

Digitaal vertrouwen

Auteurs

Helmer van Merendonk (Hogeschool Utrecht), Juul de Louw (Koning Willem-1 College), Peter Eikelboom (SURF), Marlies Rikken (SURF)

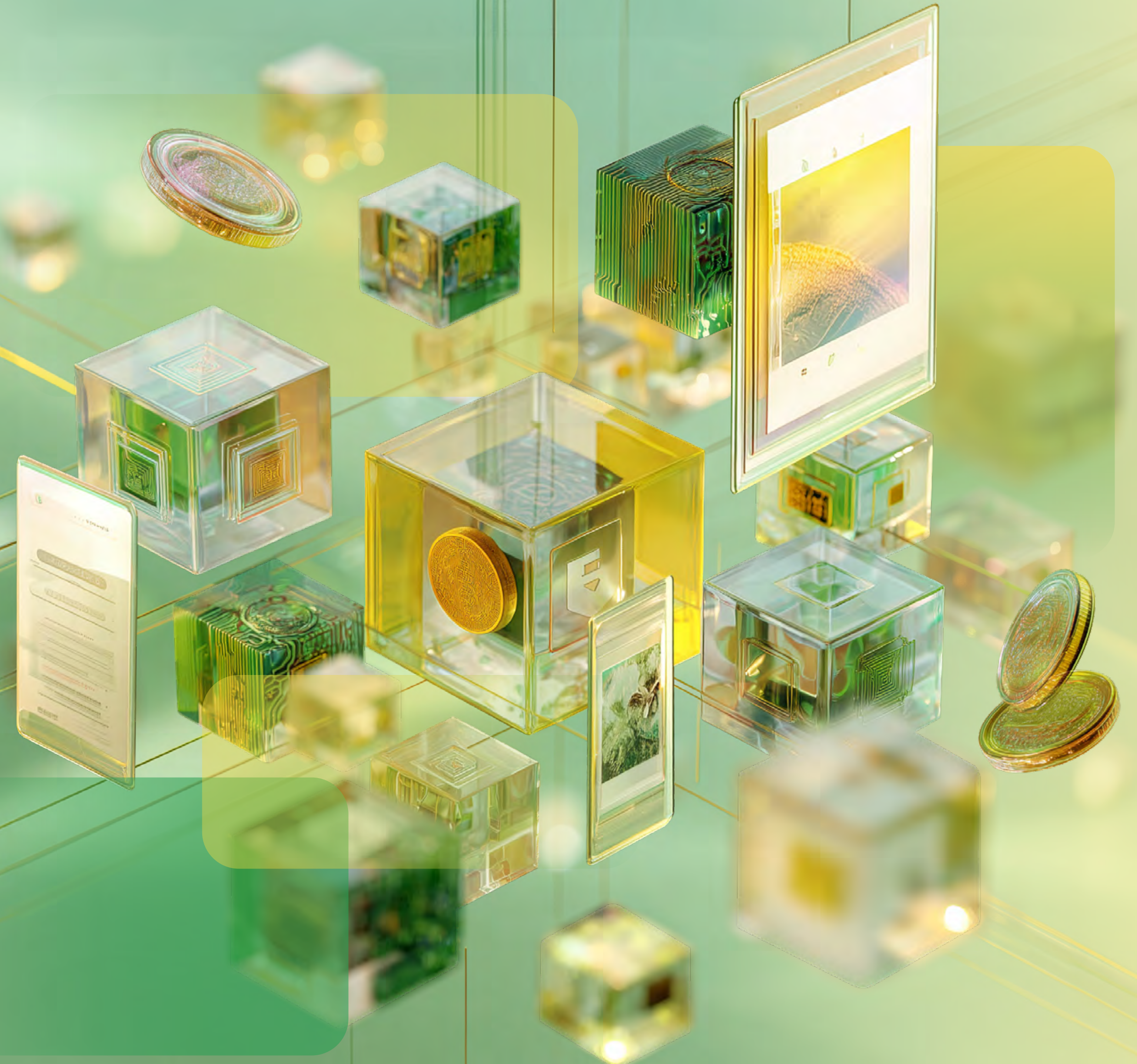
1. Opkomst van betrouwbare authenticatie

2. Meer decentralisatie van gegevenseigendom dankzij SSI-oplossingen

3. Opkomst van organisatorische wallets

4. Bevordering van transparantie in toeleveringsketens met digitale productpaspoorten

5. Digital trust frameworks: van hiërarchische naar gedistribueerde modellen van vertrouwen



Inleiding

Vertrouwen vormt de basis van alle digitale interacties. Het is het vertrouwen dat mensen, systemen en technologieën betrouwbaar, veilig en integer zullen handelen. In de digitale wereld betekent vertrouwen dat persoonlijke gegevens worden beschermd, systemen werken zoals bedoeld en technologieën ethische en veilige praktijken handhaven. Naarmate digitale ecosystemen complexer worden, wordt het behouden en verdienen van dat vertrouwen niet alleen een technische uitdaging, maar ook een strategische prioriteit.

Er vindt een verschuiving plaats in de manier waarop digitale identiteiten en verifieerbare credentials van personen, organisaties en objecten (fysiek en digitaal) worden behandeld. De Europese Unie (EU) loopt voorop in deze transformatie met het Digital Europe Program (DIGITAL). Centraal in deze transformatie staat het European Union Digital Identity

(EUDI) Wallet-initiatief, dat burgers meer en veilige controle over hun digitale identiteiten wil geven. In een tijdperk waarin verkeerde informatie, desinformatie en identiteitsmisbruik wijdverbreid zijn, kan het opslaan van digitale identiteiten en credentials in digitale wallets helpen om de verantwoordingsplicht te verbeteren, eigendom te beschermen en misbruik van persoonsgegevens te verminderen. Tegen 2027 zal elke EU-burger toegang hebben tot een eerste versie van een digitale wallet. Deze wallet kan worden gebruikt om persoonlijke gegevens op te slaan en te delen. Deze informatie heeft betrekking op zowel online als offline openbare en particuliere diensten in de hele EU.

De EUDI Wallet zal in veel aspecten van het moderne leven toepasbaar zijn en zal gevolgen hebben voor de manier waarop mensen belangrijke identificatiegegevens gebruiken

en raadplegen. Zo zal het bijvoorbeeld mogelijk zijn om een digitale versie van iemands rijbewijs op te slaan, waardoor het niet meer nodig is om altijd een fysiek exemplaar bij zich te hebben. Naast identificatiegegevens zal de EUDI Wallet zorgen voor een naadloze erkenning van kwalificaties en autorisatie in de hele EU, waardoor toelating tot het onderwijs, het beheer van credentials, de overplaatsing van studenten, sollicitaties en de mobiliteit van talent worden vereenvoudigd. Tegelijkertijd zal fraude worden teruggedrongen en zullen veilige en cryptografisch beschermde identiteiten en credentials worden bevorderd. Dit zal helpen om vervalsing tegen te gaan en het vertrouwen in kwalificaties te vergroten.

De toekomst van digitaal vertrouwen zal mensen meer controle geven over hun eigen gegevens, door conceptuele modellen zoals Self-Sovereign Identity (SSI) te omarmen,

samen met het gebruik van digitale wallets om hun identiteit en credentials te delen. Het succes van deze initiatieven zal een aanzienlijke impact hebben op burgers, alsook op publieke en private organisaties. Digitaal vertrouwen zorgt ervoor dat de identiteiten en gegevens van mensen en organisaties veilig worden behandeld, dat digitale interacties betrouwbaar zijn en dat hun privacy, wat betreft hun identiteit en gegevens, wordt beschermd. Nieuwe typen van vertrouwensnetwerken zullen een digitale wereld creëren die veiliger, eerlijker en betrouwbaarder is voor iedereen.

Bijdragers

Yvo Hunink (oprichter van Regen Studio), **Niels van Dijk** (SURF), **Peter Leijnse** (SURF), **Michiel Schok** (SURF), **Peter Nobels** (HU)

TREND #1

Opkomst van betrouwbare authenticatie

Publieke waarden

-  Autonomie Persoonlijke empowerment
-  Rechtvaardigheid Transparantie | Gelijkwaardigheid | Inclusie | Integriteit
-  Menselijkheid

Volwassenheid

- WATCH
- PLAN
- ACT

Drivers

Individualisering en empowerment; Cybersecurity en vertrouwen; Digitale transformatie

Europese kaders (eIDAS 2.0 en MiCA-verordening) geven het digitale landschap een nieuwe vorm met twee nieuwe concepten: Verifiable Credentials (VC's) en digitale activa. Beide zullen tegen 2030 een verschuiving mogelijk maken naar betrouwbare digitale herkenning van fysieke en digitale objecten.

VC's zijn fraudebestendige digitale bewijzen (diploma's of kwalificaties) die worden uitgegeven door vertrouwde instanties en die individuen in hun digitale wallet kunnen bewaren.

Digitale activa in de vorm van tokens, waaronder niet-vervangbare tokens (NFT's), vertegenwoordigen digitale waarde, toegang of eigendom. Het is ontworpen om overdraagbaar te zijn: zodra een token je wallet verlaat, gaan de bijbehorende rechten mee, waardoor ze geschikt zijn voor (waarde)uitwisseling, eenmalige erkenning of deelname aan initiatieven.

Aspect	Verifiable Credential	Token/digitale activa
Functie	Herbruikbaar bewijs van prestaties of vaardigheden, identiteit of status	Overdraagbare waarde, toegang of deelname
Herbruikbaarheid	Ja, de houder kan het meerdere keren tonen	Nee, het beweegt met eigendom
Privacy	Door de gebruiker gecontroleerde, selectieve openbaarmaking	Vaak openbaar, afhankelijk van het ontwerp van het token
Verificatie	Via digitale handtekening en open standaarden (bijv. W3C, OpenID4VC)	Via blockchain-consensus en slimme contracten

SIGNALEN

Europese regelgeving

eIDAS 2.0-verordening (eur-lex.europa.eu) [↗](#)

Verordening betreffende markten voor crypto-activa (MiCA) (eur-lex.europa.eu) [↗](#)

Nederlandse overheid - Toekomstverkenning Digitalisering 2030 (rijksoverheid.nl) [↗](#)

Onderwijs, vaardigheden en leven lang ontwikkelen

SELFIE voor werkgebaseerd leren (education.ec.europa.eu) [↗](#)

Digitale referenties en leven lang ontwikkelen (unesdoc.unesco.org) [↗](#)

Union of Skills (2024) (commission.europa.eu) [↗](#)

Kaders

Verifiable Credentials en digitale identiteit (2024) - Verifiable Credentials gegevensmodel 2.0 (w3.org) [↗](#)

OpenID voor Verifiable Presentations and Credentials (OpenID4VC) (2024) (openid.net) [↗](#)

Europese digitale identiteitsportemonnee – Architectuur en referentiekader (2024) (eu-digital-identity-wallet.github.io) [↗](#)

Digitale activa en tokens

Tokenisering van activa op de financiële markten: de volgende generatie van waardeoverdracht (2025) (reports.weforum.org) [↗](#)

“Technologieën voor digitaal vertrouwen, zoals Verifiable Credentials, fungeren als de nieuwe onzichtbare handdruk in het digitale tijdperk. Ze stellen mensen en organisaties in staat om bij elke interactie direct en veilig te bewijzen wie ze zijn en wat ze weten.”

- Adam Eunson, COO, AuvoDigital

IMPACT



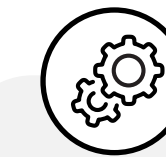
Onderwijs

- Leerlingen/studenten krijgen meer controle over hun leer- en loopbaantrajecten met digitale wallets, waarmee ze betrouwbare, verifieerbare prestaties kunnen beheren en delen over contexten en landsgrenzen heen. Deze verschuiving verhoogt de mobiliteit, autonomie en zichtbaarheid.
- Onderwijsinstellingen nemen nieuwe rollen op zich als uitgevers en validators binnen gedecentraliseerde erkenningsnetwerken, waar formele certificaten en doelgerichte tokens naast elkaar bestaan. Deze transformatie ondersteunt modulaire leertrajecten, gepersonaliseerde erkenning en bredere betrokkenheid van belanghebbenden, van werkgevers tot maatschappelijke partners.



Onderzoek

- Gedecentraliseerde reputatiemodellen en op tokens gebaseerde systemen maken transparantere, collaboratieve ecosystemen en nieuwe manieren om bijdragen te erkennen mogelijk. Op systeemniveau bieden eIDAS 2.0 en MiCA de juridische basis die interoperabele, leerlinggerichte ecosystemen mogelijk maakt en laat opschalen.
- Een toekomstbestendig onderwijs- en onderzoekslandschap, waarin vertrouwen, flexibiliteit en erkenning zijn verankerd, waardoor individuen en instellingen zich kunnen ontplooien in een digitaal verbonden wereld.



Operations

Dankzij interoperabele en betrouwbare gegevensuitwisseling zullen gestroomlijnde processen, minder administratieve taken en geautomatiseerde verwerking van certificaten worden gerealiseerd.

TREND #2

Meer decentralisatie van data-eigendom dankzij SSI-oplossingen

Publieke waarden

	Autonomie	Keuzevrijheid Onafhankelijkheid Privacy
	Rechtvaardigheid	Inclusie Gelijkwaardigheid Integriteit
	Menselijkheid	Sociale samenhang Betekenisvol contact Welzijn Veiligheid Zelfontplooiing Respect

Volwassenheid

WATCH

PLAN

ACT

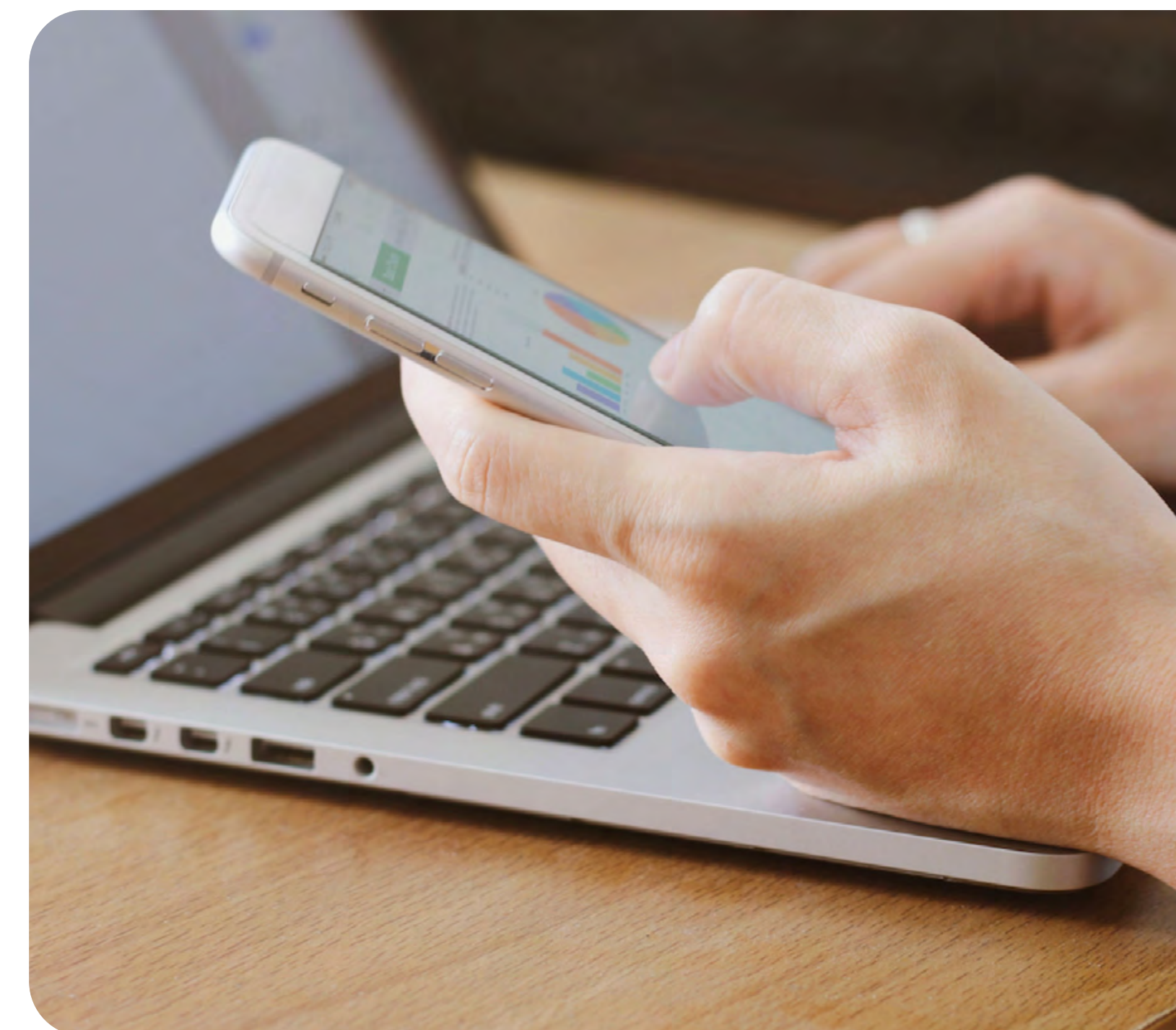
Drivers

Individualisering en empowerment; Cybersecurity en vertrouwen; Digitale transformatie; Dynamiek binnen gemeenschappen en maatschappelijke samenhang

De toenemende waarde van persoonsgegevens heeft geleid tot misbruik door vele actoren in de samenleving, variërend van grote technologiebedrijven tot gegevensmakelaars en zelfs overheden.

Dit heeft geleid tot een tegenbeweging die zich richt op empowerment van gebruikers en bescherming van gegevensrechten. Binnen het domein van digitale identiteit en vertrouwen wordt deze verschuiving naar datadecentralisatie en individuele controle doorgaans aangeduid als Self-Sovereign Identity (SSI).

De kernprincipes van SSI zijn onder meer gegevensoverdraagbaarheid, gegevensminimalisatie en toegang tot persoonsgegevens. In wezen streeft SSI ernaar individuen meer zeggenschap te geven en gegevensrechten te beschermen, waarbij de binnenkort te verschijnen EUDI Wallet een typische SSI-oplossing is.



SIGNALEN

De weg naar Self-Sovereign Identity

(lifewithalacrity.com) [↗](#)

eIDAS 2.0-verordening - kader voor digitale identiteit en authenticatie

(digitale-strategie.ec.europa.eu) [↗](#)

Wet op het hoger onderwijs en wetenschappelijk onderzoek (NL)

(wetten.overheid.nl) [↗](#)

Een digitale identiteit en persoonlijke digitale wallet voor EU-burgers, inwoners en bedrijven

(ec.europa.eu) [↗](#)

Gegevens per bron (digitaleoverheid.nl) [↗](#)

IMPACT



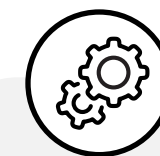
Onderwijs

Onderwijsinstellingen geven diploma's uit die moeten worden opgeslagen om te kunnen worden gevalideerd. Om deze diploma's aan personen te kunnen koppelen is persoonlijke informatie nodig. Dit maakt het een uitdaging om processen te ontwerpen die een evenwicht bieden tussen privacy en bruikbaarheid en tegelijkertijd autonome besluitvorming bevorderen.



Onderzoek

De verschuiving naar Self-Sovereign Identity (SSI) verandert het beheer van persoonsgegevens ingrijpend. Onderzoekers worden aangespoord om goede praktijken te volgen en systemen te reguleren die zowel mensenrechten en wetgeving naleven als technisch uitvoerbaar zijn, en die interdisciplinair onderzoek met brede maatschappelijke en beleidsrelevantie ondersteunen.



Operations

- Oververeenvoudigde gebruikersprocessen kunnen leiden tot onbewuste beslissingen en onbedoelde gegevensuitwisseling, terwijl overmatige complexiteit de bruikbaarheid kan belemmeren. Een evenwichtige aanpak is essentieel. Tools die zijn gebaseerd op principes van Self-Sovereign Identity (SSI) kunnen gebruikers in staat stellen hun rechten uit te oefenen en tegelijkertijd voldoen aan de AVG-vereisten.
- Door gebruikers meer zeggenschap te geven, wordt de institutionele controle over uitgegeven certificaten verminderd. Instellingen moeten identiteiten of wallets verifiëren voordat ze certificaten uitgeven, zodat gebruikers deze certificaten sectoroverstijgend kunnen toepassen.

TREND #3

Opkomst van organisatorische wallets

Publieke waarden

	Autonomie	Privacy
	Rechtvaardigheid	Integriteit
	Menselijkheid	Veiligheid

Volwassenheid

WATCH

PLAN

ACT

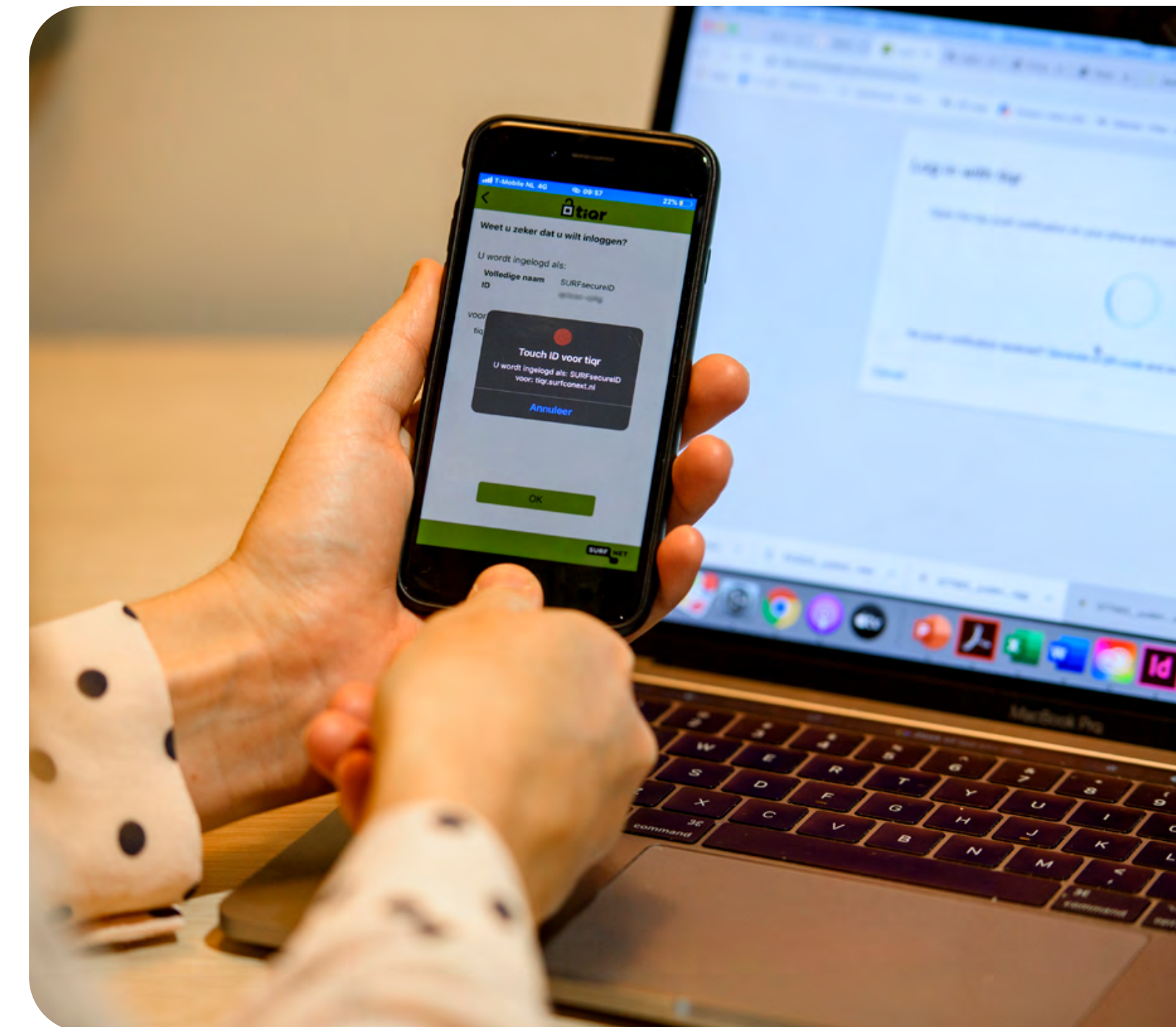
Drivers

Individualisering en empowerment; Cybersecurity en vertrouwen; Digitale transformatie

Vertrouwens- en interoperabiliteitskwesties hebben zakelijke interacties in heel Europa belemmerd. Het in 2025 aangekondigde initiatief European Business Wallet (EBW) pakt deze inefficiënties aan met een uniforme, grensoverschrijdende digitale identiteitsoplossing voor organisaties.

Organisatorische wallets zijn digitale webgebaseerde wallets die veilige digitale identificatie bieden, het delen van gegevens stroomlijnen en wettelijke kennisgevingen door bedrijven en andere rechtspersonen vergemakkelijken. In tegenstelling tot persoonlijke wallets ondersteunen organisatorische wallets toegang voor meerdere gebruikers en op rollen gebaseerde machtigingen (zoals volmachten).

Met één muisklik kunnen de identiteit, status en kenmerken van een organisatie worden herkend, waardoor fraude (zoals valse websites of phishing) kan worden voorkomen, kosten met betrekking tot compliance kunnen worden verlaagd en grensoverschrijdende samenwerking kan worden versneld.



Organisatorische wallets moeten rekening houden met de complexiteit van de identiteit van rechtspersonen, zoals het beheer van de levenscyclus van credentials, internationale standaarden en integratie met handelsregisters.

SIGNALEN

Beleid

EU-architectuur en referentiekader (ARF) (github.com) [↗](#)

European Business Wallet: digitale identiteit, veilige gegevensuitwisseling en wettelijke kennisgevingen voor eenvoudige, digitale bedrijfsvoering. (ec.europa.eu) [↗](#)

Gebruiksscenario's en experimenten

Onderzoek naar digitale identiteitsportefeuilles van de EU voor rechtspersonen met Company Passport en iSHARE (coe-dsc.nl) [↗](#)

Grootschalige EU-proefprojecten met wallets voor bedrijven (digital-strategy.ec.europa.eu) [↗](#)

“Nu de Europese Unie op weg is naar de volledige implementatie van de EU Digital Identity Wallet (EUDI), moeten bedrijven zich voorbereiden op een digitale transformatie in de manier waarop identiteiten worden geverifieerd, klanten worden aangemeld en elektronische handtekeningen worden gezet.”

- Signicat (signicat.com)

IMPACT



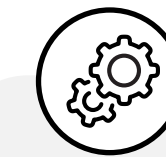
Onderwijs

- Onderwijzers en studenten zouden moeten profiteren van een aanzienlijke vermindering van administratieve vertragingen bij internationale uitwisselings-/mobiliteitsprogramma's zoals Erasmus+ en grensoverschrijdende onderwijs- of studiemogelijkheden.
- Veilige, geverifieerde institutionele credentials maken een snelle en betrouwbare bevestiging mogelijk van inschrijvingen, kwalificaties en affiliaties rond stages, vervolgstudies of samenwerkingsverbanden.
- Minder blootstelling aan phishing en frauduleuze communicatie vergroot het vertrouwen en de digitale veiligheid in wetenschappelijke correspondentie en beschermt persoonlijke en institutionele informatie.



Onderzoek

- Een verminderd risico op identiteitsfraude of frauduleuze samenwerkingsverzoeken beschermt intellectueel eigendom en de geloofwaardigheid van projectonderzoek.
- Geverifieerde institutionele identiteiten zouden de totstandkoming van grensoverschrijdende samenwerkingsverbanden, gezamenlijke financieringsaanvragen en consortiumovereenkomsten moeten versnellen.



Operations

- Onmiddellijke verificatie van de identiteit van instellingen zal een snellere uitvoering van informatie-uitwisseling in Europese publiek-private partnerschappen en onderzoekssamenwerkingen mogelijk maken, waardoor de administratieve werklast wordt verminderd.
- Op rollen gebaseerde digitale toegang en betrouwbare officiële communicatie versterken de veiligheid door het risico op phishing te verminderen en de juridische geldigheid te waarborgen. Bovendien worden de kosten met betrekking tot compliance verlaagd door veilige, geverifieerde informatie-uitwisseling.
- Integratie met interne systemen stroomlijnt het controleren en goedkeuren van credentials, waardoor de efficiëntie wordt verbeterd en processen worden geoptimaliseerd, hoewel er wel een initiële investering in personeelstraining en technologische infrastructuur nodig is.

TREND #4

Bevordering van transparantie in toeleveringsketens met digitale productpaspooorten

Publieke waarden

	Autonomie	Keuzevrijheid Onafhankelijkheid Privacy
	Rechtvaardigheid	Inclusie Gelijkwaardigheid
	Menselijkheid	Sociale samenhang Betekenisvol contact Welzijn Veiligheid Zelfontplooiing Respect

Volwassenheid

WATCH

PLAN

ACT

Drivers

Regelgeving en naleving (compliance); Cybersecurity en vertrouwen; Digitale transformatie

De EU-verordening inzake ecologisch ontwerp voor duurzame producten (ESPR) is medio 2024 in werking getreden. Deze verordening verplicht bedrijven om informatie openbaar te maken over de herkomst van hun producten en de milieu-impact ervan. Deze verplichte implementatie van digitale productpaspooorten (DPP's) zorgt ervoor dat productgegevens authentiek, betrouwbaar, en conform regelgeving zijn.

De implementatie van DPP's zal een uitdaging zijn, en productie- en productgegevens moeten worden geverifieerd en toegankelijk zijn via een gegevensdrager. Ontwikkelingen op het vlak van wetgeving zullen invloed hebben op standaarden en DPP-dienstverleners.

Terwijl de wetgeving wordt afgerond, ontwikkelen Europese normalisatie-instellingen de standaarden voor DPP's, die begin 2026 moeten worden aangenomen.



SIGNALEN

Verordening inzake ecologisch ontwerp voor duurzame producten (commission.europa.eu) [↗](#)

Centre of Excellence for Digital Product Passports (coe-dpp.nl) [↗](#)

Gegevensuitwisseling – Digitaal productpaspoort (tno.nl) [↗](#)

Standpuntnota van Fides (voorheen Dutch Blockchain Coalition) over betrouwbare DPP's (fides.community) [↗](#)

“Digitale productpaspoorten zullen het belangrijkste middel worden voor het rapporteren van alle productgerelateerde nalevingsinformatie binnen de Europese Unie. Bedrijven die verder gaan dan alleen voldoen aan de regelgeving en DPP’s centraal stellen in hun supply chain-informatiesystemen, zullen aanzienlijke extra voordelen ervaren.”

- Yvo Hunink, oprichter van Regen Studio en medeauteur van het position paper over betrouwbare digitale productpaspoorten

Gebruiksscenario's en pilots

Demonstratie van functionerende DPP's in verschillende sectoren (cirpass2.eu) [↗](#)

Digitale productpaspoorten: lessen van een early adopter (Brits dameskledingmerk Nobody’s Child) (voguebusiness.com) [↗](#)

IMPACT



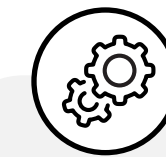
Onderwijs

- Verschillende scholen en universiteiten bespreken al de mogelijkheden van het gebruik van DPP's, de uitdagingen die daarmee gepaard gaan, en werken aan prototypes.
- Studenten onderzoeken de effecten op duurzaamheid, geschikte bedrijfsmodellen en de technische (on)mogelijkheden die gepaard gaan met de inzet van DPP's.



Onderzoek

DPP's kunnen ook relevant zijn voor onderzoek en datasets, met name op het gebied van duurzaamheid, IT, productlevenscyclusanalyse en transparantie in de toeleveringsketen.



Operations

- Onderwijsinstellingen kunnen hun impact op het milieu minimaliseren en hun inkoop- en campusbeheer verbeteren.
- Hoewel ze niet verplicht zijn om te voldoen aan de richtlijn inzake duurzaamheidsverslaglegging voor bedrijven (CSRD), kiezen veel instellingen proactief voor duurzame producten en partners.
- Het DPP zal de inkoop verbeteren, de transparantie vergroten en het vastgoedbeheer verbeteren, waardoor campussen weloverwogen, duurzame keuzes kunnen maken.



TREND #5

Digital Trust Frameworks: van hiërarchische naar gedistribueerde modellen van vertrouwen

Publieke waarden

	Autonomie	Keuzevrijheid Persoonlijke empowerment Onafhankelijkheid Privacy
	Rechtvaardigheid	Inclusie Gelijkwaardigheid Integriteit
	Menselijkheid	Sociale samenhang Betekenisvol contact Welzijn Veiligheid

Volwassenheid

WATCH

PLAN

ACT

Drivers

Individualisering en empowerment; Cybersecurity en vertrouwen; Digitale transformatie

Het vertrouwen dat we in diploma's stellen, is grotendeels gebaseerd op verificatie door gezaghebbende bronnen; we kunnen niet uitsluitend vertrouwen op de beweringen van een persoon zelf. Daarom worden onderwijsinstellingen als gezaghebbend beschouwd wanneer ze diploma's en getuigschriften afgeven. Instellingen moeten verifiëren dat de persoon cursussen of examens heeft gevolgd, en de instelling zelf moet aantoonbaar geaccrediteerd zijn.

De huidige vertrouwenskaders (trust frameworks) die dit systeem ondersteunen, zijn grotendeels hiërarchisch. Nieuwe standaarden, zoals OpenID Federation, maken niet-hiërarchisch vertrouwen mogelijk, vormen een aanvulling op bestaande identiteitsfederaties en maken meer onafhankelijke samenwerkingen mogelijk.

Dit neemt echter niet weg dat vertrouwen nog steeds nodig is. Er zijn nog steeds autoriteiten nodig voor de accreditatie van instellingen en diploma's.



Bovendien zijn er, wanneer processen een hoog niveau van vertrouwen vereisen, aanvullende technische controles en organisatorische regels en voorschriften nodig.

SIGNALEN

OpenID wereldwijde standaarden

OpenID Federation 1.0-specificatie (openid.net) [↗](#)

OpenID API-specificatie voor de uitgifte van Verifiable Credentials (openid.net) [↗](#)

Identiteitsfederaties in de praktijk

OpenID Connect Federation: Hoe multilaterale federaties op te zetten met behulp van OIDC (indico.geant.org) [↗](#)

Identiteitsfederaties en het interfederatieve eduGAIN (wiki.geant.org) [↗](#)

EduGAIN OIDC-proefproject (indico.cern.ch) [↗](#)

IMPACT



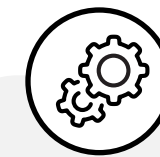
Onderwijs

De rol van instellingen in het onderwijsdata-ecosysteem verandert, en verzoeken om data en toegang tot tools komen zowel van binnen als buiten het ecosysteem. Hierdoor zal het opbouwen van vertrouwen in de authenticiteit van credentials steeds uitdagender worden.



Onderzoek

De invloed van het EU-kader voor digitale identiteit op de adoptie van digitale wallets in onderzoek en onderwijs, en de gevolgen daarvan voor vertrouwenskaders, wordt momenteel onderzocht.



Operations

Instellingen moeten bepalen hoe credentials op betrouwbare wijze aan personen kunnen worden toegekend. Dit vereist identiteitscontrole bij inschrijving, tijdens beoordelingen en mogelijk zelfs bij aanwezigheid.



Meer informatie over digitaal vertrouwen?

[Bezoek surf.nl](https://surf.nl) 

SURF Utrecht

Kantoren Hoog Overborch
Hoog Catharijne
Moreelsepark 48
3511 EP Utrecht
+31 88 787 30 00

SURF Amsterdam

Science Park 140
1098 XG Amsterdam
+31 88 787 30 00

futuring@surf.nl
www.surf.nl