aan	Tweede Kamer der Staten-Generaal, vaste commissie voor Digitale Zaken vaste commissie voor Financiën vaste commissie voor Economische Zaken
cc	Minister van Financiën Minister van Justitie en Veiligheid Minister van Economische Zaken
ons kenmerk	SPF20260601
datum	1 juni 2026
onderwerp	EUDI-wallet, Business Wallet en eIDAS-verordening

Geachte Kamerleden,

Stichting Privacy First heeft kennisgenomen van de brief die de Minister van Financiën op 11 mei jl. inzake de EUDI-wallet aan de Tweede Kamer heeft gestuurd en die zal worden geagendeerd voor het commissiedebat *Digitaliserende overheid* van de commissie Digitale Zaken. Voorts zagen wij het voornemen van de commissie Digitale Zaken om een technische briefing en een rondetafelgesprek over de Business Wallet en de eIDAS-verordening te organiseren. [1] Het antwoord op onze brandbrief van 9 maart jl. over de vrijwilligheid van de EUDI-wallet staat op de agenda van de procedurevergadering van de commissie Financiën d.d. 4 juni as. [2]

Naar aanleiding daarvan vragen wij uw aandacht voor het volgende.

Vrijwilligheid EUDI-wallet

Privacy First heeft op 9 maart jl. een brandbrief gestuurd aan de Minister van Financiën, waarin wij hebben meegedeeld dat in het ontwerp voor de nadere regels ('RTS') op grond

[1] https://www.tweedekamer.nl/kamerstukken/besluitenlijsten/detail?id=2026D23632&did=2026D23632

[2] https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2026A01486

Stichting Privacy First
John M. Keynesplein 10
1066 EP Amsterdam

https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279

KvK 34298157
ANBI erkend

van de antiwitwasverordening (AMLR) door de nieuwe Europese antiwitwasautoriteit (AMLA) de vrijwilligheid van de EUDI-wallet wordt ondergraven.[3] In onze brief hebben we verwezen naar onze reactie in de consultatie van de Europese Banken Autoriteit (EBA) van 6 juni 2025, waarin wij hebben gemeld dat financiële instellingen digitale ondernemingen zijn geworden.

Wij hebben kennisgenomen van de brief van 11 mei jl. aan de Tweede Kamer, waarin de Minister het standpunt inneemt dat die vrijwilligheid niet wordt ondergraven.[4] Het standpunt in de brief van 11 mei jl. is gebaseerd op een formele uitleg van de RTS en de eIDAS-verordening en niet op wat wij in onze brandbrief en in de consultatiereactie aan EBA hebben vermeld. Daarin signaleren wij dat er weliswaar een vrijwilligheidsbepaling in de eIDAS verordening staat, maar dat die bepaling feitelijk wordt ondergraven doordat financiële instellingen (FI's) in Nederland vrijwel geen fysieke kantoren meer hebben en in de praktijk aansturen op digitale identificatie van hun cliënten. Dit standpunt hebben wij in een consultatie van AMLA herhaald. Dit is door de Minister van Financiën genegeerd.

Overigens bevestigt de Europese Banken Federatie (EBF) in hun recente commentaar op de ontwerp-RTS dat de EUDI-wallet verplicht wordt gesteld. [5]

In onze consultatiereactie inzake de Business Wallet hebben wij opnieuw gepleit voor maatregelen om de vrijwilligheid van de wallets te waarborgen. Voor informatie over onze consultatiereacties over eIDAS-onderwerpen verwijzen wij naar bijlagen 1 en 2 bij deze brief.

Ook in andere domeinen dan in de witwasbestrijding kan gaan spelen dat de vrijwilligheid van de eIDAS-wallets feitelijk wordt ondergraven. Wij verwijzen naar de recente publicatie van de Nederlandse School voor Openbaar Bestuur (NSOB) in opdracht van de Alliantie Digitaal Samenleven. [6] In dit rapport wordt gewaarschuwd dat digitalisering het risico vergroot op uitsluiting bij essentiële diensten. In diverse andere rapporten wordt hetzelfde gesignaleerd en wordt onder meer vastgesteld dat een grote groep Nederlanders problemen heeft met internetbankieren.

In een gesprek dat wij zeer recent hadden met medewerkers van het ministerie van Financiën werd door hen gesteld dat er voldoende toegankelijkheidsmaatregelen zouden

---

[3] https://privacyfirst.nl/artikelen/brandbrief-privacy-first-over-verplichtstelling-europese-digitale-identiteit-bij-banken/

[4] *Reactie op verzoek commissie over de brandbrief van Privacy First over verplichtstelling Europese digitale identiteit bij banken*, https://zoek.officielebekendmakingen.nl/kst-1247853

[5] https://www.ebf.eu/ebf-media-centre/updates/ebf-feedback-on-amla-draft-regulatory-technical-standard-on-customer-due-diligence-under-article-281-amlr/

[6] https://www.nsob.nl/overzicht-van-publicaties/toegankelijk-toch

zijn genomen en dat het gebruik van de EUDI-wallet in de financiële sector daadwerkelijk vrijwillig zou zijn. Daar zijn wij het niet mee eens.

Identificatie wordt steeds riskanter

Het onderwerp identificatie is breder dan alleen de EUDI-wallet.

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 (zie bijlage 3). Naar aanleiding daarvan hebben wij in het voorjaar van 2025 een gesprek met medewerkers van het ministerie en DNB gehad. Dit heeft er niet toe geleid dat er maatregelen zijn genomen.

Ook de afgelopen tijd signaleert Privacy First zorgwekkende ontwikkelingen rondom identificatie. Zo hebben wij gezien dat één van de Nederlandse grootbanken haar cliënten zich laat identificeren via het uitlezen van de beveiligde omgeving van het identiteitsbewijs (SE) en het uit de SE ophalen van persoonsgegevens, zoals de foto. In een overzicht van identificatiemethoden gebeurt dit in drie van de vier beschreven varianten (via de bank-app, op kantoor van de bank met een Android telefoon, als er een medewerker van de AMP groep langs komt). Alleen als de cliënt van deze bank gebruikmaakt van Ockto (die in strijd met de AVG via de gegevens van de cliënt inlogt bij MijnOverheid), wordt de DE niet uitgelezen. Wij hebben geen juridische basis kunnen vinden voor de toegang die deze bank tot de SE van het identiteitsbewijs verkrijgt; daarbij maakt de bank gebruik van derden, die de toegang tot de SE feitelijk verkrijgen. Deze bank laat op grote schaal kopieën van identiteitsbewijzen maken en slaat deze langdurig op, te weten tot vijf jaar na het einde van de zakelijke relatie, wat bij banken zeer langdurig is.

Dit zijn voor burgers gevaarlijke praktijken, terwijl de huidige witwaswetgeving niet voorschrijft dat kopieën van identiteitsbewijzen en biometrische persoonsgegevens door banken of andere witwasbestrijdingsplichtigen bewaard moeten worden. Het volstaat op grond van de huidige wet dat de persoonsgegevens (naam, geboortedatum en dergelijke) worden geregistreerd.

In de huidige tijd wordt identificatie voor mensen steeds riskanter. Privacy First begrijpt niet waarom de wetgever geen maatregelen neemt om de risico's te beperken.

Integriteit en ontbreken tegenstrijdig belang in eIDAS-systeem

In onze consultatiereactie inzake de Business Wallet [7] hebben wij de Europese Commissie

[7] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14663-Europese-portemonnee-voor-ondernemingen-digitale-identiteit-veilige-gegevensuitwisseling-en-juridische-kennisgevingen-voor-eenvoudige-digitale-bedrijven/F33399513_nl

er op gewezen dat voor beide soorten eIDAS-wallets geldt dat daarin private partijen een rol kunnen spelen, onder meer als aanbieder van wallets. Opvallend is dat aan die private partijen wel technische en organisatorische eisen worden gesteld, maar dat zij niet worden getoetst op integriteit en het ontbreken van tegenstrijdig belang. Privacy First stelt in de consultatiereactie voor om dit ernstige gebrek in het Europese walletsysteem te verhelpen. Wij stellen voor dat in eIDAS een bepaling wordt opgenomen die aanbieders van essentiële diensten verplicht om fysieke identificatiemogelijkheden aan te bieden naast de EUDI-wallet, zodat de vrijwilligheidsbepaling in eIDAS niet wordt ondergraven.

Vragen over de wallet

Ook als de EUDI-wallet daadwerkelijk vrijwillig zou zijn, heeft Privacy First nog veel vragen:

Hoe wordt voorkomen dat digitale identificatie een hulpmiddel wordt om mensen permanent in de gaten te houden en hun leven te beïnvloeden?

Daar hebben veel mensen zorgen over. Zie bijvoorbeeld de nieuwsbrief van Privacy International (PI) van november 2025 waarin zij schreven:

> *This week, we've been reading stories about how 'identity' is being rebuilt as a system of control. The UK government is piloting live facial recognition at its ports, US border agencies are expanding the same technology to local police and the US Department of Homeland Security wants to collect DNA from not just immigrants, but citizens related to them. Each step tightens the link between who we are and how we're allowed to move. This is a pivotal moment about who gets to exist seamlessly in digital society. The question now becomes whether recognition will serve inclusion, or enforce hierarchy. At PI, we believe these systems are built with malice, not just to enforce, but to target. We also know that once deployed they will expand in scope, and more and more people will be targeted. Governments and industry are building a future of limitless power.*

Wij denken dat die zorgen terecht zijn, als we zien wat er in de VS en het VK gebeurt. [8] Hoe wordt een surveillance-samenleving voorkomen? Hoe wordt gezorgd dat burgers vertrouwen kunnen hebben in de identificatiesystemen? Mooie woorden en basisconcepten die er redelijk uitzien, zijn niet voldoende.

Hoe wordt geborgd dat de ontvangende partijen ('relying parties') niet overvragen? (Voorkoming van overidentificatie.)

[8] Zie bijvoorbeeld over de VS: *Uncle Sam wants to scan your iris and collect your DNA, citizen or not*, en *DHS Gives Local Cops a Facial Recognition App To Find Immigrants*, (waarbij iedereen wordt gescand). In het VK zijn er ook voorbeelden, niet alleen de Offline Safety Act met haar uitwassen maar ook *UK Home Office live facial recognition adoption begins with POC at ports*.

In het huidige eIDAS-systeem hoeft de ontvangende partij alleen op te geven welke gegevens ('datapunten') zij uit de wallet willen opvragen. Waarom wordt hier geen toezicht op gehouden?

Wordt in de wallets ingebouwd dat ontvangers niet meer vragen dan zij eerder hebben opgegeven? Als dit niet goed is geregeld, is dit naar de mening van Privacy First een lek in het systeem.

Waar komen de gegevens terecht?

Op welke manier wordt er voor gezorgd dat burgers, maar ook burgerrechtenorganisaties, in beeld hebben bij welke organisaties en personen (zowel privaat als publiek) de persoonsgegevens terechtkomen? Achtergrond: de trend is dat persoonsgegevens (inclusief identiteitsgegevens) zich op steeds grotere schaal verspreiden, terwijl tegenwicht ontbreekt, bijvoorbeeld omdat mensen niet eens weten waar hun gegevens rondslingeren. Nu al worden persoonsgegevens op grote schaal verspreid zonder dat burgers en kleine organisaties daar zicht op hebben, bijvoorbeeld als gevolg van de antiwitwasregels en de regels ter bestrijding van terrorismefinanciering (wat betekent dat de gegevens bij ongecontroleerde private partijen en bij hun leveranciers terechtkomen).

Wat is het verdienmodel van de walletaanbieders?

Wij komen berichten tegen dat het moeilijk is om geld te verdienen met wallets. Waarom zouden private partijen dit willen doen als er niets aan verdiend kan worden? Waarom is het uitgeven van wallets niet een publieke taak, zoals het uitgeven van paspoorten?

Is de walletprovider integer?

Hoe wordt er voor gezorgd dat klanten een keuze kunnen maken voor een integere partij, die gegevensbescherming en techniek op orde heeft? Wordt er rekening mee gehouden dat klanten een onveilige keuze gaan maken die goedkoop en 'makkelijk' is? Moet er niet voor gezorgd worden dat onveilige keuzes onmogelijk zijn?

Is sprake van autonomie?

Is de wallet te gebruiken zonder apparaat met een besturingssysteem van grote ondernemingen van buiten de EU / Big Tech (= Microsoft, Google, Apple c.s.)? Vergelijk de recente waarschuwing van DNB/AFM over digitale autonomie.[9] Worden onafhankelijke Nederlandse initiatieven zoals Yivi [10] bevorderd?

---

[9] https://www.afm.nl/nl-nl/sector/actueel/2025/okt/pb-digitale-autonomie

[10] https://yivi.app/ . Yivi heette voorheen IRMA en won in 2018 de allereerste Nederlandse Privacy Award.

Hoe wordt overidentificatie en te lang bewaren tegengegaan?

Komt er regelgeving om toekomstige onnodige identificatie te bestrijden?

Komt er regelgeving om de huidige excessieve identificatieplichten en bewaarplichten terug te draaien, bijvoorbeeld in de witwasbestrijding en bij platformaanbieders? Voorbeelden: de kopie ID's die hotels eisen; de Spaanse toeristenregels die eisen dat bepaalde aanbieders het hemd van het lijf vragen van hun hotel- en campinggasten.

Wordt er bij het ontwikkelen van de wallets gedacht aan mensen met beperkte digitale vaardigheden?

Het is ons opgevallen dat bij het thema 'toegankelijkheid' vooral wordt gedacht aan mensen met fysieke of andere beperkingen en niet aan de vele mensen met beperkte digitale vaardigheden. Zij lopen extra risico bij het gebruik van een EUDI-wallet.

Hoe zit het met de governance, feedback en rechtsbescherming?

Hoe wordt er voor gezorgd dat de belangen van klanten worden behartigd in dit systeem? Welke feedback mogelijkheden zijn er voor klanten en hoe wordt er voor gezorgd dat er iets mee wordt gedaan? Komen er laagdrempelige rechtsbeschermingsmogelijkheden voor klanten? Op welke manier wordt de handhaving ingericht? Krijgen de overheidstoezichthouders meer middelen om snel achter overtredingen aan te gaan?

Tot slot

Privacy First hoopt dat u het onderwerp identificatie in brede zin zult agenderen, aangezien de risico's op dit moment disproportioneel toenemen, niet alleen door digitale criminaliteit, maar ook door onveilige praktijken van degenen die identificeren. Het zou fijn zijn als onze vragen worden beantwoord en onze zorgen worden weggenomen.

Wij zijn graag bereid een en ander nader toe te lichten en hopen dat u aandacht aan deze brief zult besteden. Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,
namens Stichting Privacy First,

Vincent Böhre
directeur

Bijlage 1 - Privacy First publicaties inzake eIDAS, EUDI-wallet en Business Wallet

6 juni 2025	Deelname aan de consultatie van de Europese Banken Autoriteit (EBA) over de nieuwe klantenonderzoeksregels op grond van de antiwitwasverordening (AMLR): artikel Implementatieregels dienen de nadelen van antiwitwasregels te beperken [11], artikel Digitale identiteit wordt sluipenderwijs toch verplicht [12], consultatiereactie.[13]
5 mei 2026	Deelname aan de consultatie van de Europese Commissie inzake de Business Wallet: consultatiereactie.[14]
6 mei 2026	Deelname aan de consultatie van de nieuwe Europese antiwitwasautoriteit (AMLA) over de nieuwe klantenonderzoeksregels op grond van de antiwitwasverordening (AMLR). Aangezien onze reactie niet online is bekendgemaakt, is in bijlage 2 de passage over de EUDI-wallet opgenomen.

[11] https://privacyfirst.nl/artikelen/implementatieregels-dienen-de-nadelen-van-antiwitwasregels-te-beperken/

[12] https://privacyfirst.nl/artikelen/digitale-identiteit-wordt-sluipenderwijs-toch-verplicht/

[13] https://privacyfirst.nl/wp-content/uploads/Privacy-First-response-EBA-consultation-on-additional-AMLR-rules-June-2025.pdf

[14] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14663-Europese-portemonnee-voor-ondernemingen-digitale-identiteit-veilige-gegevensuitwisseling-en-juridische-kennisgevingen-voor-eenvoudige-digitale-bedrijven/F33399513_nl

Bijlage 2 - Passage over de EUDI-wallet in onze reactie van 6 mei 2026 op het AMLA consultatieverzoek

Citaat:

Article 7

In the Netherlands, it is becoming increasingly common for large organisations to no longer require any form of physical identification. Even when they do accept physical identification, they wish to read the NFC chip on the ID card and store the personal data indefinitely (up to five years after the end of the business relationship), with all the associated data protection risks. These are undesirable practices, given that a large group of Dutch people lack sufficient digital skills and another group refuses to use products and services from IT suppliers outside the EU (autonomy).

Responsibility of the European financial legislator for data protection and respecting fundamental rights

Please note that with regard to the scope of data obliged entities are required to collect and retain for long periods, the basis lies in the European AML-CFT rules. AMLA and the European Commission cannot refer to data protection authorities (national or European) for data protection aspects. The European AML/CFT rules, including the additional rules ('RTS') you are preparing, will have to ensure that citizens' fundamental rights are respected and that data protection safeguards are incorporated.

European Accessibility Act

Also relevant in this context is the European Accessibility Act (EAA), which entered into force on 28 June 2025. This directive requires obliged entities to ensure that their services are accessible to every citizen. The Dutch EAA regulator, the Netherlands Authority for the Financial Markets (AFM), recently revealed (https://www.afm.nl/nl-nl/sector/actueel/2025/apr/sb-eaa-update%201) that a significant part of the Dutch population (5.5 million people, 32%) has disabilities and/or is insufficiently digitally literate (it cannot be expected that those digital skills will increase significantly through training and education). This group of people is at extra high risk of personal data misuse, which means they are also at extra risk if obliged entities demand personal data from them as part of an AML/CFT investigation. One of the most high-risk activities for this group is identity verification.

Increasing cybersecurity risks related to financial services

On top of this, the Netherlands has for quite some time seen an increase in fraud around financial services, fraud for which financial institutions are not liable because the customer himself made the mistake. Cybersecurity risks will grow exponentially as a result of the rise of artificial intelligence and threaten the security of customers of obliged entities. Those

customers make those mistakes because of their limited digital skills. Privacy First believes that the limited skills of a large part of the Dutch population (as mentioned in the EAA passage above) should be taken into account when designing the AML/CFT rules. Those rules should ensure that people do not fall into the trap of criminals when asked for KYC information.

The consequences

Privacy First advises that physical identification should also be offered in non-face-to-face situations

Our primary comment: the draft RTS do not adequately reflect the eIDAS principle of non-mandatory use of the electronic identity.

For verification of a customer in a non-face-to-face context, Article 7(1) of the draft RTS requires that obliged entities use electronic identification means. According to Article 7(2) only in cases where no electronic identification means are available or they cannot reasonably be expected to be provided, obliged entities shall acquire the customer s identity document (or equivalent) using other remote solutions, mentioning that any alternative solution shall be commensurate to the size, nature and complexity of the obliged entity s business and its exposure to ML/TF risks.

The customer of the obliged entity is not mentioned at all!

Article 7 is not in line with the explicit principle laid down in Regulation (EU) No 910/2014 (the eIDAS Regulation) that the use of eIDAS compliant solutions shall be voluntary and that access to public and private services, and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use these solutions.

The non-mandatory character of eIDAS compliant solutions means that it is always the voluntary choice of the relevant natural or legal person to (not) use the digital identity. The decision whether to use or not use the electronic identity is free and can consequently not be made mandatory by imposing an obligation on public or private service providers to require electronic identification as a standard in non-face-to-face contexts. Imposing such an obligation would effectively render the use of electronic identification mandatory and make this principle of the eIDAS regulation illusory.

Privacy First advises that the current version of Article 7 is deleted from the draft RTS.

Any approach that makes the use of digital identity dependent on public or private entities assessment or willingness to accept a digital identity, as supposed in Article 7(3) of the draft RTS, is not voluntary. A customer s decision to use or not use an electronic identity can only depend on the customer s own choice.

Also relevant in this context is the EAA and the large number of people in the EU who have limited digital skills. As financial institutions and some other OE's have evolved into digital enterprises without offices accessible to customers, major problems arise for all the people with limited digital skills.

Further measures are necessary to limit the data protection risks.

Privacy First proposes that the AMLA creates a new draft of Article 7 expressing:

* the use of an eIDAS solution and remote solutions shall only take place on a completely voluntary basis and if such a solution is used, it is the responsibility of the obliged entity to verify that the person that is going to use this solution understands the risks of the digital mode of operation;

* a physical alternative shall always be offered at a trusted party, with the customer being enabled to verify the reliability of that party and the reliability of the equipment used;

* biometrical data are deleted immediately after the verification has taken place, the OE's do not record biometrical data.

The risks of remote solutions, described under Article 7 paragraphs 2-4 of the draft RTS are high

Privacy First is of the opinion that the level of protection of remote solutions, described under Article 6 paragraphs 2-4 of the draft RTS is insufficient, as it is based on biometric information of the customer that can easily be harvested by criminal parties and misused. Incidentally, it is not sure that eIDAS solutions are secure and there is a lot of criticism on the system.

Read the article by the *Verbraucherzentrale Bundesverband* (vzbv), https://www.vzbv.de/pressemitteilungen/digitale-identitaet-verbraucherinnen-muessen-digitalen-brieftaschen-vertrauen and the position and report. Expert Jaap-Henk Hoepman published: *Feedback on the consultation on the eID implementing regulations*, https://blog.xot.nl/2024/09/05/feedback-on-the-consultation-on-the-eid-implementing-regulations/index.html. Dutch newspaper NRC published an interview with expert Denis Roio: *Europese digitale identiteit is straks niet veilig genoeg, waarschuwen experts*, https://www.nrc.nl/nieuws/2024/12/22/europese-digitale-identiteit-is-straks-niet-veilig-genoeg-waarschuwen-experts-a4877532.

Also playing a role here is that a significant proportion of the EU population has inadequate digital abilities and the EAA requires that this is taken into account.

For our opinion on the voluntary character of the eIDAS solutions we also refer to our consultation response regarding the Business Wallet, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14663-Europese-portemonnee-voor-

ondernemingen-digitale-identiteit-veilige-gegevensuitwisseling-en-juridische-kennisgevingen-voor-eenvoudige-digitale-bedrijven/F33399513_nl.

Bijlage 3 - Privacy First activiteiten inzake identificatie

Privacy First is al langere tijd met het onderwerp identificatie bezig en heeft in september 2024 de minister van Financiën en De Nederlandsche Bank (DNB) aangeschreven met het verzoek om wetgevende maatregelen vanwege de onveilige identificatiepraktijken in de financiële sector.

Meer informatie: zie ons artikel Privacy First verzoekt De Nederlandsche Bank en Minister van Financiën om aanpassing identificatiepraktijken van financiële instellingen ; [15]

zie tevens ons verzoek met een uitvoerige toelichting (pdf).[16]

Naar aanleiding van ons verzoek hebben wij in het voorjaar van 2025 een gesprek gehad met medewerkers van het ministerie en DNB. Dit heeft niet geleid tot maatregelen of verbeteringen.

[15] https://privacyfirst.nl/artikelen/privacy-first-verzoekt-aanpassing-identificatiepraktijken-van-financiele-instellingen/

[16] https://privacyfirst.nl/wp-content/uploads/Wwft_identificatie_verzoek_PrivacyFirst_sept2024.pdf