

Eventverslag – TIP Kennissessie 8 mei 2025

Thema: Samen vooruit in online identificatie

Locatie: Jaarbeurs Utrecht

Sprekers:

- Roos Dijkxhoorn (Purasec, Privacy Company)
 - Iris van der Wel (Cleverbase)
 - Frans Hietbrink (Voorzitter werkgroep Governance TIP)
-

Doel van de sessie

De TIP-kennissessie op 8 mei 2025 bracht publieke en private partijen samen rondom een gemeenschappelijk doel: het versterken van veilige en betrouwbare online identificatie binnen uiteenlopende domeinen. Hierbij lag de nadruk op de toepassing van de Europese eIDAS-verordening en de impact van de European Digital Identity Wallet (EUDI-wallet) op online identificatie. Het dynamische juridische en technische kader voor online identificatie is complex: de sessies bood handvatten aan toezichthouders voor de beoordeling van online identificatieoplossingen – met en zonder de EUDI-wallet.

Deel 1 – Domeinspecifieke toepassing van wetgeving op eID en vertrouwensdiensten

Spreker: Roos Dijkxhoorn

Roos ging in op de uitdaging van het toepassen van Europese en nationale wetgeving, zoals eIDAS, de wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Wet digitale overheid (Wdo), op online identificatie in specifieke sectoren.

Take aways:

- Er is géén lijst beschikbaar met alle toereikende online identificatieoplossingen van vereiste betrouwbaarheidsniveaus. De EU lijsten dienen andere doelen. Zo dient de lijst met erkende eID-middelen enkel voor cross-border acceptatie van eID-middelen voor publieke dienstverlening.
- Er is geen one-size-fits-all-oplossing voor online identificatie; sectorspecifieke eisen maken maatwerk noodzakelijk.
- Professionals zijn verantwoordelijk voor het inzetten van voldoende betrouwbare identificatieoplossingen, inclusief passende, veilige verwerking in hun CRM-systemen.

- Beoordeling van benodigde betrouwbaarheidsniveau kan langs kaders van eIDAS (laag, substantieel en hoog). Kwaliteitsborging vereist inzet van relevante standaarden (o.a. ISO en ETSI). Van leveranciers mag verwacht worden dat zij hun compliance aantoonbaar maken.
- Beoordeling van identificatieoplossing gaat verder dan betrouwbaarheidsniveau: sectorspecifieke informatievraag en veiligheid CRM-systeem relevant. Inrichten van een Information Security Management System en inzet van vertrouwensdiensten zijn voorbeelden van adequate maatregelen om vastlegging van gegevens in het CRM-systeem van professional te beveiligen.
- De vertrouwensdienst voor gekwalificeerde elektronische handtekeningen is specifiek relevant in online identificatie: sterke herleidbaarheid naar ondertekenaar, legt onweerlegbaar vast wie ondertekend heeft en is onafhankelijk te valideren.
- Bestaande type informatieoplossingen hebben andere voor- en nadelen. Kies op basis van zekerheid, risk appetite en domeinspecifieke eisen:

TYPE ONLINE IDENTIFICATIEOPLOSSING

OPLOSSING	VOORDELEN	AANDACHTSPUNTEN
Gekwalificeerde elektronische handtekening	- Privacy-proof - Hoge herleidbaarheid	- Voldoet niet altijd aan sectorspecifieke informatievraag
Volledig dossier (Inclusief kopie ID)	- Volledig beeld voor onderzoek - Herkenbaar voor professionals	- Privacyrisico's - Onzekerheid over betrokkenheid gebruiker - Kans op datalekken
Hybride (IDP + vertrouwensdienst)	- Auditability - Goede balans privacy & zekerheid	- Vergt domeinkennis - Niet altijd standaard beschikbaar

Waar kun je als toezichthouder op letten bij de beoordeling van online identificatieoplossingen?

Voor de beoordeling van een toereikende online identificatieoplossing kun je kijken naar de betrouwbaarheid van het eID-middel volgens eIDAS en standaarden, de sectorspecifieke informatievraag en waarborgen voor de veiligheid en betrouwbaarheid van de vastlegging in het CRM-systeem van de professional (ISMS, vertrouwensdiensten).

Identity providers, vertrouwensdienstverleners, professionals én toezichthouders kunnen binnen TIP samenwerken om deze kaders voor beoordeling van veilige, online identificatieoplossingen verder te standaardiseren.

Deel 2 – De Europese Digitale Identiteitswallet: kansen en uitdagingen

Spreker: Iris van der Wel

Iris presenteerde de ontwikkelingen rondom de European Digital Identity Wallet (EUDI-wallet), die vanaf eind 2026 beschikbaar komt voor burgers en organisaties en de impact op online identificatie.

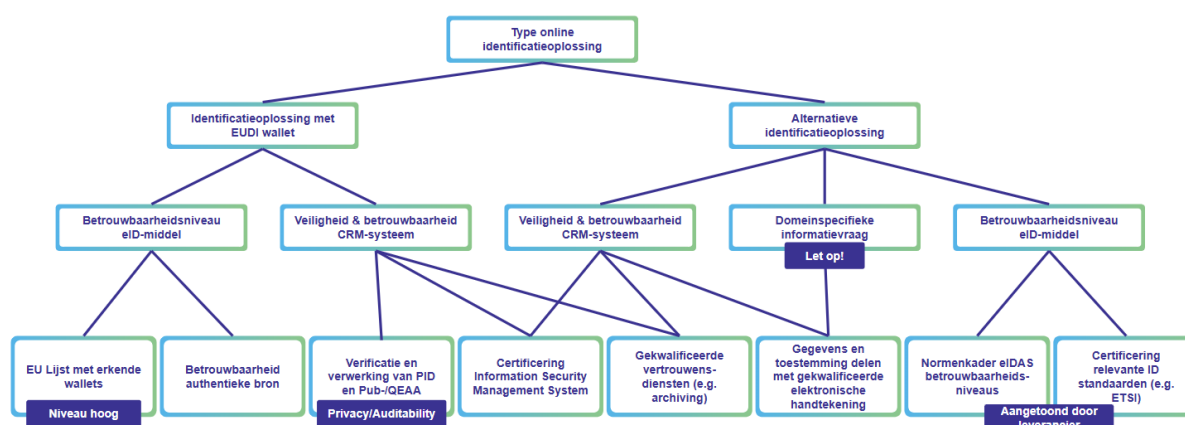
Belangrijke punten:

- De EUDI-wallet bevat 3 kernfuncties voor burgers: online identificatie, delen van geverifieerde gegevens, en gekwalificeerd ondertekenen. De wallet moet voor online identificatie voldoen aan het hoogste betrouwbaarheidsniveau volgens eIDAS.
- Nederland kiest voor een vergunningsstelsel met erkende publieke én private wallets. Gecertificeerde EUDI-wallets komen op een EU lijst die voor iedereen te controleren is. Zo kun je dus controleren of een wallet aan het vereiste niveau voldoet.
- eIDAS stimuleert gebruik van online identificatie en authenticatie met de EUDI-wallet door acceptatieplicht voor diverse publieke én private vertrouwende partijen.
- Het proces van online identificatie gaat veranderen: de wallet wordt gevuld met persoonsidentificatiedata (PID) die een gebruiker kan delen met de professional.
- Uitgifte van PID aan de wallet is beperkt tot een minimale set aan attributen; aanvullende gegevens zijn nodig voor professionals om te kunnen voldoen aan sectorspecifieke verplichtingen.

- De vertrouwensdienst voor publieke en gekwalificeerde elektronische attestatie van attributen (EAA), biedt een oplossing voor dit informatietekort. Maar deze nieuwe vertrouwensdienst is nog volop in ontwikkeling en er liggen nog open vraagstukken wat betreft privacy en auditability voor de beoordeling van de verificatie en verwerking van PIDs en EAA door professionals. De betrouwbaarheid van de bron die gebruikt is voor het uitgeven van het attest is essentieel voor het beoordelen van de betrouwbaarheid van de online identificatie.
- **Belangrijke kanttekening:** gebruik van de EUDI-wallet is vrijwillig: burgers moeten ook zonder wallet toegang tot online diensten blijven krijgen. De burger kan ook via andere, bestaande identificatie- en authenticatiemiddelen toegang te krijgen tot publieke en private diensten.
- Dus: de bevindingen uit kennissessie 1 blijven bestaan.

Waar kun je als toezichthouder op letten bij de beoordeling van online identificatieoplossingen met de EUDI wallet?

Het juridisch en technisch kader voor online identificatie met (en zonder) de EUDI wallet is complex. Op basis van de take aways uit beide sessies bieden wij een overzicht van aspecten die relevant zijn voor online identificatie en die toezichthouders en dienstverleners mee kunnen nemen in de beoordeling van online identificatieoplossingen – nu en straks met de wallet.



Dit overzicht is niet compleet – er zijn nog open vraagstukken waar Wallet & Identity providers, vertrouwensdienstverleners, professionals én toezichthouders samen invulling aan kunnen geven. Binnen TIP kunnen we samenwerken om open vraagstukken en kaders voor beoordeling van veilige, online identificatieoplossingen verder te standaardiseren.

Gezamenlijk perspectief – TIP als ecosysteem

Spreker: Frans Hietbrink

Frans benadrukte het belang van samenwerking binnen het TIP-ecosysteem om te komen tot betrouwbare digitale transacties, met aandacht voor:

- Heldere afspraken en specificaties.
- Gebruik van vertrouwensdiensten (zoals gekwalificeerde handtekeningen, archivering, en attesten).
- Toepassingen in de praktijk, zoals implementaties bij banken (ABN AMRO, ING, Rabobank) en makelaars (NVM/HDN).

TIP biedt structuur en governance om innovatie en compliance te combineren en versnellen.

Belangrijkste inzichten

- Geen universele oplossing: identificatie blijft afhankelijk van domein en toepassing.
- De komst van de EUDI-wallet creëert nieuwe mogelijkheden, maar ook nieuwe verantwoordelijkheden.
- Beoordeling van online identificatie moet plaatsvinden op drie niveaus:
 1. Betrouwbaarheid van het eID-middel
 2. Veiligheid en volledigheid van het CRM-systeem
 3. Voldoen aan domeinspecifieke informatie-eisen

Aanbevelingen voor organisaties

- Bereid je tijdig voor op de komst van de EUDI-wallet en bijbehorende regelgeving.
- Ga na welke attributen nodig zijn voor compliance in jouw sector.
- Werk samen met identity providers en vertrouwensdienstverleners voor een toekomstbestendige oplossing.
- Gebruik de kaders van TIP om transparantie, privacy en zekerheid te waarborgen.