KERNBOODSCHAP

Project Start Architectuur (PSA) IAM vervanging

VISTA college

- Tijdige vervanging met behoud van noodzakelijke functies en toegang.
- Initiële oplevering en ingebruikname uiterlijk 17 december 2027.
- Aantoonbare uitbreidbaarheid voor beschreven ontwikkelingen.
- SaaS, beheer en ondersteuning gedurende de contractperiode.
- Kaders K01–K16 - bijlage architectuurkaders.



VISTA bepaalt scope en acceptatie. De leverancier toont de werking aan.

richting | borging | toekomstvast

Aanleiding en continuïteit

Noodzakelijke toegang voor onderwijs en bedrijfsvoering

- De ondersteuning van de huidige IAM-voorziening eindigt. Tijdige vervanging is noodzakelijk.
- De nieuwe dienst is uiterlijk 17 december 2027 geaccepteerd en operationeel.
- AS-IS betekent behoud van noodzakelijke functies en toegang. De technische inrichting kan veranderen.
- VISTA bepaalt per functie wat behouden, vervangen, overgedragen of beëindigd wordt.
- De leverancier beproeft migratie, terugval en overdracht. VISTA beoordeelt en accepteert.

De vervanging behoudt de noodzakelijke resultaten voor VISTA.



continuïteit | risico | tijdig

Eigenaarschap en samenwerking

Verantwoordelijkheden vóór iedere ingebruikname

- De afdelingsmanager IV&T borgt de rolverdeling met ICT FB en ICT TB.
- Per use-case en relevante variant liggen proces-, systeem- en data-eigenaren aantoonbaar vast vóór ingebruikname.
- De teamleider ICT TB is systeemeigenaar IAM. IM en de architect bewaken beleid en samenhang.
- De leverancier leidt de uitvoering en levert de afgesproken SaaS-dienst en ondersteuning.
- De VISTA-projectleider organiseert interne inzet, beoordeling en acceptatie.
- VISTA besluit binnen bestaande mandaten over scope, risico's en afwijkingen.



Bestaande benoemingen vormen de basis. Ontbrekende rollen vragen een besluit.

business | keten | regie

Samenhang en taakverdeling

- IAM/IGA beheert identiteiten, accounts en rechten en ondersteunt controles op toegang.
- De aangewezen bron bepaalt de gegevens. Eigenaren bepalen de toegangsregels.
- Het ontwerp verdeelt taken tussen IAM/IGA, bronnen en aangesloten systemen.
- Per koppeling zijn gegevens, beveiliging, foutafhandeling en verantwoordelijke bekend.
- Open standaarden, documentatie en ketentests maken de werking aantoonbaar.

Functie	Verantwoordelijkheid
Bronnen	Geldige relaties en betrouwbare brongegevens
IGA en IAM	Identiteiten, accounts en rechten beheren
Inloggen en federatie	Identiteit controleren en vertrouwen afspreken
Aangesloten systemen	Toegestane handelingen uitvoeren en begrenzen
Beheer en regie	Werking bewaken, fouten herstellen en verantwoorden

Het architectuurkader beschrijft functies. De leverancier werkt het ontwerp uit.

IAM | IGA | integratie | data

Instroom, wijziging en vertrek

Toegang volgt een geldige relatie met VISTA

- VISTA bevestigt gebruikersgroepen en bronnen, zoals EduArte, Magister en AFAS.
- Rollen en kenmerken bepalen de rechten. Wijzigingen en vertrek werken door in alle betrokken systemen.
- De leverancier toont verwerking en intrekking aan in elk aangesloten systeem.
- Use cases en relevante varianten verbinden scope, eigenaren en ketentests.

Een verwerkte bronwijziging moet tot het juiste toegangsresultaat leiden.



instroom | wijziging | vertrek

Uitbreidbaarheid en sectoraansluiting

Voorzienbare ontwikkelingen vragen aantoonbare mogelijkheden

- De leverancier toont bij oplevering de vereiste uitbreidbaarheid voor beschreven scenario's aan.
- Een actuele, met VISTA afgestemde roadmap benoemt mogelijkheden, afhankelijkheden en kosten.
- Kunnen anticiperen op: eduID, SURF Access, Aanmelden Inschrijven en Intekenen (AII) en ontwikkelingen rond LLO.
- Nieuwe aansluitingen volgen na besluitvorming, realisatie, testen en acceptatie.

Sectorplanning geeft richting. VISTA besluit over concrete invoering.



MORA | MOSA | eduID | SURF

Beveiliging, privacy en AI

Passende bescherming vanaf de eerste ingebruikname

- Minimale rechten, passende MFA en periodieke rechtencontrole beschermen de toegang.
- Privacy- en beveiligingsmaatregelen gelden voor de hele keten. VISTA beoordeelt de noodzaak van een DPIA.
- Bestaande technische accounts hebben een eigenaar, doel en begrensde, controleerbare rechten.
- Nieuwe AI-agenttoegang vraagt een afzonderlijk besluit over taken, rechten en menselijke verantwoordelijkheid.
- VISTA legt de vereiste bescherming van beheerrechten en de PAM-omvang eenduidig vast in het PvE.



Bestaande toegang blijft beschermd. Nieuwe AI-toepassingen vragen een besluit.

DPIA | Zero Trust | AI

Dienstverlening en ketenregie

Afspraken gelden vanaf iedere ingebruikname

- SaaS, beheer en ondersteuning starten per ingebruikgenomen onderdeel.
- IV&T borgt met ICT FB en ICT TB ketencoördinatie, mandaten, vervanging en escalatie.
- Afspraken dekken lesweken, vakanties, avond- en weekendtijden en sluitingsweken.
- Advantive dekt vooral Microsoft. VISTA bevestigt de ketenafspraken voor overige SaaS-diensten.
- SLA en DAP onderscheiden beschikbaarheid, ondersteuning en calamiteitenafhandeling.
- Exit afspraken borgen overdraagbare gegevens, instellingen en regels, met termijnen en kosten.

Vóór ingebruikname zijn ketenafspraken vastgesteld en beproefd.



SLA/DAP | KPI | exit

Zeven KPI-onderwerpen

VISTA bepaalt resultaten en normen. De leverancier onderbouwt de meting.

- 1 Beschikbare en herstelbare SaaS dienstverlening en ondersteuning
- 2 Correcte en tijdige verwerking: bronwijzigingen
- 3 Blijvend passende en veilige toegang: bestaande rechten
- 4 Beheerste wijziging en ontwikkeling
- 5 Effectieve regie en verbetering, één loket functie is ingericht (PDCA)
- 6 Overdraagbare dienstverlening
- 7 Voorspelbare en transparante kosten

Per KPI: norm, meetwijze, verantwoordelijke, bewijs en opvolging.



meten | sturen | verbeteren

Toetsing en besluitvorming

Kaders, eisen en bewijs blijven aan elkaar gekoppeld

- VISTA toetst vóór publicatie, bij ontwerp en realisatie, vóór ingebruikname en bij overdracht.
- De leverancier levert bewijs. Eigenaren en deskundigen beoordelen hun deel, de architect de samenhang.
- Tijdens beheer volgt ten minste jaarlijks een architectuurtoets en bij belangrijke veranderingen of incidenten.
- De SaaS-dienst krijgt daarnaast minimaal jaarlijks een interne of externe audit.
- VISTA belegt besluiten over afwijkingen en risico’s bij de bevoegde rollen.

Elke bevinding heeft een eigenaar, vervolgactie en termijn.



besluiten | eigenaren | scope

Oplevering, uitbreidbaarheid en dienstverlening

Onderdeel	Wat hoort erbij?	Moment en besluit
Oplevering en dienst (project opdracht)	Noodzakelijke functies en toegang, migratie en acceptatie. SaaS, beheer en ondersteuning met duidelijke rolverdeling.	Uiterlijk 17 december 2027 operationeel. Dienstverlening vanaf ingebruikname gedurende het contract.
Uitbreidbaarheid	Bij oplevering aantonen hoe beschreven ontwikkelingen mogelijk zijn zonder fundamentele herbouw van de kern.	Actuele roadmap met afhankelijkheden en kosten. VISTA besluit afzonderlijk over concrete uitbreidingen.
Continue verbetering	Onderhoud en beheerste verandering, met balans tussen dagelijkse dienstverlening (RUN) en verandering (CHANGE).	Gedurende het contract. VISTA en leverancier wegen prioriteiten, capaciteit, continuïteit en kosten.

Concrete uitbreidingen worden na besluitvorming, testen en acceptatie onderdeel van de dienst.

K01–K08 Identiteit, toegang en koppelingen

Samenvatting en voorgestelde borging.

Kader	Kern van de afspraak	Uitwerking en bewijs
K01	Houd persoon, relaties, accounts en rechten herkenbaar. Behoud toegang uit andere geldige relaties.	PvE en use-cases Ontwerp en ketentest
K02	Verwerk instroom, wijzigingen en vertrek aantoonbaar tot in de aangesloten systemen.	PvE, use-cases, SLA en DAP Verwerkings- en intrekkingsbewijs
K03	Wijs per gegeven een leidende bron aan. Houd kwaliteit en afleiding van rechten uitlegbaar.	PvE en ontwerp Bronafspraken en gegevenstoets
K04	Beperk rechten, pas passende MFA toe en controleer bestaande rechten en beheerrechten.	PvE en beveiligingsafspraken Rechtencontrole en beveiligingstest
K05	Gebruik passende federatieve toegang. VISTA bepaalt de geldige relatie en toegangsrechten.	PvE en aansluitontwerp Vertrouwensafspraken en ketentest
K06	Gebruik open, gedocumenteerde koppelingen met beveiliging, foutafhandeling en versieafspraken.	PvE en koppeldocumentatie Interface- en foutafhandelingstest
K07	Verdeel integratietaken tussen IAM, bronnen en andere voorzieningen. Benoem de verantwoordelijke.	Scope, ontwerp, SLA en DAP Takenverdeling en ketentest
K08	Maak gegevens, instellingen, regels en documentatie bruikbaar overdraagbaar, met afgesproken exitkosten.	PvE, exitafspraken en prijzenblad Export- en overdrachtsproef

K09–K16 Bescherming, continuïteit en regie

Samenvatting en voorgestelde borging.

Kader	Kern van de afspraak	Uitwerking en bewijs
K09	Beoordeel en bescherm privacy en beveiliging in de hele keten, met noodzakelijke gegevens en maatregelen.	PvE en privacyafspraken Risicobeoordeling en zo nodig DPIA
K10	Maak handelingen en besluiten herleidbaar. Leg per logsoort doel, inzage en bewaartermijn vast.	PvE en logafspraken Loggingtest en controlebewijs
K11	Beproef migratie, terugval en herstel. Leg hersteldoelen per kritieke dienst vast volgens beleid.	PvE, SLA en continuïteitsplan Migratie- en herstelproef
K12	Geef technische identiteiten een verantwoordelijke persoon, een doel en beperkte, controleerbare rechten.	PvE en register technische accounts en periodieke controle
K13	Leg per use-case en variant alle proces-, systeem- en data-eigenaren vast vóór ingebruikname.	VISTA-register en rolafspraken Bevestiging door bevoegd management
K14	Leg prestaties, ondersteuning en ketensamenwerking vast, inclusief mandaten en bereikbaarheid per tijdvenster.	SLA, DAP en prijzenblad Rapportage en calamiteitenbeheersing
K15	Toon beschreven uitbreidbaarheid aan. Organiseer onderhoud en beheerste verandering gedurende het contract.	PvE, roadmap, prijzenblad scenario’s en acceptatie criteria
K16	Houd documentatie en bewijs actueel. Organiseer toetsing en minimaal jaarlijks een audit van de SaaS-dienst.	PvE, SLA en DAP Documentatie, toets- en auditrapport