Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2026-2027

36 890 Digitaal pakket van de Europese Commissie COM(2025)835, COM(2025)836, COM(2025)837, COM(2025)838

AJ **VERSLAG VAN EEN NADER SCHRIFTELIJK OVERLEG**
Vastgesteld 17 november 2026

De vaste commissies voor Digitalisering[1] en voor Economische Zaken / Klimaat en Groene Groei[2] hebben nader schriftelijk overleg gevoerd met de staatssecretaris van Economische Zaken en Klimaat de staatssecretaris Digitale Economie en Soevereiniteit over **het voorstel voor een Verordening tot instelling van Europese portemonnees voor ondernemingen.**[3] Bijgaand brengen de commissies hiervan verslag uit. Dit verslag bestaat uit:

- De uitgaande brief van 14 oktober 2026.
- De antwoordbrief van 17 november 2026.

De griffier voor dit verslag,
Van Dooren

[1] Samenstelling:
Baumgarten (JA21), Beukering (Fractie-Beukering), Fiers (PRO), Van Gasteren (Fractie-Van Gasteren), Goossen (BBB), Hartog (Volt), Van Hattem (PVV), Janssen (SP), Kanis (D66), Lievense (BBB), Van Meenen (D66), Musa (VVD), Nicolaï (PvdD), Van den Oetelaar (FVD), Panman (BBB) (ondervoorzitter), Petersen (VVD), Ramsodit (PRO), Recourt (PRO), Van Rooijen (50PLUS), Roovers (PRO), Van de Sanden (Fractie-Van de Sanden), Steenkamp (CDA), Talsma (ChristenUnie), Veldhoen (PRO) (voorzitter), Visseren-Hamakers (Fractie-Visseren-Hamakers), De Vries (SGP), Walenkamp (Fractie-Walenkamp)
[2] Samenstelling:
Van Aelst-den Uijl (SP), Van Ballekom (VVD), Baumgarten (JA21), Beukering (Fractie-Beukering), Bovens (CDA), Crone (PRO), Dessing (FVD), Van Gasteren (Fractie-Van Gasteren), Van der Goot (OPNL), Van Gurp (PRO), Holterhues (ChristenUnie), Karaaslan (D66), Kluit (PRO) (voorzitter), Kroon (BBB), Van Langen-Visbeek (BBB) (ondervoorzitter), Van Meenen (D66), Panman (BBB), Perin-Gopie (Volt), Petersen (VVD), Van Rooijen (50PLUS), Van de Sanden (Fractie-Van de Sanden), Schalk (SGP), Steenkamp (CDA), Straus (VVD), Van Strien (PVV), Thijsssen (PRO), Visseren-Hamakers (Fractie-Visseren-Hamakers), Walenkamp (Fractie-Walenkamp)
[3] Zie E-dossier E260004.

BRIEF VAN DE VOORZITTERS VAN DE VASTE COMMISSIES VOOR DIGITALISERING EN VOOR ECONOMISCHE ZAKEN / KLIMAAT EN GROENE GROEI

Aan de staatssecretaris Digitale Economie en Soevereiniteit

Den Haag, 14 oktober 2026

De commissies Digitalisering en Economische Zaken / Klimaat en Groene Groei hebben met belangstelling kennisgenomen van uw brief van 19 augustus 2026 met de beantwoording van de nadere vragen over het voorstel voor een Verordening tot instelling van Europese portemonnees voor ondernemingen (COM(2025)838), ook wel EU Business Wallet (hierna: EBW) genoemd.[4] Naar aanleiding hiervan hebben de leden van de fractie van **PRO** nog enkele vervolgvragen.

Kent u het artikel “One wallet, 27 systems: can the EU build an untraceable Digital ID?”[5] Kunt u ingaan op de belangrijkste kritiekpunten uit het artikel rondom digitale veiligheid, betrokkenheid van de wetenschap en maatschappelijke organisaties, traceerbaarheid van burgers en privacy en grensoverschrijdende werking?

U verwijst in antwoord op vraag één naar het document SWD(2025) 837 final. Daar konden de leden van de fractie van PRO niet direct de onderbouwing vinden voor de marktwerking, behalve dat in hoofdstuk vijf de mogelijke oplossingsrichtingen zijn meegenomen dat het goed zou zijn als de EBW *business* zou kunnen opleveren. Zoals u zelf al schrijft kan marktwerking voordelen hebben, maar dat hoeft niet. Het kan ook tot versplintering in dienstverlening, extra controles en hoge winstuitkeringen leiden en voor bedrijven dus juist leiden tot extra kosten. Kunt u daarom inhoudelijk beter onderbouwen waarom u in deze strategische stap voor de administratie van bedrijven niet kiest voor honderd procent staatseigendom? Wat zijn de nadelen van die route die niet zouden opwegen tegen de nadelen van martkwerking?

Bij de beantwoording van vraag tien wordt geschetst hoe het overlegcircuit eruit ziet rond de EBW. De vragen “Zijn de mandaten, gezamenlijke doelen, termijnen en escalatieroutes helder?” en “Kunt u dit aan deze leden inzichtelijk maken?” worden echter niet beantwoord. Daarom stellen deze leden de vraag: Kunt u de verdeling van mandaten, doelen, termijnen en escalatieroutes delen?

Kunt u aangeven welke extra menskracht en middelen ter beschikking worden gesteld aan de Rijksinspectie Digitale Infrastructuur om de extra taken rond de EBW uit te voeren? Kunt u aangeven wanneer deze extra inzet operationeel moet zijn en hoe zich dat verhoudt tot de start van de EBW?

Heeft Logius recent een actuele uitvoeringstoets afgegeven? Zo ja, kunt u deze met de Kamer delen?

---

[4] *Kamerstukken I* 2025/26, 36.890, AA
[5] “One wallet, 27 systems: can the EU build an untraceable Digital ID?”, euronews.nl, 17 september 2026.

In antwoord op vraag dertien stelt u: “Maatregelen die veilige toegang bieden aan gebruikers zonder Google-account of Apple-ID zullen worden onderzocht en, indien dat veilig kan, worden geïmplementeerd voordat de publieke EDI-wallet beschikbaar komt voor gebruikers.”[6] Het hele punt van de leden van de fractie van PRO is echter dat verplicht gebruik van Google of Apple voor gebruikers juist bewezen niet veilig is. Recente voorbeelden waarbij personen en organisaties vanwege politieke voorkeuren van de President van Amerika op sanctielijsten worden gezet, laten zien dat er voor burgers en bedrijven tegenwoordig grote en soms onverantwoorde geopolitieke risico’s aan het gebruik van Amerikaanse tech zitten. Wat gaat u doen om te garanderen dat bedrijven en burgers onafhankelijk kunnen blijven van extraterritoriale techniek, die onverwacht en buitenrechtelijk tegen hen ingezet kan worden?

Bent u bekend met de kritiek van Stichting Privacy First, zoals verwoord in hun brief en in het artikel: “Privacy first eist actie van Tweede Kamer tegen digitale wallet”?[7] Daarin wordt gesteld dat twee EU-verordeningen, de eIDAS, waar de antiwitwasautoriteit ‘*Authority for Anti-Money Laundering and Countering the Financing of Terrorism’* (AMLA) uit voortvloeit, en de verordening waar de EBW uit voortvloeit, botsen qua vrijwilligheid van het gebruik van de digitale identiteit en wallet. Hoewel vrijwillige inzet de norm zou moeten zijn, wordt het vrijwel onmogelijk om een bankrekening te openen voor mensen die geen gebruik wensen te maken van de EBW. Kunt u ingaan op de twee resterende kritiekpunten:
a. Gebrek aan screening: aanbieders van de identificatie-wallets worden vooraf niet streng gescreend op integriteit of het ontbreken van tegenstrijdige (commerciële) belangen.
b. Risico op overidentificatie: er ontbreken harde technische waarborgen die voorkomen dat ontvangende partijen, zoals bedrijven, onnodig veel persoonsgegevens opvragen en opslaan.

De vaste commissies voor Digitalisering en Economische Zaken / Klimaat en Groene Groei zien met belangstelling uit naar uw reactie en ontvangen deze graag binnen vier weken na dagtekening van deze brief.

De voorzitter van de commissie Digitalisering
G.V.M. Veldhoen

De voorzitter van de commissie Economische Zaken & Klimaat en Groene Groei
S.M. Kluit

[6] Kamerstukken I 2025/26, 36.890, AA, p. 9.
[7] “Privacy first eist actie van Tweede Kamer tegen digitale wallet”, dutchitleaders.nl, 6 juni 2026; “Brandbrief Privacy First over verplichtstelling Europees digitale identiteit bij banken”, privacyfirst.nl, 9 maart 2026.

BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 17 november 2026

Hierbij zend ik u de antwoorden op de verdere vervolgvragen van de leden van de fractie van PRO over het voorstel van de Europese Commissie voor een verordening tot instelling van Europese portemonnees voor ondernemingen (COM(2025) 838). Deze beantwoording volgt op twee eerdere sets vragen, waarvan de beantwoording op respectievelijk 24 april 2026 (Kamerstukken I 2025/2026, 36.890, R) en 19 augustus 2026 (Kamerstukken I 2025/2026, 36.890, AA) met uw Kamer is gedeeld.

W.J.M. Aerdts
Staatssecretaris van Economische Zaken en Klimaat

182671

Vragen van de leden van de fractie van PRO.

1.
Kent u het artikel “One wallet, 27 systems: can the EU build an untraceable Digital ID?” Kunt u ingaan op de belangrijkste kritiekpunten uit het artikel rondom digitale veiligheid, betrokkenheid van de wetenschap en maatschappelijke organisaties, traceerbaarheid van burgers en privacy en grensoverschrijdende werking?

Antwoord vraag 1:
Het is belangrijk Europese Digitale Identiteit (EDI)-wallets te onderscheiden van Europese Business Wallets (EBW). EDI-wallets zijn apps voor burgers, EBW zijn gecombineerde vertrouwensdiensten beschikbaar voor bedrijven. De herziene eIDAS-verordening[8] creëert een raamwerk voor EDI-wallets, waarbinnen lidstaten nationaal EDI-wallets uitgeven of erkennen. Specifiek voor bedrijven is de verordening voor EBW door de Europese Commissie geïntroduceerd op 19 november 2025. De EBW-verordening bouwt voort op de eIDAS-verordening en bevindt zich nog in de onderhandelfase. Vorige maand (oktober 2026) zijn de eerste trilogen over dit wetsvoorstel begonnen.

Ik ben bekend met het artikel en ook de analyses en open brieven van *epicenter.works* en *EDRi*. In het artikel worden belangrijke risico's geadresseerd die de introductie van het Europese Raamwerk voor Digitale Identiteit, met daarin EDI-wallets, met zich meebrengt. Het kabinet is zich terdege bewust van deze risico's en zet zich zowel nationaal als Europees in voor de maatregelen die nodig zijn om deze te beheersen.

Het EDI-stelsel wordt een digitaal fundament voor digitale dienstverlening en, in bepaalde gevallen, ook fysieke dienstverlening. Binnen dit stelsel kunnen burgers die dat willen zich identificeren en gegevens delen met aangesloten publieke en private organisaties. EDI-wallets staan onder exclusieve controle van de burger en vervullen hierin een sleutelrol door gegevensaanbieders en gegevensafnemers met elkaar te verbinden. Daarbij is het van belang dat de aangesloten diensten ook toegankelijk blijven voor mensen die geen EDI-wallet willen gebruiken.

Het EDI-stelsel is bedoeld om breed inzetbaar te zijn en dienstverlening in uiteenlopende sectoren te ondersteunen, waaronder vervoer, energie, het bankwezen, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs en telecommunicatie. Dat biedt kansen, maar brengt ook risico's met zich mee. De gevolgen van beveiligingsincidenten, fouten of uitval van het EDI-stelsel kunnen groot zijn. Daarom hecht Nederland belang aan een zorgvuldige implementatie, waarbij in de hele EU hoge eisen worden gesteld aan de veiligheid en betrouwbaarheid van zowel EDI-wallets als de aangesloten diensten. Het kabinet zet zich daarom samen met andere lidstaten in voor zo hoog mogelijke en geharmoniseerde beveiligingsnormen en voor de totstandkoming van Uniebrede cybersecuritycertificering.

Naast digitale veiligheid is de bescherming van de privacy van burgers belangrijk. Het artikel wijst op het risico van overidentificatie: doordat identificatie met een EDI-wallet eenvoudig en laagdrempelig wordt, zouden organisaties vaker om identificerende persoonsgegevens kunnen vragen, ook wanneer dat niet noodzakelijk is. Het kabinet onderkent dit risico en zet zich samen met andere lidstaten voortdurend in om dit risico door op EU-niveau verankerde maatregelen te mitigeren.

[8] 'eIDAS' staat voor 'electronic Identities And trust Services'

De eIDAS-verordening bevat daarom, in aanvulling op de Algemene verordening gegevensbescherming (AVG), verschillende waarborgen.
Zo is het gebruik van een EDI-wallet vrijwillig en blijft het recht op alternatieve toegang tot dienstverlening bestaan. Daarnaast voorziet de verordening ook in het recht om pseudoniemen te gebruiken wanneer geen wettelijke identificatieplicht bestaat.

Het kabinet zet zich in voor de komst van een geharmoniseerde methode voor pseudoniemen en draagt bij aan de ontwikkeling van een Europese standaard hiervoor. Ook moeten organisaties die gegevens opvragen transparant zijn over welke gegevens zij voor welke dienstverlening willen ontvangen en deze informatie in een centraal openbaar register laten vastleggen voordat zij van een EDI-wallet gebruik kunnen maken. Het kabinet heeft zich succesvol ingezet voor de toevoeging van een technische maatregel die iedere EDI-wallet in staat stelt de naleving van deze registratie te toetsen.

Het artikel benoemt daarnaast het risico dat online gedrag van burgers traceerbaar kan zijn. Ook dit risico neemt het kabinet serieus. De eIDAS-verordening bevat waarborgen om de traceerbaarheid van het gebruik van EDI-wallets tegen te gaan. Bij het ontwerp van het nationale stelsel en de publieke wallet hanteert het kabinet het principe *privacy-by-design*. Het systeem wordt zo ontworpen dat geen enkele partij behalve de burger inzicht heeft in het gebruik van de wallet. Tegelijkertijd moet wel worden gezorgd dat burgers zo goed mogelijk geholpen kunnen worden wanneer zij in de problemen komen.
Gelet op deze risico's hecht het kabinet grote waarde aan een beheerste en gefaseerde implementatie van het EDI-stelsel. Daarbij moeten de veiligheid, betrouwbaarheid en bescherming van publieke waarden steeds leidend zijn. Alleen op die manier kan een digitaal fundament ontstaan waarop burgers, bedrijven en overheden daadwerkelijk veilig kunnen bouwen.

Tot slot onderschrijft het kabinet het belang van transparantie en onafhankelijke toetsing door de wetenschap en maatschappelijke organisaties, zoals ook in het artikel wordt bepleit. Bij de nationale implementatie van het EDI-stelsel vindt daarom regelmatig overleg plaats met wetenschappelijke en maatschappelijke partijen. Binnenkort worden de concept-eisen waaraan EDI-wallets bij certificering moeten voldoen ter openbare consultatie aangeboden, zodat belanghebbenden hierop kritisch kunnen reflecteren. Daarnaast wordt de broncode van EDI-wallets openbaar beschikbaar gesteld, zoals ook het geval is bij de Nederlandse Publieke wallet.[9] Daarmee worden onafhankelijke onderzoekers en maatschappelijke organisaties in staat gesteld de technische implementatie en de daaraan gestelde eisen te onderzoeken en van feedback te voorzien. Deze transparantie en onafhankelijke toetsing vormen een belangrijke aanvulling op de formele certificering en beveiligingsonderzoeken die onder meer walletaanbieders straks moeten ondergaan en dragen bij aan een zorgvuldige en verantwoorde invoering van het EDI-stelsel.

2.
U verwijst in antwoord op vraag één naar het document SWD(2025) 837 final. Daar konden de leden van de fractie van PRO niet direct de onderbouwing vinden voor de marktwerking, behalve dat in hoofdstuk vijf de mogelijke oplossingsrichtingen zijn meegenomen dat het goed zou zijn als de EBW *business* zou kunnen opleveren. Zoals u zelf al schrijft kan marktwerking voordelen hebben, maar dat hoeft niet. Het kan ook tot versplintering in dienstverlening, extra controles en hoge winstuitkeringen

[9] GitHub - MinBZK/nl-wallet: NL Wallet - A digital identity wallet provided by the government. · GitHub

leiden en voor bedrijven dus juist leiden tot extra kosten. Kunt u daarom inhoudelijk beter onderbouwen waarom u in deze strategische stap voor de administratie van bedrijven niet kiest voor honderd procent staatseigendom? Wat zijn de nadelen van die route die niet zouden opwegen tegen de nadelen van marktwerking?

Antwoord vraag 2:
De Europese Commissie kiest voor een marktgedreven benadering om innovatie te stimuleren en dienstverlening mogelijk te maken die aansluit bij de behoeften en omvang van verschillende organisaties. Zo kunnen kleinere mkb-bedrijven desgewenst kiezen voor een meer laagdrempelig, goedkoper en eenvoudig te integreren alternatief, terwijl grotere ondernemingen kunnen kiezen voor een diep geïntegreerd systeem met uitgebreidere functionaliteiten. Het voorstel waarborgt tegelijkertijd dat alle kernfunctionaliteiten voor alle EBW's beschikbaar zijn en stelt gemeenschappelijke eisen aan onder meer interoperabiliteit en betrouwbaarheid. Het kabinet steunt deze benadering, omdat zij gemeenschappelijke Europese randvoorwaarden combineert met ruimte voor innovatie en maatwerk door aanbieders. De EBW's zijn daarnaast grotendeels gebaseerd op de gekwalificeerde vertrouwensdiensten, waarvoor reeds ruim 10 jaar aanbieders vanuit de markt – in tegenstelling tot de overheid - veel ervaring hebben. Een volledig publiek stelsel zou bovendien (structurele) publieke investeringen vergen in de ontwikkeling, het beheer, het onderhoud en de beveiliging van de EBW's.

3.
Bij de beantwoording van vraag tien wordt geschetst hoe het overlegcircuit eruit ziet rond de EBW. De vragen "Zijn de mandaten, gezamenlijke doelen, termijnen en escalatieroutes helder?" en "Kunt u dit aan deze leden inzichtelijk maken?" worden echter niet beantwoord. Daarom stellen deze leden de vraag: Kunt u de verdeling van mandaten, doelen, termijnen en escalatieroutes delen?

Antwoord vraag 3:
Voor de EBW geldt dat de voorgestelde verordening momenteel nog in onderhandeling is tussen het Europees Parlement, de Raad en de Europese Commissie. De verordening is dus nog niet formeel vastgesteld. Wel heb ik opdracht gegeven tot het uitvoeren van een onderzoek naar de te verwachten uitvoeringslasten voor Nederlandse publieke dienstverleners. Op basis van de uitkomsten daarvan kunnen nadere stappen voor de nationale uitvoering worden bepaald.

Voor EDI-wallets geldt dat de herziene eIDAS-verordening reeds in werking is en deze de gezamenlijke doelen en termijnen bepaalt en ook aangeeft welke mandaten er nationaal geregeld moeten worden. De eIDAS-verordening is rechtstreeks toepasselijk in Nederland. Wel is het nodig om de verordening nationaal op een aantal onderdelen verder te operationaliseren. Zo dient een toezichthouder aangewezen te worden en dient de inrichting en het beheer van een register voor vertrouwende partijen geregeld te worden. Het kabinet bereidt hiertoe een uitvoeringswet voor. Bij de voorbereidingen voor de nationale implementatie wordt aangesloten op de *governance* van het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO), de mandaten en doelen uit de meerjarenroadmap van de Programmeringsraad Generieke Digitale Infrastructuur (PGDI), en termijnen en escalatieroutes die daarmee samenhangen.

4.
Kunt u aangeven welke extra menskracht en middelen ter beschikking worden gesteld aan de Rijksinspectie Digitale Infrastructuur om de extra taken rond de EBW uit te voeren? Kunt u aangeven wanneer deze extra inzet operationeel moet zijn en hoe zich dat verhoudt tot de start van de EBW?

Antwoord vraag 4:
De EBW-verordening is nog niet formeel vastgesteld, zie het antwoord op vraag 3. Ik ben in goed contact met de RDI om waar al mogelijk voorbereidingen te treffen voor de komst van de EBW. De RDI kan echter pas een volledige uitvoeringstoets voltooien wanneer de verordening formeel is vastgesteld en alle technische specificaties uitgekristalliseerd zijn.

5.
Heeft Logius recent een actuele uitvoeringstoets afgegeven? Zo ja, kunt u deze met de Kamer delen?

Antwoord vraag 5:
Nee, Logius heeft nog geen uitvoeringstoets uitgevoerd. Dat geldt zowel voor de EDI-wallets als de EBW's. De uitvoeringstoets voor EDI-wallets wordt uitgevoerd zodra de concept-uitvoeringswet voor de eIDAS revisie beschikbaar is.

6
In antwoord op vraag dertien stelt u: "Maatregelen die veilige toegang bieden aan gebruikers zonder Google-account of Apple-ID zullen worden onderzocht en, indien dat veilig kan, worden geïmplementeerd voordat de publieke EDI-wallet beschikbaar komt voor gebruikers." Het hele punt van de leden van de fractie van PRO is echter dat verplicht gebruik van Google of Apple voor gebruikers juist bewezen niet veilig is. Recente voorbeelden waarbij personen en organisaties vanwege politieke voorkeuren van de President van Amerika op sanctielijsten worden gezet, laten zien dat er voor burgers en bedrijven tegenwoordig grote en soms onverantwoorde geopolitieke risico's aan het gebruik van Amerikaanse tech zitten. Wat gaat u doen om te garanderen dat bedrijven en burgers onafhankelijk kunnen blijven van extraterritoriale techniek, die onverwacht en buitenrechtelijk tegen hen ingezet kan worden?

Antwoord vraag 6:
Om te komen tot een betrouwbaar stelsel van EDI-wallets moeten maatregelen worden getroffen tegen verschillende dreigingen. Eén van de dreigingen is dat malafide partijen middels phishing en malware proberen om identiteitsfraude te plegen en/of persoonsgegevens te verkrijgen, waardoor bescherming tegen malafide apps nodig is. Voor gebruikers die van Apple- en Google-producten gebruik maken, zijn daarvoor reeds maatregelen getroffen. Voor gebruikers die niet van die platformen gebruikmaken, wordt nog onderzocht hoe daartegen het beste kan worden beschermd.

Een andere mogelijke dreiging is de afhankelijkheid van extraterritoriale techniek. Die dreiging is met de introductie van EDI-wallets niet geheel weg te nemen. Het marktaandeel van smartphones van aanbieders van landen buiten de EU is immers heel groot. Het voornemen is om ook ondersteuning te bieden aan gebruikers die niet van die aanbieders gebruik willen maken. Dit draagt eraan bij de afhankelijkheid van die aanbieders te verminderen. Gebruikers van EDI-wallets kunnen dan, als zij dat willen, gebruik maken van een andere aanbieder dan wel op een later moment overstappen op een platform van een andere aanbieder.

7
Bent u bekend met de kritiek van Stichting Privacy First, zoals verwoord in hun brief en in het artikel: "Privacy first eist actie van Tweede Kamer tegen digitale wallet"? Daarin wordt gesteld dat twee EU-verordeningen, de eIDAS, waar de antiwitwasautoriteit '*Authority for Anti-Money Laundering and Countering the Financing of Terrorism'* (AMLA) uit voortvloeit, en de verordening waar de EBW uit voortvloeit, botsen qua vrijwilligheid van het gebruik van de digitale identiteit en wallet. Hoewel vrijwillige inzet de norm zou moeten zijn, wordt het vrijwel

onmogelijk om een bankrekening te openen voor mensen die geen gebruik wensen te maken van de EBW. Kunt u ingaan op de twee resterende kritiekpunten:
a. Gebrek aan screening: aanbieders van de identificatie-wallets worden vooraf niet streng gescreend op integriteit of het ontbreken van tegenstrijdige (commerciële) belangen.
b. Risico op overidentificatie: er ontbreken harde technische waarborgen die voorkomen dat ontvangende partijen, zoals bedrijven, onnodig veel persoonsgegevens opvragen en opslaan.

Antwoord vraag 7:
Ja, ik ben bekend met deze brandbrief en refereer daarbij aan de reactie op deze brandbrief door de Minister van Financiën (medeondertekend door EZK) (Kamerstuk 26643-1511).[10] De eIDAS-verordening borgt dat het gebruik van EDI-wallets vrijwillig is. Bestaande alternatieve identificatie- en authenticatiemiddelen moeten beschikbaar blijven. Voor de specifieke gevolgen van de antiwitwasregelgeving (AMLA) verwijs ik naar de Minister van Financiën.
U vraagt in te gaan op het punt dat er een gebrek aan screening zou zijn. De eIDAS-verordening schrijft geen voorafgaande screening voor op integriteit of op het ontbreken van tegenstrijdige (commerciële) belangen. Aanbieders van EDI-wallets ondergaan een kwaliteitstoets, zij moeten immers gecertificeerd worden zoals toegelicht in het antwoord op vraag 1. Deze certificering ziet toe op de naleving van de technische en beveiligingseisen uit de verordening en moet worden onderscheiden van een bredere toets op de integriteit en eventuele commerciële belangen van aanbieders. Aanvullende specifieke eisen inzake integriteit en belangen zullen in het kader van open toelating worden opgenomen, bijvoorbeeld in de vorm van controles van solvabiliteit, soevereiniteit en naleving van de AVG.

U vraagt daarnaast in te gaan op het risico van overidentificatie. Zoals toegelicht in de beantwoording van de eerste vraag, moeten organisaties die gegevens willen ontvangen vooraf aangeven welke gegevenscategorieën zij willen opvragen. EDI-wallets controleren technisch of een gegevensverzoek binnen deze geregistreerde categorieën valt. Deze technische controle houdt niet in dat bij de registratie ook wordt getoetst of het beoogde gegevensverzoek noodzakelijk en proportioneel is. Die verantwoordelijkheid ligt, in lijn met de AVG, bij de organisatie die de gegevens verwerkt. Wel maakt het openbare register het eenvoudiger voor eenieder om overvraging en overidentificatie op te sporen en aan te kaarten. Organisaties die zich niet aan de geregistreerde gegevensverzoeken houden, kunnen uit het register worden geweerd en daardoor geen gegevensverzoeken meer aan EDI-wallets sturen.

[10] Reactie op verzoek commissie over de brandbrief van Privacy First over verplichtstelling Europese digitale identiteit bij banken.pdf