform de inrichting binnen de applicatie) toegekende rollen, Autorisaties en Accounts omvatten.
EF-96	Provisioning & Connectivity	De Oplossing heeft rechtstreekse Koppeling met het Bronsysteem om actuele Medewerker- en organisatie gegevens te kunnen verwerken en het terugschrijven van Medewerker-gegevens naar het Bronsysteem mogelijk te maken.
EF-97	Provisioning & Connectivity	De Oplossing kan password synchronisatie per Account-type en/of Doelsysteem aan- en uitzetten. Toelichting: De 'master' is de on-premise Active Directory.
EF-98	Provisioning & Connectivity	De Oplossing kan wijzigingen in Doelsystemen en provisioning (near-)real time doorvoeren in aangesloten Doelsystemen.
EF-99	Provisioning & Connectivity	De Oplossing heeft een instelbare treshhold ter detectie op bulkwijzigingen zoals Account- verwijdering / rolaanpassingen e.d., met roll-back mogelijkheden. Beheerders moeten hierbij actie kunnen ondernemen op doorvoeren van de bulkwijziging ter voorkoming van ongewenste situaties als gevolg van een ketenwijziging (bijv. afdelingsnaamswijziging naar een afdeling die [nog] niet in het rollenmodel stond).
EF-100	Provisioning & Connectivity	De Oplossing biedt detectie (in zowel waarschuwingsscherm als rapportages) van minimaal, maar niet gelimiteerd tot, nieuwe Accounts en nieuwe groepen die zijn aangemaakt of verwijderd. Met minimaal, maar niet gelimiteerd tot, door wie(persoon), op welk tijdstip en de datum. Voorbeelden: Operationele afdelingen die zelf rechten zetten buiten het proces om en die willen we detecteren. Maar ook pentesten, of echte hacks, waarbij Accounts gemaakt worden (buiten het normale proces om).
EF-101	Provisioning & Connectivity	De Oplossing biedt detectie (in zowel waarschuwingsscherm als rapportages) van mutaties in accounts en groepen, van minimaal, maar niet gelimiteerd tot, als deze worden toegevoegd of verwijderd. Met minimaal, maar niet gelimiteerd tot, door wie(persoon), op welk tijdstip en de datum. Bijvoorbeeld wanneer (buiten het proces om) een Account in AD van Actief naar Inactief gezet wordt (of vice versa).
EF-102	Provisioning & Connectivity	De Oplossing biedt foutafhandeling voor aangeleverde (datauitwisselings)bestanden, waarbij fouten vanuit Bron- en Doelsystemen gesignaleerd en gelogd worden. Bijvoorbeeld: ontbrekende gegevens, onjuiste coderingen, mislukte verwerking, etc.)

Nummer	Categorie	Omschrijving
EF-103	Provisioning & Connectivity	De Oplossing monitort continue de status van de actieve Koppelingen.
EF-104	Provisioning & Connectivity	De Oplossing registreert de ingetrokken accounts in een logbestand. Toelichting: Een ingetrokken Account is een Account die op verwijderd of gedeactiveerd staat. Dit kan vanuit verschillende processen zijn gebeurd, zoals bijvoorbeeld vanuit het Attestatieproces.
EF-105	Provisioning & Connectivity	De Oplossing biedt overzicht van welke (AD) groepen gekoppeld zijn aan Doelsystemen.
EF-106	Provisioning & Connectivity	De Oplossing biedt overzicht van geneste groepen op de gekoppelde Doelsystemen.
EF-107	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage die alle Identiteiten toont met meer dan één Account (en welke dat zijn), inclusief in- en uitdienstdatum.
EF-108	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage die alle afdelingen getoont waar geen Locatie aan is gekoppeld.
EF-109	Rapportage functionaliteit	Opdrachtnemer levert een standaard rapportage waarmee gecontroleerd kan worden dat er daadwerkelijk geen dubbele Accounts zijn aangemaakt.
EF-110	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage waarmee gecontroleerd kan worden dat er geen dubbele resources in een systeem zijn (bijv. geen dubbele AD groepen voor dezelfde applicatie).
EF-111	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage die alle functionele Accounts toont die gekoppeld zijn aan een functionele mailbox, maar waar geen (in dienst zijnde) Leidinggevende aan gekoppeld is
EF-112	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage die een overzicht toont met alle Accounts waarvan de Medewerker uitdienst is maar nog actief is in overeenstemming met de norm (nu 30 dagen).
EF-113	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage waarmee inzichtelijk gemaakt wordt aan welke rollen geen Autorisaties zijn gekoppeld.
EF-114	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage waarmee inzichtelijk gemaakt wordt welke rollen door wie uit te delen zijn (ook als het veld door wie leeg is).
EF-115	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage waarmee inzichtelijk gemaakt wordt welke resources extern wel zijn verwijderd maar nog niet in de Oplossing zelf. Het gaat hier om een rapportage van resources die zijn verwijderd in de Doelapplicatie, maar nog bestaan in de Oplossing.
EF-116	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage die een overzicht van Autorisaties toont die handmatig zijn toegevoegd in systemen maar geen koppeling hebben met de Oplossing, bijvoorbeeld een AD-groep die niet gebruikt is in de Oplossing. Zie ook toelichting EF-58.
EF-117	Rapportage functionaliteit	Opdrachtnemer levert een standaardrapportage met een overzicht van Identiteiten waarvan het wachtwoord binnenkort gaat verlopen.

Nummer	Categorie	Omschrijving
EF-118	Risk Modeling	De Oplossing kan Attributen uit het Bronsysteem gebruiken om een Identiteits-risicoscore te beïnvloeden, zoals locatie, werknemersstatus enzovoort.
EF-119	Risk Modeling	De Oplossing kan Eindgebruikers en Accounts met een hoog risico gemakkelijk identificeren middels analyses en rapportages.
EF-120	Risk Modeling	De Oplossing kan de (risico)score van een Eindgebruiker en Account verhogen als zij toegang krijgen tot bestanden en mappen die gevoelige data bevatten.
EF-121	Role Management	De Oplossing maakt automatische roltoekenning/-intrekking mogelijk op basis van attributen van Idetiteiten zoals, maar niet beperkt tot functie, afdeling, locatie, leidinggevende, begin- en einddatum.
EF-122	Role Management	De Oplossing biedt scheduling (plannen in de tijd) voor rol en/of toegangsrecht toekenning en rol en/of toegangsrecht intrekking.
EF-123	Role Management	De Oplossing is configureerbaar zodat per rol / toegangsrecht wanneer deze automatisch (direct [default] of niet) worden ingetrokken aan het einde van het dienstverband.
EF-124	Role Management	Bij elke rol moet een roleigenaar kunnen worden opgenomen, zodat zij ook als verantwoordelijke worden aangewezen bij een rol-Attestatie.
EF-125	Self-Service Access Requests	De Oplossing faciliteert het aanvragen/wijzigen/intrekken van minimaal, maar niet gelimiteerd tot, Accounts(alle types), Autorisaties en rollen.

EA2023047 Identity & Access Management: Bijlage F - Programma van Eisen (non-functionals)

Nummer	Categorie	Omschrijving
ENF-01	Algemeen	Opdrachtnemer is verantwoordelijk voor de realisatie van de toekomstige situatie, zoals beschreven in Bijlage J - Toekomstige situatie (SOLL)
ENF-02	Algemeen	Opdrachtnemer stelt een functioneel-technische handleiding beschikbaar van alle Beheerders-functionaliteit binnen de Oplossing, waaronder informatie over Koppelingen, rapportages en gebruikersbeheer.
ENF-03	Algemeen	De Eindgebruiker kan de Oplossing benaderen via een webbased applicatie.
ENF-04	Algemeen	De presentatielaag van de Oplossing (browser) functioneert met minimaal de laatste twee versies van: - Google Chrome; - Microsoft Edge; En moet marktconforme browsers ondersteunen (Marktconform als het een aandeel heeft van 5% (of meer) van de markt, volgens W3.org, of de natuurlijke opvolger is van een bestaande marktconforme browser).
ENF-05	Algemeen	De Oplossing is gebruikersvriendelijk (conform de meest actuele versie van WCAG). Dit houdt tenminste in dat het aantal handelingen dat nodig is om een taak uit te voeren zo beperkt mogelijk is, dat de gebruikersinterface overzichtelijk is, dat gebruikersinterface en gebruikerservaring (user experience) intuïtief zijn en beperkte training vereisen, dat er een snelle eenvoudige zoekfunctie beschikbaar is voor Eindgebruikers waarmee informatie en functies eenvoudig vindbaar zijn.
ENF-06	Beheerprocessen en monitoring	Audit-logs mogen nooit verloren gaan, ook niet bij verstoringen
ENF-07	Koppelingen en integraties	De Oplossing moet aansluiten op de standaard dienst (autorisatie): 'SVB eenmalig aanloggen' Nu gerealiseerd door Azure AD SSO/MFA.
ENF-08	Koppelingen en integraties	De Oplossing moet aansluiten op ten minste 1 van de verplichte standaarden van de overheid (PTOLU): SAML 2.0 of Oauth 2.0/OpenID Connect 1.0. Alternatief: WS-Federation v1.2
ENF-09	Koppelingen en integraties	Procesdata en metadata kunnen uit de productie-omgeving worden geëxporteerd, zodat rapportages kunnen worden gemaakt voor analyse- en verantwoordingsdoeleinden.
ENF-10	Koppelingen en integraties	De Oplossing biedt een directe mailfunctionaliteit (versturen van email vanuit de applicatie) via Microsoft 365 m.b.v. het SMTP protocol, met ondersteuning van Modern Authentication.
ENF-11	Koppelingen en integraties	Gegevens in Koppelingen zijn tijdens transport minimaal volgens de standaard TLS 1.2 of hoger.
ENF-12	Koppelingen en integraties	Koppelingen met Bron-en Doelsystemen zijn mogelijk via queueing in IBM MQ en ActiveMQ en webservices in SOAP/XML en REST/JSON.
ENF-13	Koppelingen en integraties	Koppelingen hebben duidelijke specificaties die beschreven zijn in descriptor documents.

Nummer	Categorie	Omschrijving
ENF-14	Koppelingen en integraties	Koppelingen zijn RESTful en ondersteunen Create-Read-Update-Delete (CRUD) functies.
ENF-15	Koppelingen en integraties	Opdrachtnemer zorgt dat alle (maatwerk- en standaard) Koppelingen blijven werken bij nieuwe software-releases- en upgrades van de Oplossing. Deze Koppelingen maken tevens deel uit van het informatiebeveiligingsbeleid van Opdrachtnemer en vallen binnen de scope van de SLA.
ENF-16	Koppelingen en integraties	Opdrachtnemer zorgt dat de Oplossing blijven voldoen aan de IAM Integratiestandaarden van het forum standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden). Dit geldt voor de verplichte standaarden én de aanbevolen standaarden op het gebied van IAM.
ENF-17	Koppelingen en integraties	Koppelingen stellen de SVB in staat om near-realtime data uit te wisselen met de test-en acceptatie omgeving.
ENF-18	Retransitie	Alle aanwezige SVB data en gegevens in de Oplossing worden binnen twee weken na beëindiging van de Overeenkomst kosteloos geretourneerd aan de SVB, in een gangbaar en marktconform formaat.
ENF-19	Retransitie	Voor alle geretourneerde SVB data en gegevens wordt een bestandsbeschrijving meegestuurd.
ENF-20	Retransitie	Opdrachtnemer verleent alle medewerking die noodzakelijk is voor een soepele overdracht van de Dienstverlening naar een nieuwe leverancier.
ENF-21	Retransitie	Opdrachtnemer zal op verzoek van de SVB een Senior consultant aanbieden tegen de geldende Tarieven, voor eventuele nazorg of begeleiding bij de overdracht.
ENF-22	Retransitie	Opdrachtnemer levert een blauwdruk van de meest actuele systeemconfiguratie en de inrichting van de Oplossing. Deze blauwdruk kan worden geïmporteerd in een eventuele nieuwe instantie van gebruikte software, onder beheer van een nieuwe leverancier. Als import niet mogelijk is dan geeft de blauwdruk tenminste voldoende informatie om een nieuwe instantie van de software zodanig (handmatig) te configureren en in te richten dat deze identiek is aan de Oplossing en dezelfde functionaliteiten biedt. Hiermee wordt geborgd dat bij beëindiging van de Overeenkomst de tijd en kennis die is geïnvesteerd tijdens configuratie en inrichting van de Oplossing, nimmer verloren gaat.
ENF-23	Retransitie	Alle aanwezige SVB data en gegevens in de Oplossing worden permanent verwijderd conform AVG richtlijnen na bevestiging van ontvangst van de data door de SVB na beëindiging van de Overeenkomst. Alle kosten, boetes en herstelbetalingen, voortvloeiende uit het niet permanent verwijderen van de SVB data en gegevens uit de oplossing welke leiden tot een datalek voor de SVB zullen verhaald worden op de Opdrachtnemer.
ENF-24	Service management	Eindgebruikers moeten de Oplossing vanaf een SVB-werkplek kunnen benaderen en de Oplossing kunnen gebruiken in overeenstemming met de afgesproken service levels.
ENF-25	Service management	Opdrachtnemer moet voorzien in passende technische en organisatorische maatregelen, waaronder monitoring, om Incidenten in de productie-omgeving van de Oplossing snel (conform SLA) te kunnen detecteren, onderzoeken en op te lossen.

Nummer	Categorie	Omschrijving
ENF-26	Service management	Opdrachtnemer zorgt voor back-ups (en restoremogelijkheden) zodat er geen dataverlies kan optreden. Opdrachtnemer is verantwoordelijk voor controle van de integriteit van die back-ups, alsmede het waarborgen van de vertrouwelijkheid en beschikbaarheid daarvan.
ENF-27	Service management	De Opdrachtnemer heeft een Single Point Of Contact voor escalaties.
ENF-28	Service management	Opdrachtnemer moet voorzien in technische en organisatorische maatregelen, waaronder een incidentmanagementtool, voor het prompt registreren, administreren en rapporteren van Incidenten, problemen, wijzigingen, en vergelijkbare correspondentie. Opdrachtnemer zorgt ervoor dat de SVB te allen tijde toegang heeft tot deze incidentmanagementtool, en dat de SVB te allen tijde de status van Incidenten, problemen, wijzigingen, en bijbehorende correspondentie kan inzien.
ENF-29	Service management	Opdrachtnemer draagt zorg voor de volledige infrastructuur van de Oplossing, waaronder de in ieder geval housing, hosting en het technisch beheer.
ENF-30	Service management	In geval van een ernstig Incident waardoor de Dienstverlening voor langere tijd onbeschikbaar of onbruikbaar is geweest, levert Opdrachtnemer op verzoek van de SVB binnen 10 werkdagen een 'Root Cause Analysis' plus passend verbeterplan aan, met daarin tenminste de volgende informatie: • Beschrijving van het Incident en het aantal getroffen gebruikers • Beschrijving van de oorzaak van het Incident • Beschrijving van de tijdelijke en/of permanente oplossing. • Beschrijving van de maatregelen ter voorkoming van herhaling • Planning van het vervolgproces • Overige feiten en cijfers
ENF-31	Service management	Opdrachtnemer zorgt voor geografische redundantie van de oplossing en hosting zodat uitwijken mogelijk is bij uitval.
ENF-32	Service management	Alle Gebruikersinterface-schermen van de Oplossing worden binnen 5 seconden getoond.
ENF-33	Service management	Batchverwerkingen (mag ook overdag) binnen de Oplossing beïnvloeden de performance van de Oplossing voor andere Eindgebruikers niet negatief.
ENF-34	Service management	Opdrachtnemer geeft periodiek inzicht (ten minste éénmaal per maand) in de geleverde prestaties, dmv een SLA rapportage op de afgesproken KPI's
ENF-35	Service management	Direct na inwerkingtreding van de Overeenkomst zal de Opdrachtnemer met de SVB afspraken maken over de invulling van een Dossier Afspraken en Procedures (DAP), waarin operationele afspraken worden gemaakt die gedurende de inrichting van de Prestatie en tijdens de looptijd van de Nadere overeenkomst van toepassing zijn.

Nummer	Categorie	Omschrijving
ENF-36	Service management	Bij het niet halen van de afgesproken service levels van de Dienstverlening, start Opdrachtnemer onverwijld een onderzoek naar de oorzaak daarvan en rapporteert zij schriftelijk hierover aan de SVB. Dat rapport moet ook een (voorlopig) plan voor verbetering en planning daarvan bevatten. Opdrachtnemer neemt het initiatief om deze rapportage met de SVB te bespreken.
ENF-37	Service management	Opdrachtnemer rapporteert periodiek (ten minste éénmaal per kwartaal) over de voortgang van de realisatie van eventuele verbeterplannen.
ENF-38	Service management	De Opdrachtnemer verplicht zich tot verbeteren / vernieuwen / bijhouden en tijdig realiseren van deze verbeteringen c.q. wijzigingen in de Oplossing naar aanleiding van nieuwe of gewijzigde wet- en regelgeving en landelijke standaarden voor overheden zonder hiervoor extra kosten in rekening te brengen.
ENF-39	Service management	Op verzoek van de SVB kunnen er aanvullende overleggen naast het maandelijks rapportage worden ingeregeld zoals: - security overleg - tactisch overleg - strategisch overleg - architectuur overleg
ENF-40	Service management	De Oplossing heeft een Beschikbaarheid van ten minste 99,5% op maandbasis exclusief gepland Onderhoud. Beschikbaarheid wordt gemeten over iedere periode van (1) kalendermaand.
ENF-41	Service management	Opdrachtnemer zal een SLA opstellen die onderdeel zal worden van de Overeenkomst en die ten minste voldoet aan de eisen uit het PVE.
ENF-42	Service management	Opdrachtnemer doet een voorstel voor de parameters in de SLA op basis waarvan de prioriteit (P1 t/m P5) van Incidenten en problemen wordt vastgesteld. De prioritering wordt bepaald aan de hand van impact x getroffen gebruikersgroep, bij voorkeur uitgedrukt in een matrix.
ENF-43	Service management	Opdrachtnemer hanteert de volgende Responstijden: - Prio 1: 95% < 15 min - Prio 2: 95% < 15 min - Prio 3: 95% < 60 min - Prio 4: 95% < 8 uur - Prio 5: 95% < 8 uur

Nummer	Categorie	Omschrijving
ENF-44	Service management	Opdrachtnemer hanteert de volgende Oplostijden : - Prio 1: 95 % < 4 uur - Prio 2: 95 % < 8 uur - Prio 3: 95 % < 16 uur - Prio 4: 95 % < 50 uur - Prio 5: 95 % < 120 uur
ENF-45	Service management	De productieomgeving van de Oplossing is voldoende schaalbaar en performant zodat deze op piekmomenten tot 1500 concurrent users kan opvangen, tegen gelijkblijvende performance en in overeenstemming met SLA.
ENF-46	Service management	Gepland Onderhoud vindt uitsluitend op werkdagen plaats tussen 21:00u en 7:00u CET. Dag en tijdstip worden tenminste vijf (5) kalenderdagen vooraf gecommuniceerd aan de SVB, waarbij duidelijk wordt gemaakt waarvoor Onderhoud nodig is, en hoe lang het maximaal gaat duren.
ENF-47	Service management	Minimaal tien (10) Beheerders kunnen simultaan werken op de productie-omgeving
ENF-48	Service management	Opdrachtnemer denkt mee met de SVB in het beheersen van de dagelijkse problematiek, werkt goed samen met de SVB en stelt zich op als een partner van de SVB.
ENF-49	Service management	Opdrachtnemer fungeert als schakel tussen materie en techniek, bezit hiervoor voldoende IT-kennis en materiedeskundigheid, en is in staat om op een strategisch niveau met de SVB mee te denken.
ENF-50	Service management	Opdrachtnemer denkt mee over de consequenties van door de SVB ingediende wijzigingsvoorstellen, en wijst op de mogelijke gevolgen als deze wijzigingsvoorstellen een negatieve impact kunnen hebben.
ENF-51	Training	De Opdrachtnemer draagt zorg voor de uitvoering van opleidingen voor de volgende gebruikers: 1. Beheerders 2. IAM coordinatoren 3. Product Owners