| | |
|---|---|
| **aan** | Tweede Kamer der Staten-Generaal<br>Vaste commissie voor Digitale Zaken |
| **ons kenmerk** | SPF20260908 |
| **datum** | 8 september 2026 |
| **onderwerp** | Position paper Stichting Privacy First t.b.v. het rondetafelgesprek d.d. 10 september 2026 inzake de European Business Wallet en eIDAS-verordening |

# Privacy First position paper eIDAS

## Onze belangstelling voor identificatie c.a.

De belangstelling van Stichting Privacy First voor identificatie en daarmee samenhangende vraagstukken dateert al van lang geleden. In 2010-2015 procedeerden wij tegen de opslag van vingerafdrukken ten behoeve van identiteitsbewijzen in een centrale databank. Sindsdien is Privacy First zich met identificatie en biometrie bezig blijven houden. In september 2024 hebben wij de Minister van Financiën en De Nederlandsche Bank (DNB) verzocht om maatregelen om de risico's rondom identificatie door financiële instellingen te verminderen.

## Recente eIDAS commentaren Privacy First

Op 5 mei 2026 nam Privacy First deel aan de Europese consultatie over de EU Business Wallet. Op 1 juni 2026 verstuurden wij een uitvoerige brief aan onder meer de Tweede Kamer commissie voor Digitale Zaken over de EUDI-wallet, de Business Wallet en de eIDAS-verordening. Deze brief is in dit artikel aangekondigd.

## De behoefte van de ontvangende partijen

Privacy First begrijpt dat er veel ontvangende partijen (*relying parties*) zijn die goede redenen hebben om behoefte te hebben aan de wallets. Echter, dan moeten die wallets wel aan bepaalde eisen voldoen. Simpel gezegd hebben de wallets de volgende basiskenmerken:

* verificatie van de identiteit en authenticatie (inlogmiddel);
* digitale kaartenbak met gegevens die relevant zijn voor ontvangende partijen.

De ontvangende partijen kunnen zowel overheden zijn (bijvoorbeeld gemeenten in het sociaal domein) als bedrijven (bijvoorbeeld banken). De houder van de wallet zal hier als 'gebruiker' worden aangeduid. Wij benadrukken dat onze opmerkingen zowel voor de EUDI-

wallet als de Business Wallet gelden. Ook bij ondernemingen zijn mensen betrokkenen, zodat ook daar de AVG en andere regels op het gebied van gegevensbescherming een rol spelen.

## Voorwaarden

Essentieel voor het functioneren van de wallets en maatschappelijke acceptatie zijn de volgende voorwaarden:

1. **Vrijwilligheid voor de gebruiker**: op dit moment is die vrijwilligheid alleen theoretisch (door vermelding in de eIDAS-verordening), maar kunnen ontvangende partijen in de praktijk weigeren een overeenkomst aan te gaan / de dienst te verlenen als de wallet niet wordt gebruikt. Onder het nieuwe Europese antiwitwaspakket is voorgesteld om de EUDI-wallet verplicht te maken (zie onze brandbrief en eerdere deelname aan de EBA-consultatie). Privacy First bepleit extra maatregelen om de vrijwilligheid te waarborgen.

2. **Veiligheid en vertrouwelijkheid**: het mag bijvoorbeeld niet zo zijn dat private actoren in het systeem die geen recht hebben om van vertrouwelijke gegevens kennis te nemen, metadata zouden kunnen verzamelen die waardevolle commerciële informatie vormt en dit kunnen correleren met data uit andere datasets. De digitale kaartenbak moet veilig zijn en ook kunnen worden geleegd als de gegevens niet meer nodig zijn. Cybersecurity is vanwege AI een groeiend risico, zoals te zien is aan de waarschuwingen jegens de financiële sector door ESRB, de ESAs en FSB. Recent heeft het OM er eveneens aandacht voor gevraagd. Diverse technische deskundigen hebben in het verleden vraagtekens geplaatst bij de techniek van het eIDAS-ecosysteem.

3. **Integriteit en ontbreken van tegenstrijdig belang** bij de private actoren in het systeem, onder meer bij de wallet-aanbieder, maar ook bij de actoren die een faciliterende rol hebben, zoals de IT-partijen die voor verbindingen zorgen (zoals de verbinding tussen de gegevensbron [1] en de wallet). Het is essentieel om te voorkomen dat vertrouwelijke gegevens in verkeerde handen komen en op onjuiste manieren worden gebruikt. Zoals het uitgeven van identiteitsbewijzen en rijbewijzen een overheidstaak is, zou het aanbieden van wallets dat ook moeten zijn. Nu wallet-aanbieders ook private partijen kunnen zijn, moeten aan hen hoge eisen worden gesteld.

4. Een **integer verdienmodel** voor de wallet-aanbieder. Dit sluit aan op het vorige element. Voorkomen moet worden dat de wallets alleen door grote techbedrijven worden aangeboden, omdat een onafhankelijke en integere zelfstandige aanbieder er geen droog brood aan kan verdienen.

5. Voorkoming van **overidentificatie en overvragen** (het onnodig verstrekken van gegevens). Privacy First bepleit extra maatregelen om dit te waarborgen, bijvoorbeeld

[1] Bijvoorbeeld de overheid.

een verbod op gebruik van wallet-aanbieders / identificatiepartijen van buiten het woonland en een verbod op *real name policies* als dat niet nodig is voor het type dienst.

6. Systemen dienen zeker te stellen dat **de ontvangende partijen** hun verplichtingen nakomen (onder andere security, nalaten van overidentificatie en overvragen, tijdig verwijderen).

7. **Toegankelijkheid en een alternatief**: ook de grote groep mensen die onvoldoende digitaal vaardig zijn (dat kunnen ook ondernemers uit het MKB zijn), moeten in staat zijn met de wallets om te gaan en de risico's te begrijpen. Verder dient aan iedereen een bruikbaar alternatief te worden geboden zodat het ook mogelijk is om zonder de wallet te blijven functioneren. Dat is ook relevant voor mensen die niet willen meedoen aan de "digidwang" tot het gebruik van producten/diensten van digitale oligopolisten.

8. **Autonomie** van het walletsysteem, dus ook bruikbaar zonder dure smartphone of tablet met een besturingssysteem (OS) van een van de oligopolisten. Ook de wallet-aanbieders en andere relevante actoren in het eIDAS-systeem dienen aan autonomie-eisen te voldoen en geen advertentiebedrijven te faciliteren.[2]

9. **Controleerbaarheid** van de werking van de wallet en van de verspreiding van gegevens. De wallet dient geen 'black box' te zijn, de broncode van de wallet dient *open source* te zijn en geverifieerd te kunnen worden. De gebruikers en degenen die hun belangen behartigen moeten kunnen verifiëren waar de gegevens terechtkomen.

10. De wallets mogen geen middel worden voor permanente **surveillance** van mensen, noch door de overheid, noch door private partijen zoals banken en grote techbedrijven / advertentiebedrijven.

11. Volwassen **governance** van het systeem, inclusief goede feedback-mogelijkheden zodat onvolkomenheden en risico's snel worden ontdekt; adequate rechtsbescherming.

12. **Handhaving**: het heeft geen zin om mooie theoretische regels te maken als er geen handhaving is.

## Tot slot

Op basis van wat we nu weten is Privacy First er niet zeker van dat aan bovenstaande voorwaarden wordt voldaan. Zolang niet aan deze voorwaarden wordt voldaan is invoering van de EUDI-wallet en Business Wallet in onze optiek onverantwoord.

---

[2] De Europese Commissie faciliteert ten onrechte een advertentiebedrijf, want om de embedded video op de site van de Commissie over de wallet te bekijken, moeten de voorwaarden van Google worden geaccepteerd.