



Uitvoeringsorganisatie
Bedrijfsvoering Rijk
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Inkoop Oplossingskader

UBR|HIS

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage	D3
Kenmerk	201700268.067
Betreft Europese aanbesteding	Informatiesysteem voor Schatkistbankieren

Inhoud

1.	Inleiding	3
1.1.	Definition of Done	3
1.2.	Principes, Non-functionals en Aansluitvoorwaarden	3
2.	Toe te passen principes	4
2.1.	Inleiding	4
2.2.	De informatievoorziening is compliant met voor de overheid geldende wetgeving, voorschriften en standaarden	4
2.3.	De klant of gebruiker staat centraal.....	4
2.4.	Alle bij Schatkistbankieren vastgelegde gegevens zijn broninformatie of worden van een bronregistratie afgenomen.....	5
2.5.	Gelijksoortige functies worden modulair ingericht en informatie wordt aangeboden, opgevraagd en gecommuniceerd	5
2.6.	Gegevens zijn onafhankelijk van systemen en functies ingericht	5
3.	Non-functional requirements	6
3.1.	Functionele geschiktheid	6
3.2.	Prestatie-efficiency	6
3.3.	Uitwisselbaarheid	7
3.4.	Bruikbaarheid	7
3.5.	Betrouwbaarheid.....	8
3.6.	Beveiligbaarheid	8
3.7.	Onderhoudbaarheid.....	9
3.8.	Overdraagbaarheid.....	10
4.	Aansluitvoorwaarden Housing en Hosting.....	11
4.1.	Inleiding	11
4.2.	Vertrouwelijkheid	11
4.3.	Mission Critical Cloud.....	11
4.4.	Omgevingen	11
4.5.	Servers.....	12
4.6.	Operating systems	12
4.7.	Networking	12
4.8.	Directory Services	12
4.9.	Technische Standaarden	13

1. Inleiding

Dit document plaatst de vereisten, waaraan de oplossing voor Schatkistbankieren moet voldoen, in context en vormt het uitgangspunt voor het opstellen van acceptatiecriteria.

1.1. Definition of Done

Voor het iteratieve proces van realisatie en implementatie stelt het ministerie de volgende definition of done voor:

- a) **Documentatie** (in de vorm van bestanden of databases) is bijgewerkt:
 - Beheerdocumentatie;
 - Gebruikershandleiding;
 - Procesdocumentatie;
- b) De user story voldoet aan de in dit document gestelde eisen en de specifiek voor de user story opgestelde acceptatiecriteria;
- c) De **Product Owner** heeft de user story bekeken en goedgekeurd;
- d) De **actor** uit de user story heeft de user story bekeken en goedgekeurd. Indien de actor een deelnemer is, gebeurt dit samen met een medewerker van het ministerie;
- e) De **Functioneel Beheerder** heeft de user story bekeken en goedgekeurd;
- f) De **Technisch Beheerder** heeft – indien relevant – de user story bekeken en goedgekeurd;

1.2. Principles, Non-functionals en Aansluitvoorwaarden

Binnen de navolgende hoofdstukken komen de volgende onderwerpen aan de orde:

- Hoofdstuk twee beschrijft de algemene principes met betrekking tot informatievoorziening zoals opgesteld door de CIO van het ministerie van Financiën;
- Hoofdstuk drie omvat de zogenoemde Non-functionals die van toepassing zijn op de oplossing voor Schatkistbankieren;
- Hoofdstuk vier beschrijft de aansluitvoorwaarden, dat wil zeggen de eisen die worden gesteld vanuit de derde partij (Beheerpartij) die is gecontracteerd voor housing en hosting.

Specifieke acceptatiecriteria per user story, zijn/worden opgenomen in Bijlage D4 Product Backlog.

Overige acceptatiecriteria worden vastgesteld binnen het kader van hetgeen beschreven is in hoofdstukken twee, drie en vier. Vaststellen betekent in dit verband: rechtstreeks toepassen dan wel, waar nodig, nader afleiden/concretiseren.

Er kan sprake zijn van overlap tussen de hier beschreven vereisten in hoofdstukken twee, drie en vier. Bij aanvang van de realisatie van versie 1 van het systeem voor Schatkistbankieren zal eventuele overlap tussen vereisten worden weggenomen waarna aanpassing van deze Bijlage volgt.

2. Toe te passen principes

2.1. Inleiding

Het Agentschap van Generale Thesaurie en de Rijkshoofdboekhouding zijn de processen van Schatkistbankieren aan het optimaliseren en digitaliseren. Hiertoe is een project opgestart dat moet leiden tot:

- Een betere dienstverlening naar Deelnemers aan Schatkistbankieren.
- Een verhoogde kwaliteit van de door Schatkistbankieren geleverde diensten.
- Een toename in de efficiëntie en doelmatigheid in de processen Schatkistbankieren bij zowel Deelnemers als in de eigen operatie.

Om te zorgen dat de ondersteunende informatievoorzieningen voldoen aan de bij het Ministerie van Financiën gestelde uitgangspunten worden onderstaande principes gehanteerd. Deze principes gelden voor alle informatievoorzieningen en worden deels ingevuld door het ministerie zelf en deels door leveranciers.

2.2. *De informatievoorziening is compliant met voor de overheid geldende wetgeving, voorschriften en standaarden*

Voor Schatkistbankieren betekent dit dat de van belang zijnde wet- en regelgeving, voorschriften, overheidsbouwstenen en standaarden zijn onderzocht. De inrichting van de informatievoorziening is hier compliant aan. Voorbeelden voor relevante onderwerpen bij Schatkistbankieren zijn:

1. De privacywetgeving bij de vastlegging van Deelnemers en andere gebruikers. Vastgelegd in een privacy impact assessment (PIA); maatregelen die hier uit voortvloeien zijn opgenomen in het Programma van Eisen;
2. Wet digitale overheid met o.a. door de overheid erkende voorzieningen voor Identity Management;
3. De archiefwet voor de vastlegging en bewaartermijn van persoonsgegevens en zaakdossiers.
4. Het hergebruik van overheidsbouwstenen, zoals bijvoorbeeld het gebruik van basisregistratie voor de vastlegging van Deelnemers;
5. Veiligheidsnormen bij het gebruik van vertrouwelijke gegevens. Denk aan normen als:
 - o (BIR:2017 en DGOBR Quickscan BIR:2014),
 - o BIO (Baseline Informatiebeveiliging Overheid die in de maak is, maar in 2019 ingaat),
 - o het VIR-BI en
 - o de standaarden NEN-ISO/IEC 27001 en 27002.

Van toepassing zijnde beveiligingsnormen op basis van een uitgevoerde IRAM (Information Risk Assessment Methodology) zijn opgenomen in het programma van Eisen

6. Overheidsreferentienormen, zoals de NORA en de eigen EA van het departement Ministerie van Financiën wanneer deze gereed is;
7. Het gebruik van (open) standaarden, zoals vastgelegd door het Forum Standaardisatie.

2.3. *De klant of gebruiker staat centraal*

Zichtbaar kan aangetoond worden dat de informatievoorziening vanuit gebruiker is ingericht, zodat de informatievoorziening gebruikers optimaal ondersteunt bij de dagelijkse uitvoering van hun werkzaamheden. Gebruikers worden daarom al vroeg betrokken bij de inrichting van de processen, de ontwerpen van informatievoorziening, het beoordelen van de presentaties van de gebruikersinterface en de werking van het systeem, etc. Hiervoor worden gebruikersraden ingericht en representatieve gebruikers bij het project betrokken.

Dit wordt vervolgens eveneens tijdens de gehele levenscyclus van de informatievoorziening geborgd. Want de werking van het systeem kan en zal in de loop van tijd zeer waarschijnlijk veranderen.

2.4. Alle bij Schatkistbankieren vastgelegde gegevens zijn broninformatie of worden van een bronregistratie afgenomen

Belangrijk is dat gegevens integer en betrouwbaar zijn. Daarom worden gegevens door geïdentificeerde entiteiten vastgelegd of van bronregistraties afgenomen. De gegevens zijn daarbij uniek geïdentificeerd en verrijken het gegevenslandschap zonder dat er overlap tussen of dubbelingen in vastgelegde gegevens bestaat.

Het kopiëren van gegevens is uit den boze. Deze worden altijd van de vastgelegde bron afgenomen. Zo wordt voorkomen dat er fouten ontstaan op basis van verkeerde (kopieën van) gegevens.

2.5. Gelijksortige functies worden modulair ingericht en informatie wordt aangeboden, opgevraagd en gecommuniceerd

Gelijksortige bedrijfsfuncties met bewerkingen op gelijksortige informatieobjecten worden zoveel mogelijk gebundeld en in afgebakende en ontkoppelbare modules gerealiseerd. Functies en gegevens worden daarbij via koppelvlakken en open standaarden ontsloten en als diensten (services) beschikbaar gesteld aan de omgeving.

Zo wordt bereikt dat:

- het beheer en het aanpassen van functies chirurgisch kan worden uitgevoerd op de specifieke functionele module en de koppelvlakken van de module. Het beheer blijft zo beperkt tot die module en zijn koppelvlakken. De complexiteit van veranderingen, de beheerlast en de doorlooptijd van het realiseren van functionele aanpassingen zal hierdoor afnemen;
- functionaliteit en informatie als dienst wordt aangeboden. Het wordt zo eenvoudiger om specifieke functionele modules via services beschikbaar te stellen voor hergebruik. Functionaliteit – en daarmee ook informatie – wordt eenvoudiger benaderbaar. Ook vanuit andere processen en informatievoorzieningen, als de situatie hierom vraagt.

2.6. Gegevens zijn onafhankelijk van systemen en functies ingericht

De business logica van de bedrijfsfuncties is gescheiden van de gegevens, zodat:

- deze eenvoudig benaderbaar zijn vanuit andere modules met andere bedrijfsfuncties (data integratie).
- gegevens gemakkelijk kunnen worden verplaatst tussen verschillende toepassingsprogramma's, computeromgevingen of cloud services (data portabiliteit).
- er een complexiteitsreductie wordt gerealiseerd, welke tot een overzichtelijker en eenvoudiger beheer van het gegevenslandschap leidt.

Hierdoor wordt het eenvoudiger om gegevens in een breder verband te kunnen (her)gebruiken en wordt het eenvoudiger om gegevens van systeem A naar systeem B te migreren bij bijvoorbeeld de vervanging van een (deel van een) applicatie of module.

3. Non-functional requirements

Voor de in te richten oplossing ter ondersteuning van het proces schatkistbankieren zijn hieronder de relevante non-functional requirements toegelicht. Bij het beschrijven van de non-functional requirements is er gebruik gemaakt van ISO 25010. De nadere invulling van deze requirements kan als volgt plaatsvinden:

- concrete eisen, welke zijn opgenomen in Bijlage 1 Akkoordverklaring Programma van Eisen;
- acceptatiecriteria, welke zijn opgenomen in Bijlage D4 Product Backlog;

3.1. Functionele geschiktheid

De mate waarin een softwareproduct of computersysteem functies levert die voldoen aan de uitgesproken en veronderstelde behoeften, bij gebruik onder gespecificeerde condities.

Functionele compleetheid

De mate waarin de set van functies alle gespecificeerde taken en gebruikersdoelen ondersteunen.

Het systeem moet functioneel alle taken ondersteunen die minimaal nodig zijn om het proces van Schatkistbankieren te ondersteunen. Daarnaast is het wenselijk dat een aantal wensen worden gerealiseerd. Welke wensen dit betreft wordt benoemd in het processendocument.

Functionele correctheid

De mate waarin een softwareproduct of computersysteem de juiste resultaten met de benodigde nauwkeurigheid beschikbaar stelt.

De functies van het systeem moeten resulteren in de juiste effecten en met name in de financiële administratie.

3.2. Prestatie-efficiency

De prestaties in verhouding tot de hoeveelheid middelen gebruikt onder genoemde condities

Snelheid

De mate waarin antwoord- en verwerkingstijden en doorvoersnelheid van een product of systeem, tijdens de uitvoer van zijn functies, voldoet aan de wensen.

Het systeem moet handmatige verwerkingen direct verwerken, zonder dat er een pauze ontstaat. Hetzelfde geldt voor het maken van offertes, eenvoudige overzichten. Bij complexe rapportages en batchverwerkingen is een beperkte verwerkingstijd (een aantal seconden tot minuten afhankelijk van het proces) acceptabel.

Middelenbeslag

De mate waarin de hoeveelheid en type middelen die gebruikt worden door een product of systeem, tijdens de uitvoer van zijn functies, voldoet aan de wensen.

Op het moment dat van het systeem tijdelijk hogere prestatie worden gevraagd, kan deze capaciteit snel en gemakkelijk worden bijgeschakeld.

Capaciteit

De mate waarin de maximale limieten van een product- of systeemparemeter voldoet aan de wensen.

Er moeten minstens 530 gebruikers (500 deelnemers en 30 medewerkers van het ministerie van Financiën) tegelijk in het systeem kunnen werken. Het totale aantal unieke gebruikers is voorzien op 6.135 (6100 deelnemers en 35 medewerkers van het ministerie van Financiën).

3.3. Uitwisselbaarheid

De mate waarin een product, systeem of component informatie uit kan wisselen met andere producten, systemen of componenten, en/of het de gewenste functies kan uitvoeren terwijl het dezelfde hard- of softwareomgeving deelt.

Beïnvloedbaarheid

De mate waarin een product zijn gewenste functies efficiënt kan uitvoeren terwijl het een gemeenschappelijke omgeving en middelen deelt met andere producten, zonder nadelige invloed op enig ander product.

Wanneer een systeem is opgebouwd uit verschillende modules, dan moet het samenspel vlekkeloos werken zonder in te leveren op de prestatie en visualisatie op het scherm.

Koppelbaarheid

De mate waarin twee of meer systemen, producten of componenten informatie kunnen uitwisselen en de uitgewisselde informatie kunnen gebruiken.

Informatie moet eenvoudig tussen functioneel afgebakende modules kunnen worden uitgewisseld via open standaarden. Dit geldt ook voor nog niet benoemde modules die in de toekomst mogelijk nog aan het systeem worden toegevoegd.

3.4. Bruikbaarheid

De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om effectief, efficiënt en naar tevredenheid gespecificeerde doelen te bereiken in een gespecificeerde gebruikscontext.

Leerbaarheid

De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om gespecificeerde leerdoelen te bereiken met betrekking tot het gebruik van het product of systeem met effectiviteit, efficiëntie, vrijheid van risico, en voldoening, in een gespecificeerde gebruikscontext.

Het systeem is eenvoudig in het gebruik. De essentiële functies van het systeem kunnen zonder cursus of toelichting worden gebruikt.

Voor interne gebruikers van Schatkistbankieren is het denkbaar dat bepaalde functies complexer zijn en uitleg nodig hebben.

Bedienbaarheid

De mate waarin een product of systeem attributen heeft die het makkelijk maken om het te bedienen en beheersen.

De werking moet voor zichzelf spreken. Daar waar nodig biedt het systeem toelichtingen, naar voorbeeld van de gele ballonnetjes van de Belastingdienst. Door diverse schermen heen klikken om een handeling uit te voeren is uit den boze.

Voorkomen gebruikersfouten

De mate waarin het systeem gebruikers beschermt tegen het maken van fouten.

Bij de invoer van schermen wordt via algoritmes getoetst op foutieve invoer van gegevens en de compleetheid van de ingevoerde gegevens.

Volmaaktheid gebruikersinteractie

De mate waarin een gebruikersinterface het de gebruiker mogelijk maakt om een plezierige en voldoening gevende interactie te hebben.

De gebruikersinterface ziet er modern uit (webbankieren). Het voldoet aan de webrichtlijnen.

3.5. Betrouwbaarheid

De mate waarin een systeem, product of component gespecificeerde functies uitvoert onder gespecificeerde condities gedurende een gespecificeerde hoeveelheid tijd.

De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

Beschikbaarheid

De mate waarin een systeem, product of component operationeel en toegankelijk is wanneer men het wil gebruiken.

Het systeem is tenminste op werkdagen (target2 settlement dagen) van 6:00 uur tot 20:00 uur voor 99,8% beschikbaar. Geplande momenten voor systeemonderhoud vallen buiten deze beschikbaarheidseis.

Foutbestendigheid

De mate waarin een systeem, product of component werkt zoals bedoeld ondanks de aanwezigheid van hard- of softwarefouten.

Het systeem moet foutmeldingen genereren wanneer het crasht, maar blijft wel werken. Ingevoerde data blijft ondanks vastlopen van het systeem bewaard.

Herstelbaarheid

De mate waarin het product of systeem, in geval van een onderbreking of bij een fout, de direct betrokken gegevens kan herstellen en het systeem in de gewenste staat kan terug brengen.

Al uitgevoerde bewerkingen worden bewaard en hersteld na het uitvallen van het systeem. Foutieve invoer kan door de betrokken gebruiker zelf worden hersteld.

3.6. Beveiligbaarheid

De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

Vertrouwelijkheid

De mate waarin een product of systeem ervoor zorgt dat gegevens alleen toegankelijk zijn voor diegenen die geautoriseerd zijn.

Alleen die gegevens zijn voor de gebruiker zichtbaar, die deze gebruiker vanuit zijn rol (op basis van zijn identiteit), werkzaamheden en toegekende autorisaties nodig heeft (AVG).

Integriteit

De mate waarin een systeem, product of component ongeautoriseerde toegang tot of aanpassing van computerprogramma's of gegevens verhindert.

Alleen die functies zijn voor de gebruiker toegankelijk, die deze gebruiker vanuit zijn rol (op basis van zijn identiteit), werkzaamheden en toegekende autorisaties nodig heeft (AVG).

Ongeautoriseerde toegang tot functies van het systeem zijn onmogelijk en er wordt signaleerd en gelogd, wanneer hier pogingen toe worden gedaan.

Voor de meest cruciale functies (financiële functies en instellen van autorisaties) geldt het vier ogen principe.

Onweerlegbaarheid

De mate waarin kan worden bewezen dat acties of gebeurtenissen plaats hebben gevonden, zodat later deze acties of gebeurtenissen niet ontkend kunnen worden.

Alle handelingen en bewerkingen door gebruikers en het systeem worden gelogd en voor een bepaalde periode bewaard (archiefwet).

Verantwoording

De mate waarin acties van een entiteit getraceerd kunnen worden naar die specifieke entiteit.

Alle handelingen en bewerkingen door gebruikers en het systeem zijn traceerbaar naar een entiteit of persoon.

Authenticiteit

De mate waarin bewezen kan worden dat de identiteit van een onderwerp of bron is zoals wordt beweerd.

De bewijsbaarheid van identiteit is gebaseerd op meer factor authenticatie.

Voorkeur voor deelnemers gaat uit naar een door de overheid geaccepteerde standaard, zoals eHerkenning.

De mate waarin een claim over de oorsprong of de auteur van de informatie verifieerbaar is, bijvoorbeeld aan handschrift.

Alle handelingen en bewerkingen in het systeem worden gekoppeld aan een entiteit, waarvan de identiteit en autorisatie (bevoegdheid) is gecontroleerd.

Voorkeur voor deelnemers gaat uit naar een overheidsvoorziening, zoals eHerkenning.

3.7. Onderhoudbaarheid

De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden door de aangewezen beheerders.

Modulariteit

De mate waarin een systeem of computerprogramma opgebouwd is in losstaande componenten zodat wijzigingen van een component minimale impact heeft op andere componenten.

Het systeem is modulair uit functionele modules of componenten opgebouwd. Over de koppelvlakken zijn afspraken gemaakt, zodat een module of component via het plug-and-play principe vervangen of vernieuwd kan worden. Functies uit modules of componenten van het systeem kunnen door externe systemen worden aangesproken en worden gebruikt.

Uitgangspunt van deze eis is het vereenvoudigen van het functionele beheer en het terugdringen van complexiteit bij de doorlooptijd van het realiseren van wijzigingen.

Analyseerbaarheid

De mate waarin het mogelijk is om effectief en efficiënt de impact, van een geplande verandering van één of meer onderdelen, op een product of systeem te beoordelen, om afwijkingen en/of foutoorzaken van een product vast te stellen of om onderdelen te identificeren die gewijzigd moeten worden.

Het kunnen analyseren van de impact van een wijziging is belangrijk om de complexiteit en de effecten van de wijziging te kunnen bepalen. Dit in relatie met het bepalen of een wijziging qua impact gewenst is en om te kunnen bepalen of en wanneer deze wordt doorgevoerd.

Wijzigbaarheid

De mate waarin een product of systeem effectief en efficiënt gewijzigd kan worden zonder fouten of kwaliteitsvermindering tot gevolg.

Wijzigingen worden aangebracht met inachtneming van het systeemconcept en onder architectuur. Als basis geldt, dat wijzigingen worden verzameld en uitgebracht als nieuwe release van het systeem. Daarnaast moeten ook kleine wijzigingen kunnen worden uitgevoerd, vooruitlopend op een nieuwe release. Spoedwijzigingen zijn het gevolg van incidentafhandeling en worden verwerkt conform afspraak in de Service Level Agreement. Wijzigingen leiden niet tot het optreden van eerder herstellende onvolkomenheden of onvolkomenheden in onderdelen van het systeem die niet gewijzigd zijn.

Testbaarheid

De mate waarin effectief en efficiënt testcriteria vastgesteld kunnen worden voor een systeem, product of component en waarin tests uitgevoerd kunnen worden om vast te stellen of aan die criteria is voldaan.

Alle functionele - en niet functionele wijzigingen die aan het systeem worden gesteld, kunnen door testen worden aangetoond. Dit geldt ook tijdens en na de realisatie van het systeem. Er is een OTAP omgeving ingericht.

3.8. Overdraagbaarheid

De mate waarin een systeem, product of component effectief en efficiënt overgezet kan worden van één hardware, software of andere operationele of gebruiksomgeving naar een andere.

Aanpasbaarheid

De mate waarin een product of systeem effectief en efficiënt aangepast kan worden voor andere of zich ontwikkelende hardware, software of andere operationele of gebruiksomgevingen.

Het systeem kan gemakkelijk bij een willekeurige Beheerpartij worden ondergebracht.

Installeerbaarheid

De mate waarin het product of het systeem effectief en efficiënt geïnstalleerd of verwijderd kan worden in een gespecificeerde omgeving.

De installatie van het product of het systeem is te automatiseren.

Vervangbaarheid

De mate waarin een product een ander specifiek softwareproduct, met hetzelfde doel in dezelfde omgeving, kan vervangen.

Modules of componenten kunnen eventueel eenvoudig via het plug-and-play principe door producten van andere leveranciers worden vervangen, zonder dat dit van invloed is op de vastgelegde gegevens. Kortom: deze zijn gemakkelijk te gebruiken in of om te zetten naar de nieuwe omgeving.

4. Aansluitvoorwaarden Housing en Hosting

4.1. Inleiding

Deze specificatie is opgesteld als kader voor applicaties die binnen de Eenheid-Informatisering (Eenheid-I) moeten “landen”. Eenheid-I maakt hiervoor gebruik van de dienstverlening van een Beheerpartij voor infrastructuur housing en hosting. Overal waar in dit hoofdstuk Eenheid-I is genomen, dient dit gelezen te worden dat dit in samenwerking met de Beheerpartij voor infrastructuur. Dit hoofdstuk is bedoeld voor ontwikkelaars en leveranciers van applicaties en bevat informatie over uitgangspunten, richtlijnen, eisen en wensen waaraan voldaan moet worden.

4.2. Vertrouwelijkheid

Informatie is geclassificeerd in categorieën (labels) om aan te kunnen geven hoe met de gegevens omgegaan mag worden. Deze regelgeving heeft zowel betrekking op wat personen met de informatie mogen doen, als hoe de systemen waar de informatie op wordt verwerkt zijn geplaatst, beveiligd en ingericht.

Er zijn verschillende categorieën van vertrouwelijkheid, waarvan de belangrijkste zijn “Staatsgeheim” ook wel afgekort STG-G en “Departementaal vertrouwelijk” afgekort Dep-V. Dep-V kent verschillende niveaus, zoals “Lage dreiging en geen statelijke actoren”. Met geen statelijke actoren wordt het volgende bedoeld: “groeperingen, bewegingen, organisaties en individuen die geen onderdeel uitmaken van staatsstructuren”. Organisaties waarmee samengewerkt wordt, kunnen hun eigen regels en accreditaties opleggen, zoals gebeurt met Nato en EU.

De oplossing voor Schatkistbankieren is geclassificeerd als Departementaal Vertrouwelijk.

4.3. Mission Critical Cloud

Eenheid-I biedt voor toepassingen binnen het ministerie ontwikkel, test, acceptatie en productie omgevingen aan. Deze worden ondergebracht op de zogenaamde “Mission Critical Cloud” of “MCC”. De applicaties worden geïnstalleerd en beheerd door het co-creatieteam van Eenheid-I en de Beheerpartij.

De gewenste functionele applicatiebeschikbaarheid is 99,8%. Dit betekent dat het infrastructuurontwerp en inrichting, parameterisering en configuratie van de applicaties die beschikbaarheid mogelijk moeten maken.

4.4. Omgevingen

Per applicatie worden de volgende omgevingen voorzien:

omgeving	bevat	functie	toegang
productie	Productie data	Release in productie en beheer conform SLA	Eenheid-I co-creatieteam
acceptatie	Voor productie representatieve data	Release acceptatie en vrijgeven voor productie	Eenheid-I co-creatieteam
test	Test datasets	Release testen en vrijgeven voor Acceptatie	Eenheid-I co-creatieteam

ontwikkel	Ontwikkel datasets	Bouw aan volgende releases	Eenheid-I co-creatieteam en applicatiepartners
------------------	--------------------	----------------------------	--

4.5. Servers

Servers worden virtueel gerealiseerd, tenzij specifieke omstandigheden dit verhinderen. Het virtuele server platform biedt ontkoppeling van fysieke hardware en software: Hierdoor hebben hardware storingen en wijzigingen (zoals vervanging) veel minder impact op de bovenliggende applicatie software.

Uitgangspunten bij de inrichting:

1. Horizontaal schaalbaar (liever meer servers dan grotere servers)
2. Stateless applicaties om seamless failover te kunnen doen (state bijhouden in db of memcache)
3. Open source en free-OS (bijv Centos) om kosten laag te houden en licentie administratie te voorkomen
4. Indien mogelijk geen commerciële database applicaties, zoals bijvoorbeeld Oracle DB, MS-SQL, etc. maar bijvoorbeeld MariaDB, Postgres, etc. of een open NoSQL oplossing. Dit om kosten laag te houden, licentie administratie te voorkomen en afhankelijkheid van leveranciers (lock-in) te verminderen.

4.6. Operating systems

Applicaties moeten op virtual machine kunnen draaien met een x86 compatible operating systeem (Linux of Windows)

Applicaties moeten om kunnen gaan met een up to date operating system. Het installeren van noodzakelijke security updates en functionele updates voor het OS en ondersteunende software mogen geen verstoringen aan de applicatie geven.

Servers worden gehard conform het patroon van de BIR Operationele Handreiking. Dit betekent dat security updates en patches zijn geïnstalleerd binnen de periode die is overeengekomen conform het vigerende beveiligingsbeleid. Binnen het OS worden instellingen aangepast om te voldoen aan de security eisen, zoals de BIR-TNK.

4.7. Networking

Load balancers kunnen de functie van reverse proxy vervullen en worden ingezet wanneer de werklust wordt verdeeld over meerdere applicatieservers en/of datacenter locaties. Hierdoor kunnen ook beheeractiviteiten worden uitgevoerd zonder volledige onderbreking van de beschikbaarheid. Proxy-support en SSL-off-loading is hiermee mogelijk. Proxy functionaliteit kan worden ingezet waar volgens het BIR sprake is van een koppelvlak tussen zones met een verschillend vertrouwelijkheidsniveau en waar dientengevolge sessie ontkoppeling een eis is.

4.8. Directory Services

Directory services voorzien in zoeken, identificeren, authenticatie en autorisatie van verschillende informatieobjecten zoals servers, websites, identiteiten (gebruikers) groepen en configuraties. Directory Services worden gebruikt voor alle bouwblokken.

4.9. Technische Standaarden

Eenheid-I conformeert zich aan de open standaarden past deze toe in zijn producten. Een lijst van Rijksbrede open standaarden is te vinden op de website van het Bureau Forum Standaardisatie: <https://www.forumstandaardisatie.nl/lijt-open-standaarden>.

Ontwikkelde programmatuur mag alleen bij hoge uitzondering gebruik maken van gesloten standaarden. Gebruik van gesloten standaarden dient vooraf gemeld te worden met een motivatie voor het waarom en mag alleen na expliciete toestemming worden ingezet.