****

**Architectuur**

Security Nederland

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Omschrijving** |
| 0.1 | Concept | 5-9-2023 | Ludo CuijpersLeo JaarsmaHenk LinksSebastiaan van Trigt | Basisdocument |
|  |  |  |  |  |

**Vastgesteld door Security Nederland:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| 1.0 |  |  | College van Bestuur |

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en MBO Raad geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.



Creative commons

MBO Raad 4.0 Nederland

(CC BY 4.0) **Copyright**

De gebruiker mag:

Het werk kopiëren, verspreiden en doorgeven

Remixen – afgeleide werken maken

Onder de volgende voorwaarde:

Naamsvermelding – De gebruiker dient bij het werk de naam van MBO Raad te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Inhoudsopgave

[1. Inleiding 3](#_Toc144831359)

[1.1. Doel architectuur 3](#_Toc144831360)

[1.2. Overzicht architectuurprincipes 3](#_Toc144831361)

[1.3. KISS: Keep - IT - (Stupid) – Simple 3](#_Toc144831362)

[1.4. Gegevens vastleggen, valideren en raadplegen in bronsysteem 3](#_Toc144831363)

[1.5. Integratie op basis van services 4](#_Toc144831364)

[1.6. Software-as-a-Service, tenzij 4](#_Toc144831365)

[1.7. Geautoriseerde toegang tot gegevens (systemen, netwerk) 4](#_Toc144831366)

[1.8. De Security Nederland technische infrastructuur is gestandaardiseerd en gebaseerd op volwassen technische componenten 4](#_Toc144831367)

[2. MORA architectuur 5](#_Toc144831368)

[2.1. Aanleiding 5](#_Toc144831369)

[2.2. MORA architectuur en toegewezen proceseigenaren 5](#_Toc144831370)

[2.3. Gebruikte applicaties 6](#_Toc144831371)

[2.4. Systeemscope en gelaagdheid 6](#_Toc144831372)

[Bijlage 1: Aandachtspunten en eisen vanuit Informatiebeveiliging en Privacy aan nieuwe applicaties 7](#_Toc144831373)

# Inleiding

## Doel architectuur[[1]](#footnote-2)

Architectuur gaat om samenhang en verbinding:

* tussen bedrijfsdoelen en inrichting van processen en IT (wat, waarom, hoe)
* in het groeipad van heden naar toekomst (houvast bij veranderen)
* tussen realisatie in projecten en organisatiebelang (balans in goed vs. snel vs. goedkoop)

Architectuur krijgt meerwaarde door samenspel in …

* sturing (visie, samenhang in plannen en projecten)
* inhoud (processen én ICT tezamen beschouwd en afgestemd)
* structuur (werkwijze, overleg, rol- en taakverdeling)

Architectuur geeft inhoudelijk inzicht en richting met …

* principes
* richtlijnen/ standaarden
* modellen (o.a. applicatieplaten)
* roadmap (input voor projectenkalender)

## Overzicht architectuurprincipes



## KISS: Keep - IT - (Stupid) – Simple

**rationale:**

- een gestandaardiseerde processen en IT zijn beter beheersbaar en beter aanpasbaar
 en dragen bovenal bij aan efficiency en het inzetten van doelsystemen in hun kracht,
 d.w.z. (standaard-) functionaliteit gebruiken zoals bedoeld

 best practice voor een eenduidige en consistente informatievoorziening

**gevolgen/ toepassing:**
- best practices van software leveranciers toepassen (proces- en applicatie inrichting)
- standaard configuratie- en parameter instelbaarheden van doelsystemen beperken (less is more)
- haalplicht bij bronsystemen, brengplicht van bronsystemen (t.b.v. eenmalige, eenduidige vastlegging)

## Gegevens vastleggen, valideren en raadplegen in bronsysteem

**rationale:**

- gegevens over o.a. studens, medewerker, klant, product, premie/ tarief, etc. zijn alleen valide en bruikbaar in een proces en/of data-analyse indien afkomstig van het leidende informatiesysteem

**gevolgen/ toepassing:**

- voor elk (kern-)gegeven is helder wat het bronsysteem is

- elk bronsysteem is toegankelijk voor gegevensvastlegging, -wijziging en –raadpleging

## Integratie op basis van services

**rationale:**- het hanteren van bronsystemen impliceert uitwisseling van gegevens tussen processen en systemen

**gevolgen/ toepassing:**
- Security Nederland maakt bij voorkeur gebruik van gecertificeerde (API-)koppelingen, mits geschikt
- Security Nederland maakt daarnaast gebruik van een eigen, iPaaS-gebaseerde integratievoorziening

## Software-as-a-Service, tenzij

**rationale:**
- Security Nederland prefereert cloud-gebaseerde ICT-oplossingen vanwege cloud-voordelen
 (o.a. ontzorging, standaardisatie, flexibiliteit) en de doorontwikkeling van de regie-organisatie

**gevolgen/ toepassing:**- nieuwe ontwikkeling op basis van SaaS, bestaande applicaties zo nodig passief vervangen door SaaS

## Geautoriseerde toegang tot gegevens (systemen, netwerk)

**rationale:**- beheersing van toegang tot gegevens(-verwerking) en aantoonbaar voldoen aan wettelijke en compliance

vereisten vergt toewijzing van rollen en rechten aan gebruikers en monitoring van gebruik

**gevolgen/ toepassing:**
- inrichten van een (centraal) bronsysteem voor gebruikers- en rechtenbeheer,
- inrichten van autorisatie(-matrices) in overige applicatiesystemen.
- registratie van en rapportage over toegang tot functionaliteit en gegevens

## De Security Nederland technische infrastructuur is gestandaardiseerd en gebaseerd op volwassen technische componenten

**rationale:**- infrastructuur-oplossingen maken niet het verschil voor Security Nederland, maar moeten wel goed,

kosteneffectief en schaalbaar zijn, zowel de oplossingen voor (applicatie-) integratie als de oplossingen voor

bijv. werkplekken en (applicatie-) hosting.

**gevolgen/ toepassing:**

- goed is goed genoeg, mits toekomstvast voor 3-5 jaar, schaalbaar, kosteneffectief;
- open standaarden, evt. aangevuld of verrijkt met NL onderwijs standaarden (MORA)
- nieuwe infrastructuur ontwikkelingen op basis van cloud(-infra) tenzij,
- infrastructuurcomponenten kiezen o.b.v. Security Nederland standaarden,
 (e.g. Microsoft Azure/Power ecosysteem voor ETL/ DWH en BI/ rapportage)

# MORA architectuur

## Aanleiding

De snel veranderende arbeidsmarkt en samenleving vragen om vernieuwing en verandering, ook binnen de mbo/hbo-sector. Samenwerking tussen scholen is daarvoor noodzakelijk; een school kan deze veranderingen niet alleen waarmaken. De referentiearchitectuur voor het mbo, de MORA, biedt een gemeenschappelijke structuur en taal om deze samenwerking mogelijk te maken. Ook biedt de MORA een basis om de eigen architectuur mee in te richten, zodat des school optimaal blijft aangesloten op andere scholen.

In de MORA is beschreven hoe een mbo/hbo-school werkt. Welke processen lopen er allemaal binnen een school? Welke informatie gaat er van persoon naar persoon en welke functionaliteiten is er nodig om dit allemaal te ondersteunen? De MORA schrijft niet voor hoe dit allemaal organiseerd moet worden, want dat verschilt van school tot school.

Er zitten veel voordelen aan het gebruik van een architectuur binnen een organisatie. Als duidelijk is hoe zaken in elkaar zitten dan is het gemakkelijker om verbeteringen door te voeren. Verantwoordelijkheden zijn goed afgebakend en de onderwijsinstelling staat sterker naar leveranciers.

## MORA architectuur en toegewezen proceseigenaren[[2]](#footnote-3)



|  |
| --- |
| **College van Bestuur** |
|  |
| **Studentenzaken** |
|  |
| **Onderwijs** |
|  |
| **Examencommissie** |

## Gebruikte applicaties

|  |  |  |
| --- | --- | --- |
| **Proces** | **Proceseigenaar** | **Applicatie** |
| InstroomOnderwijs en studenten administrerenUitstroom | Studentenzaken | Osiris |
| Examineren en diplomeren | Examencommissie | Osiris |
| Human Resource Management | HRM | AFAS HR |
| Financieel Management | Finance | AFAS Finance |

## Systeemscope en gelaagdheid

Tabel met systemen (applicaties) die onze kroonjuwelen ondersteunen en tevens bronsystemen zijn. In de eerste regel staan de kerngegevens van de applicaties (vet gedrukt). De voorbeelden zijn weergegeven (niet vet gedrukt).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Systeem** | **Type** | **Eigenaar** | **Database**Oracle of SQL server | **Middleware**- procesverwerking- Data access- Web middleware | **Operating System**- Windows 10- RHEL 8 | **Virtualisatie**- Citrix- VMware | **Netwerk**Naam van netwerk en evt. netwerkzone | **Servers**- Windows 2016 r2- Ubuntu 22.10 |
| Osiris | SAAS | Hoofd studentenzaken |  |  |  |  |  |  |
| AFAS HR | SAAS | Hoofd HR |  |  |  |  |  |  |
| AFAS Finance | SAAS | Hoord Finance |  |  |  |  |  |  |

Koppelingen zijn weergegeven in het thema data management.

Bijlage 1: Aandachtspunten en eisen vanuit Informatiebeveiliging en Privacy aan nieuwe applicaties[[3]](#footnote-4)

Vanuit Informatiebeveiliging en Privacy zijn er o.a. de volgende aandachtspunten en eisen aan nieuwe applicaties:

1. Welke persoonsgegevens worden binnen de applicatie opgeslagen?

*De verschillende categorieën van persoonsgegevens staan in de dataregisters op de* [*Intranetpagina Informatiebeveiliging & Privacy*](https://mborijnland.sharepoint.com/sites/StafdienstIM/SitePages/Informatiebeveiliging-%26-Privacy.aspx)*.*

1. Kan functionaliteit binnen de applicatie die Security Nederland niet gebruikt, worden uitgeschakeld?

*Denk hierbij ook aan het uitschakelen van velden in de applicatie die binnen het Security Nederland proces niet gebruikt gaan worden.*

1. Op welke manier wordt geborgd dat tussentijds persoonsgegevens worden vernietigd in overeenstemming met het Documentair Structuur Plan (DSP)?

*Is verwijdering op individuele basis ook mogelijk als een gebruiker hierom vraagt?*

1. Indien de applicatie niet via Single Sign On beschikbaar komt: Voldoet de applicatie aan onze wachtwoord policy?

*De wachtwoord policy staat in het* [*IAM beleid van Security Nederland*](https://mborijnland.sharepoint.com/sites/StafdienstIM/Gedeelde%20documenten/Informatiebeveiliging%20%26%20Privacy/Autorisatie%20en%20authenticatiebeleid%20mboRijnland%20Definitief.pdf)*.*

1. Is de applicatie voorzien van Multifactor Authenticatie (MFA)?

*Wanneer in de applicatie gegevens zijn opgeslagen die zijn geclassificeerd op vertrouwelijk hoog (bijvoorbeeld BSN, beeldmateriaal, medische gegevens of functioneringsgegevens medewerker) of de applicatie wordt gebruikt voor gevoelige processen als examinering of financiën is MFA vereist.*

1. Hoe ziet het proces eruit voor het toevoegen en verwijderen van gebruikers uit de applicatie?
2. Op welke manier zijn autorisaties binnen de applicatie opgebouwd?

*Criterium moet zijn least privilege op basis van need-to-know en need-to-use, zie ook het* [*IAM beleid van Security Nederland*](https://mborijnland.sharepoint.com/sites/StafdienstIM/Gedeelde%20documenten/Informatiebeveiliging%20%26%20Privacy/Autorisatie%20en%20authenticatiebeleid%20mboRijnland%20Definitief.pdf)*.*

1. Wat wordt gelogd in de applicatie en hoe gaat deze logging worden gecontroleerd?

*Wanneer in de applicatie gegevens zijn opgeslagen die zijn geclassificeerd op vertrouwelijk hoog (bijvoorbeeld BSN, beeldmateriaal, medische gegevens of functioneringsgegevens medewerker) of de applicatie wordt gebruikt voor gevoelige processen als examinering of financiën is logging op inzage- of wijzigingsniveau vereist. Indien wordt gelogd binnen een applicatie zijn belangrijke vervolgvragen:*

* 1. *Wie kan de logging inzien?*
	2. *Hoe lang wordt de logging bewaard?*
1. Indien in de applicatie persoonsgegevens gaan worden opgeslagen moet er een verwerkersovereenkomst worden afgesloten. Is de leverancier partij bij het [Privacy Convenant](https://www.privacyconvenant.nl/de-deelnemers) of accepteert de leverancier de [model verwerkersovereenkomst van Security Nederland](https://mborijnland.sharepoint.com/sites/StafdienstIM/_layouts/15/Doc.aspx?sourcedoc=%7B17C889A4-7B29-419D-9585-56563E62CB03%7D&file=Verwerkersovereenkomst%20generieke%20model%20(alle%20andere%20leveranciers)%20v1.03.docx&action=default&mobileredirect=true&CT=1588065516084&OR=ItemsView)?
2. Beschikt de applicatie over het ISO 27001 beveiligingscertificaat dat is afgegeven door een officiële instantie, dan wel een gelijkwaardig certificaat?
3. Worden er door de leverancier pentesten uitgevoerd om de beveiliging van de applicatie te testen?
4. Is een Data Protection Impact Assessment (DPIA) vereist voor de nieuwe applicatie?

*Zie de* [*Handleiding uitvoeren Data Protection Impact Assessment (DPIA)*](https://mborijnland.sharepoint.com/%3Aw%3A/r/sites/StafdienstIM/_layouts/15/Doc.aspx?sourcedoc=%7B417E9C1E-B96E-4FB3-85BE-8844D124463A%7D&file=Handleiding%20uitvoeren%20Data%20Protection%20Impact%20Assessment%20(DPIA)%20Definitief.docx&action=default&mobileredirect=true) *voor in welke gevallen het uitvoeren van een DPIA is vereist.*

**Aandachtspunten vanuit architectuur & governance, User Experience, inkoop & beheer**

**Architectuur**

1. Wat is het doel van de applicatie, of wel: waarvoor gebruiken we het?
2. Is er een uitgewerkte domeinarchitectuur van toepassing? Zo ja, past de beoogde oplossing binnen de gestelde kaders? Zo nee, past de oplossing binnen de vastgestelde basisprincipes en heeft er een afweging met alternatieven plaats gevonden?
3. Moet er een PSA (Project Start Architectuur) worden uitgewerkt?
	1. Wat is de functie (of service) die de nieuwe applicatie gaat verzorgen?
	2. Is sprake van nieuwe of veranderde processen?
	3. Introduceert de nieuwe applicatie nieuwe gegevens (of nieuwe entiteiten of gegevens-soorten)? Zo ja: Is voor deze gegevens een eigenaar aangewezen? Is voor deze gegevens BIV-classificatie opgesteld? Dataconvenant? Bewaartermijnen?
	4. Is sprake van nieuwe functies of nieuwe techniek (anders dan de software?)
	5. Zijn wijzigingen op infrastructureel niveau voorzien?
	6. Op welke wijze worden kosten die gemoeid zijn met deze nieuwe applicatie verwerkt?
4. Is er reeds een oplossing beschikbaar binnen het bestaande/geplande applicatielandschap van Security Nederland?
5. Hoe is account provisioning geregeld? Is federatieve provisioning (SSO) via SURFconnext mogelijk?
6. Welke gegevensuitwisselingen zijn noodzakelijk? Hoe voorziet de oplossing daarin?
7. Vervangt de nieuwe applicatie een applicatie? Zo ja, wanneer en hoe wordt de oude applicatie opgeruimd en hoe worden gegevens geconverteerd, gearchiveerd of verwijderd?

**User Experience**

1. Is custom branding mogelijk voor Security Nederland?
2. (Op welke manier) is er bewust aandacht voor de user experience?
3. Zijn er vergelijkbare kanalen/oplossingen reeds in gebruik en is er beleid/bewust nagedacht over de samenhang hiermee?

**Governance, inkoop & beheer**

1. Wie is applicatie- en contracteigenaar?
2. Wie is functioneel beheerder?
3. Is de applicatie aangemeld bij ICT applicatiebeheer (via servicedesk)?
4. Moet de afdeling inkoop betrokken zijn? Is er sprake van een aanbestedingsplicht?
5. Dienen er huidige/oude contracten opgezegd te worden?

**Projectmanagement**

1. Is er een projectleider aangewezen?
2. Is er een projectplan aanwezig?
1. Bron: Lucas Onderwijs, Den Haag [↑](#footnote-ref-2)
2. Bron: MBOdigitaal en HAS green academy [↑](#footnote-ref-3)
3. Bron: mboRijnland [↑](#footnote-ref-4)