VISIE OP IDENTIFICATIE, AUTHENTICATIE EN AUTORISATIE (IAA)

VOOR DE SURFNET-DOELGROEP VAN ONDERWIJS EN ONDERZOEK

ACHTERGROND

SURFnet biedt met haar dienstverlening al jaren een stabiele en betrouwbare basis voor samenwerking binnen onderwijs en onderzoek. Voor het bepalen van de koers en samenloop van innovatie en ontwikkelingen van Identificatie, Authenticatie en Autorisatie (IAA)-gerelateerde, afspraken en dienstverlening (het IAA-stelsel) wordt de visie op dit werkveld met regelmaat herijkt, bijvoorbeeld op basis van ontwikkelingen in de maatschappij, het onderwijs en/of veranderende wet- en regelgeving. Het betreft een ketenvraagstuk dat organisaties overstijgt en waar regie op gevoerd moet worden. Vertrouwen in ons IAA-stelsel en de richting waarin dit zich ontwikkelt is cruciaal voor het effectief gebruik door alle betrokken partijen: instellingen van onderwijs en onderzoek, leveranciers en individuele gebruikers.

SURF NET

DE SURFNET VISIE OP IAA

Ons IAA-ecosysteem creëert op transparante wijze vertrouwen tussen gebruikers, instellingen en (commerciële) dienstaanbieders. De privacy en zelfbeschikking van de gebruiker zijn hierbij een essentiële voorwaarde.

De infrastructuur biedt vertrouwde en betrouwbare single sign-on-toegang tot zowel webbased als non-webbased diensten. Daarnaast faciliteert het voor de doelgroep van onderwijs en onderzoek relevante samenwerking die zich uitstrekt over landsgrenzen en sectoren. Gezien de steeds sterkere behoefte tot online samenwerken en uitwisselen van gegevens, werken we aan het ondersteunen van uniek identificerende identiteiten over instellingsgrenzen heen.

Om het juiste beveiligings- en vertrouwensniveau te bieden worden verschillende Level of Assurance (LoA's) ondersteund, waarbij we een multi-middelen strategie hanteren om leveranciersonafhankelijk te borgen. Op termijn voorzien we dat identiteiten binnen het stelsel ook door andere partijen geleverd kunnen worden. Instellingen en andere partijen gerelateerd aan onderwijs en onderzoek zullen relevant blijven voor het leveren van de onderwijs- en/of onderzoekscontext die noodzakelijk is voor bijvoorbeeld van deze context afhankelijke autorisatie of personalisatie.

Gezien de positie van ons IAA-ecosysteem in de keten zorgen we, ook bij het doorvoeren van veranderingen, voor betrouwbare dienstverlening van hoge kwaliteit. We maken slim gebruik van bestaande voorzieningen, implementaties en standaarden. Waar deze nog niet voorhanden zijn of voldoen dragen we zelf bij aan de ontwikkeling.

ONTWIKKELINGEN

Het maatschappelijk bewustzijn van de risico's van de uitwisseling en opslag van persoonsgerelateerde data neemt toe. Dat leidt onder andere tot strengere wetgeving wat betreft gebruik van persoonsgegevens. De ambitie van SURFnet is niet alleen om een stelsel te bieden dat voorloopt in de implementatie van op handen zijnde wetgeving, maar waar mogelijk ook verdere waarborgen biedt voor de privacy van gebruikers. Bovendien ambieert SURFnet een stelsel dat mee kan groeien met de laatste maatschappelijke en technologische inzichten en ontwikkelingen.

De omgeving van het identitymanagement-werkveld in Nederland en Europa is voortdurend in ontwikkeling. We zien dat aan de ontwikkeling van de Nederlandse identiteitsstelsels, zoals Idensys en iDIN. Ook zijn er voorgenomen aanpassingen in de nationale wetgeving voor uniek identificerende nummers voor het onderwijs. Dit betekent dat er enerzijds meer duidelijkheid komt over implementatie en mogelijkheden, anderzijds ontstaan daardoor juist vragen over bijvoorbeeld privacybescherming, betaalbaarheid, verrekening en inpassing van deze stelsels binnen het domein van onderwijs en onderzoek. Ook zien we dat innovatieve concepten, zoals polymorfe pseudoniemen, beproefd worden. De impact van deze concepten op de architectuur en dienstverlening is nog niet duidelijk. Ten slotte zijn ontwikkelingen vanuit Europa in beweging. Denk daarbij aan de eIDAS-verordening, de vernieuwing van EU-privacyverordening of de internationale samenwerking via eduGAIN. Bovendien zitten ook internationale commerciële spelers als Microsoft, Google en Facebook niet stil.

De ontwikkeling naar een situatie waarbij de gebruiker meer centraal staat en zijn eigen online identiteit meebrengt, maakt het mogelijk mobiliteit van studenten en onderzoekers beter te faciliteren. Zeker wanneer die identiteit verrijkt kan worden met attributen die voor onderwijs en onderzoek relevant zijn. Dat terwijl accounts nu vaak alleen geldig zijn voor de eigen instelling die bovendien bepaalt wat wel en niet mag en de eigen inbreng daardoor summier is. Een online identiteit waar de gebruiker zelf meer de regie over voert, verschaft gebruikers een zekere mate van vrijheid en draagt bij aan meer flexibiliteit in onderwijs en onderzoek. Deze ontwikkeling brengt wel vraagstukken rondom toegang en privacy met zich mee.

Het privacyvraagstuk is breder dan IAA: lang niet alle privacygevoelige informatie die verwerkt, uitgewisseld of opgeslagen wordt komt voort uit de IAA-infrastructuur. Data die verzameld wordt door een cloud-dienst tijdens gebruik, of data die tussen partijen wordt gedeeld, anders dan via attributen uitgewisseld tijdens authenticatie of autorisatie, valt buiten een nauwe definitie van IAA. Het ligt zodoende voor de hand ook heldere afspraken te maken over omgang met andere dan IAA-data. Wat betekent bijvoorbeeld een login met SURFconext, via de Identitiy Provider van een instelling? Is dit een goedkeuring van de instelling voor het gebruik van de dienst? Het is belangrijk dat de verwachting van gebruikers overeenkomt met wat hier daadwerkelijk geboden wordt, anders wordt het vertrouwen van de gebruiker geschaad.

RELATIE MET SURFNET MISSIE, VISIE, STRATEGIE

SURFnet zorgt ervoor dat studenten, docenten, onderzoekers en medewerkers eenvoudig, betrouwbaar en grenzeloos kunnen werken en samenwerken met de best mogelijke ICT-voorzieningen. In onze visie versterken excellente ICT-voorzieningen het werken en samenwerken aan toponderzoek en in het onderwijs. Daarnaast verrijkt ICT de interactie binnen het hoger onderwijs en onderzoek en het middelbaar beroepsonderwijs en stimuleert het communicatie over de grenzen van sectoren, tijd en locatie heen. Wij geloven in een wereld waarin deze ICT-voorzieningen voor iedere onderzoeker, docent, medewerker en student eenvoudig toegankelijk zijn. SURFnet werkt hiermee aan de verbonden en veilige wereld waarin koppeling van en toegang tot alles en iedereen eenvoudig en betrouwbaar is geregeld.

SURFNET RICHT ZICH OP ACTIVITEITEN EN DIENSTEN DIE VERNIEUWEND, WAARDEVOL EN WAARDENRIJK ZIJN:

- **Vernieuwend:** SURFnet richt zich op diensten met een continue innovatie-cyclus en serieuze vernieuwingsslag (functionaliteitsstap) in iedere investerings-cyclus, waarbij SURFnet zich functioneel onderscheidt van de markt, en die aanjaagt.

- **Waardevol:** SURFnet activiteiten hebben impact op de doelgroep. SURFnet is voor de doelgroep een motor voor innovatie door het wegnemen van barrières en grenzen, door het experimenteren met nieuwe mogelijk-heden en door het delen van kennis over instellingsgrenzen heen. En SURFnet ontzorgt de doelgroep door het leveren van hoog-waardige diensten en kennis.

- **Waardenrijk:** SURFnet bewaakt en borgt de waarden en randvoorwaarden op het gebied van toegankelijkheid (grenzeloos) en veilig-heid (betrouwbaar / vertrouwd).

TEN AANZIEN VAN ‘EEN VEILIGE WERELD WAARIN ALLES EN IEDEREEN VEILIG EN EENVOUDIG GEKOPPELD IS’ SPELEN DE UITGANGS-PUNTEN UIT DE SURF POSITION PAPER “EEN OPEN, TOEGANKELIJK EN BETROUWBAAR INTERNET” VOOR IAA EEN BELANGRIJKE ROL:

- *Werk continu aan een veilig en betrouwbaar Internet waar de privacy van de gebruiker gerespecteerd wordt:*
  Bij de ontwikkeling van haar internetdiensten speelt veiligheid en betrouwbaarheid een cruciale rol, SURF verzet zich tegen ontwik-kelingen die het internet minder veilig en be-trouwbaar maken. SURF heeft als aanbieder van diensten een zorgplicht jegens haar gebruikers. Een zorgplicht met betrekking tot de veiligheid en betrouwbaarheid van onze diensten inclusief grondrechten van onze gebruikers zoals privacy.

- *Bescherm de publieke kern tegen politieke en commerciële invloeden:*
  De centrale protocollen en infrastructuren van het Internet moeten als een mondiaal publiek goed beschouwd worden. Deze publieke kern van het Internet moet gevrij-waard blijven van oneigenlijke interventies van overheden en andere partijen die schade toebrengen en het vertrouwen in het Internet eroderen.

UITGANGSPUNTEN

De IAA-visie dient om regie te kunnen voeren binnen dit werkveld op de punten waar ketenpartijen (moeten) samenwerken. Omdat SURFnet gelooft in de kracht van samenwerking heeft de visie een richtinggevend karakter: zij moet betrokkenen helderheid geven over de gezamenlijke ontwikkelingsrichting en verleiden in de geest van deze visie onder eigen verantwoordelijkheid en in eigen tempo stappen te nemen.

De visie is zodanig beschreven dat ze meerjarig bruikbaar is. Om dit te realiseren is er voor gekozen zo beperkt mogelijk keuzes vast te leggen in implementatie en techniek, daardoor kan in de toekomst bij implementatie, flexibel worden ingespeeld op ontwikkelingen en stand der techniek.

De visie vertaalt zich in principes die in onderlinge samenhang moeten worden beschouwd en in sommige gevallen gewogen moeten worden omdat ze door het abstractieniveau soms een (ogenschijnlijk) tegenstrijdigheid lijken te hebben.

RICHTINGGEVENDE PRINCIPES VOOR EEN IAA INFRASTRUCTUUR / AFSPRAKENSTELSEL VOOR HOGER ONDERWIJS EN ONDERZOEK

1 Met de IAA-Infrastructuur bieden we een afsprakenstelsel dat vertrouwen in het gebruik van diensten tussen gebruikers, instellingen en (commerciële) dienstaanbieders biedt en stimuleert. Gezien de positie van onze IAA-infrastructuur in de keten zorgen we, ook bij het doorvoeren van veranderingen, voor betrouwbare dienstverlening van hoge kwaliteit. Het afsprakenstelsel is in lijn met de Europese dataprotectie-wetgeving;

2 We hebben privacy van de gebruiker hoog in het vaandel en streven daarbij een minimale vastlegging en doorgifte van gegevens van de gebruiker na;

3 De IAA-Infrastructuur beperkt zich niet alleen tot toegang voor de individuele gebruiker tot diensten, maar creëert ook de vertrouwensinfrastructuur die nodig is voor het samenwerken in groepen en het gebruik door zelfstandig opererende apparaten. We differentiëren daarbij policies binnen het afsprakenstelsel om verschillende internationale en cross-sectorale samenwerkingsbehoeften van de doelgroep te ondersteunen;

4 We stellen transparantie over onze dienstverlening en maximale informatievoorziening naar alle betrokken partijen voorop zodat iedereen een weloverwogen beslissing kan nemen;

5 Bij de vertaling van de visie naar implementatie in dienstverlening onderzoeken we steeds of en wat bestaande (praktijk) implementaties kunnen betekenen en welke standaarden daarbij geëigend zijn. Voor zover deze (nog) niet voorhanden zijn of voldoen dragen we zelf bij aan de ontwikkeling ervan;

6 We stellen de belangen van de gebruiker centraal. We doen dit bijvoorbeeld door ruimte te bieden voor eigen authenticatiemiddelen (voor zover die een passend Level of Assurance (LoA) hebben), zelfbeschikking over vrijgave van attributen in te regelen en inzage te geven in het gebruik van de identiteit en bijbehorende attributen door dienstverleners;

7 We onderkennen het nut en de noodzaak voor een uniek identificerend kenmerk voor gebruikers (studenten en medewerkers) dat bruikbaar is voor alle relevante dienstverlening. Het uniek identificerend kenmerk mag binnen het stelsel de privacy van de gebruiker niet in gevaar brengen. En mocht daar wel risico toe zijn, dan is het aan de gebruiker daar expliciet mee in te stemmen;

8 We zien dat op termijn, naast de identiteiten die geleverd worden door de Identity Providers van de onderwijs- en onderzoeksinstellingen, ook identiteiten van buiten het onderwijs- en onderzoeksdomein een rol gaan spelen in het stelsel. Gebruikers brengen dan hun eigen identiteit mee – hetgeen ze meer vrijheid en flexibiliteit geeft (bijvoorbeeld wanneer iemand aan meer dan één instelling verbonden is). Instellingen kunnen hun gebruikers dan ondersteunen door deze identiteiten te verrijken met attributen vanuit de onderwijs- en onderzoekscontext, voor zover die relevant zijn;

9 We onderkennen dat het niet alleen gaat om een basisidentiteit, maar ook om attributen die relevant zijn voor de onderwijs- en onderzoekscontext. We zien dan ook dat instellingen en andere aan onderwijs en onderzoek gerelateerde partijen als attributenprovider kunnen (gaan) optreden zodat bijvoorbeeld personalisatie of autorisatie op basis van attributen kan worden gedaan;

10 We willen dat het stelsel leveranciersonafhankelijk werkt en daarbij een brede selectie aan authenticatiemiddelen ontsluit die passen bij de situatie van de gebruiker. Dat betekent dat we een multimiddelen strategie voor zowel de eerste als tweede authenticatiefactor nastreven;

11 We zien nut en noodzaak voor het met één authenticatiemiddel kunnen authenticeren voor meerdere toepassingen binnen het stelsel. Ook zien we behoefte één authenticatie (sessie) te kunnen hergebruiken voor authenticatie naar meerdere applicaties. Kortom een hergebruik van middelen die een enkelvoudige inlog, en meervoudig gebruik van vastgestelde identiteit (SSO) bieden. Dit geldt voor webbased en non-webbased diensten, toegankelijk via de desktop of mobiele apparaten;

12 Om het juiste beveiligings- en vertrouwensniveau te bieden, ondersteunt het stelsel meerdere betrouwbaarheidsniveaus (LoA) op grond van het identificatie- en registratieproces en het gehanteerde authenticatiemiddel. Hierdoor kunnen diensten worden ontsloten die een hoger betrouwbaarheidsniveau verlangen of waar nodig een tweede factor gebruiken. Voor het normenkader van deze betrouwbaarheidsniveaus wordt aangesloten op algemene standaarden;

13 We ondersteunen het gebruik van IAA-voorzieningen en diensten door buitenlandse studenten en medewerkers alsmede Nederlandse studenten en onderzoekers wanneer ze in het buitenland verblijven. Immers onderwijs en onderzoek zijn niet alleen nationaal, maar steeds meer Europees en mondiaal georiënteerd;

Omdat onderzoek en onderwijs niet ophoudt bij de grens van de instelling ondersteunt het stelsel een diverse groep gebruikers die gerelateerd zijn aan onderwijs, onderzoek en zorg. Het gaat daarbij om leerlingen/studenten, maar ook gastgebruik dat relevant is binnen de onderwijs- en onderzoekscontext, zoals stagebedrijven, commerciële research of samenwerking met industrie.

COLOFON

Auteur
SURFnet

Ontwerp
Vrije Stijl, Utrecht

Fotografie
Pexels, Pixabay

Januari 2017

Copyright

Beschikbaar onder de licentie Creative Commons Naamsvermelding 3.0 Nederland. Meer informatie over deze licentie vindt u op http://creativecommons.org/licenses/by/3.0/deed.nl

SURFnet

Postbus 19035
3501 DA Utrecht

088 – 787 30 00
www.surf.nl/surfnet