



**van hall
larenstein**
university of applied sciences

IDENTITEIT & TOEGANG

Visie





Colofon

Auteur(s)

Richard Cuperus

E-mail

Richard.cuperus@hvhl.nl

Versienummer

0.1 concept

Uitgavedatum

31 maart 2025

Over HVHL

Hogeschool Van Hall Larenstein (HVHL) is een internationale groene kennisinstelling, waar we met passie en kunde onderwijs verzorgen, ondersteund door toegepast onderzoek binnen diverse lectoraten. We leiden proactieve professionals op, die op een verantwoorde en ondernemende wijze een positieve bijdrage leveren aan een duurzame samenleving.

Sommige rechten voorbehouden

Hoewel aan de totstandkoming van dit document de uiterste zorg is besteed, aanvaarden auteur(s) geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.



ESSENTIE VAN DE VISIE

Binnen HVHL is digitale toegang geen technisch vraagstuk, maar een afgeleide van bevoegdheden binnen processen. Deze bevoegdheden worden vastgelegd in rollen, die bepalen welke handelingen een procesdeelnemer mag uitvoeren.

Digitale toegang wordt bepaald door de combinatie van rol en context en wordt op basis daarvan automatisch en consistent gerealiseerd. De grondslag voor roltoekenning ligt in verbintenis of mandaat, waardoor digitale toegang herleidbaar is en meebeweegt met veranderingen binnen HVHL.

HVHL voert regie op bevoegdheden en roltoekenning, terwijl de technische realisatie van digitale toegang wordt ondersteund door centrale voorzieningen. Hiermee wordt digitale toegang een integraal onderdeel van de sturing op processen en samenwerking.



Inhoud

INLEIDING

1	VISIE OP IDENTITEIT EN TOEGANG	7
1.1	Digitale toegang als afgeleide van bevoegdheden	7
1.2	Nieuwe identiteit- en toegangsvoorziening als sturingsinstrument	7
1.3	Digitale toegang gebaseerd op rol en context.....	8
2	GRONDSLAGEN VOOR TOEGANG	9
2.1	Identiteit en instellingsidentiteit	9
2.2	Verbintenis als basis voor structurele toegang	9
2.3	Mandaat als basis voor aanvullende toegang	9
3	GOVERNANCE OP TOEGANG	11
3.1	Verantwoordelijkheid in de organisatie	11
3.2	Scheiding tussen besluitvorming en realisatie	11
3.3	Selfservice als onderdeel van mandatering.....	11
4	AUTHENTICATIE EN EXTERNE SAMENWERKING.....	12
5	SOEVEREINITEIT, REGIE EN ONTWIKKELING.....	13

INLEIDING

Het onderwijs en onderzoek van Hogeschool Van Hall Larenstein (HVHL) is in toenemende mate afhankelijk van betrouwbare en aantoonbaar juiste digitale toegang¹ tot applicaties², gegevensbronnen³ en onderliggende systemen (digitale voorzieningen). Deze ondersteunen medewerkers, studenten, partners en leveranciers van HVHL (procesdeelnemers) dagelijks in hun deelname aan onderwijs-, onderzoeks- en bedrijfsvoeringsprocessen (processen). In de praktijk wordt de mogelijkheid om hieraan deel te kunnen nemen bepaald door toegang tot digitale voorzieningen (digitale toegang).

Digitale toegang heeft hiermee een directe relatie tot de bevoegdheid om deel te nemen aan processen. Het verlenen van digitale toegang betekent dat een procesdeelnemer handelingen kan uitvoeren die mogelijk gevolgen heeft voor lerenden, medewerkers, partners, leveranciers en HVHL als geheel. Het beheer van digitale toegang is dan niet meer uitsluitend een technisch vraagstuk, maar vooral organisatorisch en bestuurlijk. De huidige voorziening voor het beheren van identiteiten en toegang (Identiteit- en toegangsvoorziening) bij HVHL⁴ is primair technisch van aard en biedt daardoor onvoldoende ondersteuning voor het sturen op bevoegdheden en digitale toegang als een organisatorisch en bestuurlijk vraagstuk.

Met de ministeriële aanwijzing dat het hoger onderwijs onder de NIS gaat vallen⁵ en de mogelijke overgang van de sector Hoger Onderwijs naar ISO/IEC 27001:2022 worden strengere eisen gesteld aan informatiebeveiliging en digitale weerbaarheid. De huidige IAM-oplossing sluit niet aan bij de eisen die hieruit voortvloeien.

Als laatste is de huidige IAM-oplossing end-of-life⁶ en moet vervangen worden. Dit biedt mogelijkheden om toe te werken naar een toekomstvaste inrichting die aansluit bij de veranderende organisatorische omstandigheden, technologische ontwikkelingen en HVHL's toenemende afhankelijk van betrouwbare en aantoonbaar juiste digitale toegang.

Uitgangspunt voor deze visie is een breed gedragen beeld van hoe digitale toegang tot stand komt en wordt beheerd. Deze visie beschrijft hoe HVHL organisatorische verantwoordelijkheden en bevoegdheden vertaalt naar digitale toegang.

¹ Digitale toegang is de feitelijke mogelijkheid om een digitale voorziening te gebruiken en is het resultaat van authenticatie en autorisatie van een account.

² Een applicatie is een logisch afgebakende verzameling functionaliteit die processen en gebruikers ondersteunt, terwijl een systeem het geheel vormt van technologie, verwerking en ontsluiting waarin deze applicatie wordt uitgevoerd en beschikbaar gesteld.

³ Een gegevensbron is een logisch afgebakende verzameling gegevens, terwijl een systeem het geheel vormt van technologie, verwerking en ontsluiting waarin deze gegevensbron wordt beheerd en beschikbaar gesteld.

⁴ Deze is onder andere gerealiseerd met UMRA van Tools4Ever (Identity & Access Management (IAM)-oplossing) en inQdo Connect van inQdo (Enterprise Service Bus (ESB)).

⁵ [Kamerbrief over voortgang cyberveerbaarheid in het vervolgonderwijs](#)

⁶ De datum voor end of support van de IAM-oplossing is vastgesteld op 31-12-2026 en de datum voor extended support eindigt naar verwachting op 31-12-2028.



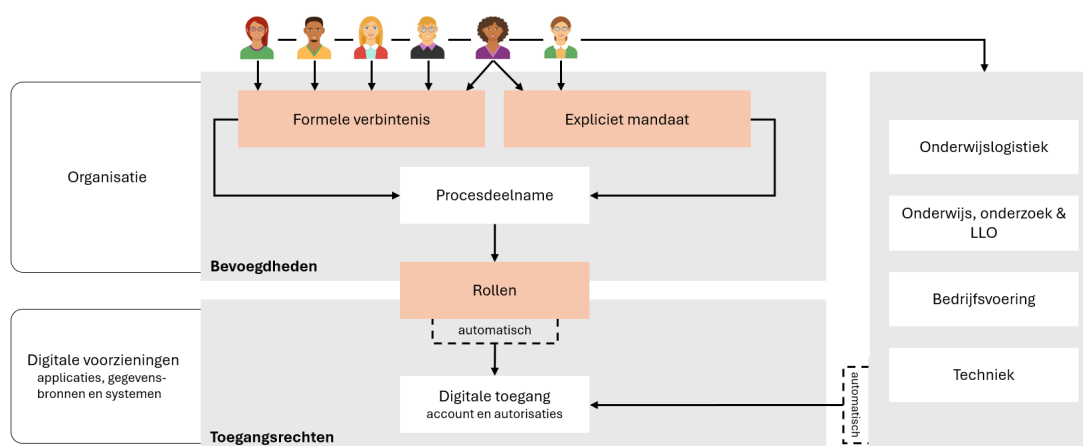
De visie sluit aan op de IVT-strategie 2026–2029 en concretiseert de daarin benoemde activiteiten op het gebied van gewaarborgde veiligheid en continuïteit en kostenoptimalisatie.

1 VISIE OP IDENTITEIT EN TOEGANG

1.1 Digitale toegang als afgeleide van bevoegdheden

Deelname van lerenden, medewerkers, partners en leveranciers van HVHL aan processen (procesdeelname) is gebaseerd op een formele verbintenis of een expliciet mandaat en bestaat uit het vervullen van één of meerdere rollen. Rollen vormen de logische representatie van de bevoegdheden die iets of iemand heeft binnen een proces en beschrijven welke handelingen zijn toegestaan.

Rollen worden toegekend aan procesdeelnemers als uitwerking van deze bevoegdheden. De aan een rol gekoppelde toegangsrechten vormen de technische implementatie hiervan en leiden automatisch tot digitale toegang in digitale voorzieningen in de vorm van een account met autorisatie.



Figuur 1 Rollen als verbinding tussen bevoegdheden en toegangsrechten

Toegangsrechten zijn daarmee geen zelfstandig doel, maar een afgeleide van bevoegdheden die binnen de organisatie zijn vastgesteld. Zonder vastgestelde bevoegdheid worden geen toegangsrechten verleend.

1.2 Nieuwe Identiteit- en toegangsvoorziening als sturingsinstrument

Met een nieuwe Identiteit- en toegangsvoorziening worden bevoegdheden van procesdeelnemers vertaald naar rollen en worden de bijbehorende toegangsrechten consistent en controleerbaar gerealiseerd in digitale voorzieningen en wordt gestuurd op:

- het faciliteren van procesdeelname;
- het borgen van functiescheiding;
- transparante en herleidbare besluitvorming.

De Identiteit- en toegangsvoorziening wordt op deze manier gepositioneerd als een instellingsbrede voorziening voor het sturen op bevoegdheden en de daaruit afgeleide digitale toegang. Dit betekent dat het toekennen van rollen - en daarmee de bijbehorende digitale



toegang - niet uitsluitend bij de afdeling IVT ligt, maar plaatsvindt binnen de verantwoordelijkheid van proceseigenaren.

Het toekennen van rollen vindt plaats binnen de context van de daadwerkelijke taken en verantwoordelijkheden van een procesdeelnemer (procesverantwoordelijkheid) en is daarmee belegd in de instelling. De technische implementatie van toegangsrechten volgt hieruit en wordt centraal en uniform uitgevoerd.

1.3 Digitale toegang gebaseerd op rol en context

Digitale toegang wordt bepaald door een combinatie van rol en context. Rollen representeren de bevoegdheden van een procesdeelnemer en bepalen welke handelingen zijn toegestaan. De context bepaalt waar deze handelingen van toepassing zijn, bijvoorbeeld binnen een opleiding, onderzoeksproject, afdeling of technisch platform.

Met deze scheiding worden bevoegdheden centraal en uniform vastgelegd, terwijl de toepassing daarvan flexibel en meer granulair aansluit bij de specifieke situatie waarin deze nodig is. De bijbehorende toegangsrechten worden op basis hiervan technisch geïmplementeerd in digitale voorzieningen.

HVHL ontwikkelt zich hiermee naar een instelling waarin toegang niet langer uniform wordt toegekend, maar aansluit bij de procesverantwoordelijkheid van een procesdeelnemer. Dit maakt het mogelijk om digitale toegang doelgericht en gedifferentieerd in te richten, passend bij contexten zoals onderwijs, onderzoek en Leven Lang Ontwikkelen (LLO), en om gebruik en bijbehorende kosten beter met elkaar in balans te brengen.

2 GRONDSLAGEN VOOR TOEGANG

2.1 Identiteit en instellingsidentiteit

HVHL onderscheidt de identiteit⁷ van een persoon van de instellingsidentiteit die door HVHL wordt beheerd.

De instellingsidentiteit⁸ vormt de centrale representatie van een persoon binnen de instelling en is de basis voor het toekennen van rollen en daarmee voor de realisatie van digitale toegang.

Een persoon kan meerdere rollen vervullen, maar wordt altijd eenduidig vastgelegd in één instellingsidentiteit. Deze instellingsidentiteit wordt instellingsbreed gebruikt en vormt de enige basis voor het realiseren van digitale toegang.

2.2 Verbintenis als basis voor structurele toegang

Digitale toegang wordt verleend aan personen die op basis van een formele juridische verbintenis procesdeelnemer zijn. Voorbeelden hiervan zijn:

- een arbeidsovereenkomst;
- een opleidingsinschrijving;
- een cursusovereenkomst;
- een detacheringsovereenkomst;
- deelname aan onderzoek;
- een leveranciersovereenkomst;
- een samenwerkingsverband.

Verbintenissen vormen de structurele grondslag voor procesdeelname. Op basis hiervan worden rollen automatisch toegekend (verbintenis-gedreven roltoekenning) die nodig zijn om binnen de organisatie te functioneren. De bij deze rollen behorende toegangsrechten worden vervolgens automatisch gerealiseerd.

Wanneer de onderliggende verbintenis wijzigt of vervalt, worden de bijbehorende rollen en toegangsrechten automatisch aangepast of ingetrokken.

2.3 Mandaat als basis voor aanvullende toegang

Naast structurele digitale toegang op basis van verbintenis kunnen aanvullende rollen worden toegekend op basis van mandaat. Dit betreft situaties waarin procesdeelname niet direct

⁷ Een eenduidige, digitale representatie van een natuurlijk persoon, gebaseerd op een minimale en samenhangende set van identificerende en beschrijvende kenmerken, waarmee die persoon herkend en onderscheiden kan worden van anderen.

⁸ Een eenduidige, digitale representatie van een natuurlijk persoon binnen HVHL, gebaseerd op de verbintenis met HVHL en de daarbij horende kenmerken.



voortvloeit uit een formele juridische verbintenis, maar expliciet wordt toegekend door een hiertoe bevoegde persoon⁹.

Mandaat-gedreven roltoekenning is in de regel tijdelijk of contextspecifiek en wordt expliciet vastgelegd. De toegangsrechten die hieruit voortvloeien worden automatisch gerealiseerd en zijn herleidbaar tot het onderliggende besluit.

⁹ In de regel is dit een proceseigenaar of rolbeheerder.

3 GOVERNANCE OP TOEGANG

3.1 Verantwoordelijkheid in de organisatie

Binnen HVHL wordt onderscheid gemaakt tussen proceseigenaar en rolbeheerder. Een proceseigenaar is eindverantwoordelijk voor het proces en de bijbehorende bevoegdheden. Een rolbeheerder is, namens de proceseigenaar, verantwoordelijk voor de definitie en het beheer van rollen binnen een proces. Het toekennen van rollen is daarmee belegd in de instelling en gekoppeld aan deze eigenaarschappen.

Deze inrichting borgt dat bevoegdheden eenduidig worden vastgesteld en dat rollen consistent en controleerbaar worden toegepast, terwijl expliciet ruimte wordt geboden voor varianten in de procesuitvoering, bijvoorbeeld per locatie, opleiding of organisatorische eenheid.

3.2 Scheiding tussen besluitvorming en realisatie

Binnen HVHL worden het vaststellen van bevoegdheden en de technische implementatie van digitale toegang duidelijk van elkaar gescheiden.

Een Identity Governance & -Administration (IGA)-oplossing ondersteunt besluitvorming over roltoekenning en legt deze vast. Een IAM-oplossing realiseert daarna op basis van de besluitvorming de bijbehorende toegangsrechten in digitale voorzieningen.

Hiermee is digitale toegang altijd een gevolg van een expliciet vastgelegde roltoekenning en dat de uitvoering hiervan uniform en controleerbaar plaatsvindt.

3.3 Selfservice als onderdeel van mandatering

Aanvragen voor aanvullende rollen verlopen op gestandaardiseerde wijze, waarbij goedkeuring plaatsvindt door bevoegde personen. Deze werkwijze ondersteunt het toekennen van mandaat-gedreven rollen en borgt dat aanvullende bevoegdheden en de daaruit voortvloeiende digitale toegang altijd gebaseerd is op expliciete besluitvorming en herleidbaar is.



4 AUTHENTICATIE EN EXTERNE SAMENWERKING

HVHL hanteert een model voor authenticatie waarbij instellingsidentiteiten centraal worden beheerd en authenticatie plaatsvindt via daarvoor geschikte digitale voorzieningen.

Externe procesdeelnemers¹⁰ kunnen gebruik maken van federatieve identiteiten, zoals eduID¹¹ en eduGAIN¹². Deze identiteiten worden gebruikt voor authenticatie, maar vormen pas een instellingsidentiteit wanneer zij zijn gekoppeld aan een verbintenis of mandaat binnen HVHL.

Hiermee wordt geborgd dat externe voorzieningen authenticatie faciliteren, maar niet bepalend zijn voor bevoegdheden en de daaruit afgeleide digitale toegang binnen HVHL.

HVHL beweegt zich richting een situatie waarin gebruik van eigen apparaten (BYOD) het uitgangspunt is. In deze context kan digitale toegang niet langer worden gebaseerd op bekende of beheerde apparaten. Dit vraagt om een inrichting onafhankelijk van het gebruikte apparaat en aansluit op principes van zero trust¹³.

¹⁰ Voorbeelden hiervan zijn gastdocenten voor LLO en surveillanten.

¹¹ <https://eduid.nl/home>

¹² <https://edugain.org/>

¹³ Zero trust betekent dat digitale toegang altijd expliciet wordt geverifieerd op basis van identiteit, rol en context, ongeacht netwerk, apparaat of locatie.

5 SOEVEREINITEIT, REGIE EN ONTWIKKELING

HVHL maakt momenteel, naast een on-premises IAM-oplossing, in beperkte mate gebruik van cloudgebaseerde oplossingen voor identiteit en toegang. Er is echter een beweging zichtbaar waarbij HVHL in toenemende mate gebruik maakt van cloudoplossingen waarbij de afdeling IVT (IVT) opereert als regieorganisatie. In deze context worden digitale voorzieningen primair geleverd door leveranciers en richt IVT zich op het stellen van kaders, het organiseren van samenhang en het borgen van regie.

Naar verwachting zal ook de Identiteit- en toegangsvoorziening zich volledig ontwikkelen richting cloud. Deze ondersteunen dan de technische implementatie van digitale toegang, maar de regie op bevoegdheden en roltoekenning blijft binnen HVHL belegd.

Cloudoplossingen voor identiteit en toegang maken het mogelijk om digitale toegang schaalbaar, uniform en gecentraliseerd te realiseren. Daarnaast sluiten deze aan op de toenemende inzet van cloudoplossingen binnen HVHL.

Cloudoplossingen brengen afhankelijkheden van leveranciers met zich mee en vragen om een andere invulling van regie door IVT. HVHL geeft hieraan invulling door:

- verantwoordelijk te blijven voor de grondslagen van digitale toegang;
- kaders te stellen voor inrichting en gebruik van de Identiteit- en toegangsvoorziening;
- gerichte keuzes te maken in inrichting en configuratie van voorzieningen.

HVHL ontwikkelt zich hiermee naar een instelling waarin digitale toegang eenduidig, herleidbaar en afgestemd op rol en context is georganiseerd. Bevoegdheden zijn expliciet vastgelegd en vertaald naar rollen, die consistent en automatisch worden gerealiseerd in digitale voorzieningen. Toegang verandert mee met de organisatie en vormt daarmee een integraal onderdeel van de sturing op processen en samenwerking.