Autorité de protection des données
Gegevensbeschermingsautoriteit

Advies nr. 36/2026 van 04 maart 2026

Betreft: advies betreffende een voorontwerp van wet inzake een dienst voor gekwalificeerde elektronische handtekeningen (CO-A-2026-002)

Trefwoorden: gekwalificeerde elektronische handtekening; eIDAS-verordening; identiteitskaart, eID

Vertaling

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, met name de artikelen 23 en 26, (hierna "WOG");

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG,* (hierna "AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "WVG");

Gelet op de adviesaanvraag van mevrouw Vanessa Matz, minister van Modernisering van de Overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid, ontvangen op 13 januari 2025;

Gelet op het verzoek om aanvullende informatie dat op 22 januari 2026 aan de aanvrager is toegezonden;

Gelet op de aanvullende informatie die de aanvrager op 6 februari 2026 heeft verstrekt;

Gelet op het verzoek om aanvullende informatie dat op 9 februari 2026 aan de aanvrager is toegezonden;

Gelet op de aanvullende informatie die de aanvrager op 11 en 13 februari 2026 heeft verstrekt;

Brengt de Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit") op 4 maart 2026 het volgende advies uit:

I. ONDERWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De aanvrager heeft bij de Autoriteit een adviesaanvraag ingediend met betrekking tot **een voorontwerp van wet *inzake een dienst voor gekwalificeerde elektronische handtekeningen*** (hierna "**het ontwerp**"). Het ontwerp past binnen het normatieve kader van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 *betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG* (hierna "**eIDAS-verordening**"), zoals gewijzigd door Verordening (EU) nr. 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 *tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit* (hierna "**eIDAS2-verordening**"[1]).

2. De memorie van toelichting bij het ontwerp vermeldt dat het tot doel heeft *"**een dienst voor gekwalificeerde elektronische handtekeningen op te richten, die door de Federale Regering ter beschikking wordt gesteld van de burgers.** Deze dienst, operationeel gemaakt door de FOD Binnenlandse Zaken en de FOD Beleid en Ondersteuning, stelt burgers in staat om, gebruik makend van een handtekeningcertificaat geactiveerd op afstand, te ondertekenen met een gekwalificeerde elektronische handtekening, in de zin van artikel 3, 12°, van de* [eIDAS-verordening]." (vetgedrukt door de Autoriteit) Om toegang tot deze dienst te krijgen moet de burger, na authenticatie via zijn elektronische identiteitskaart, een gebruikersaccount aanmaken in een informatiesysteem waarvoor in wezen de FOD Strategie en Ondersteuning en de FOD Binnenlandse Zaken een gezamenlijke verantwoordelijkheid dragen.

3. In het kader van de voorbereiding van het dossier heeft de aanvrager de Autoriteit ook aangegeven dat deze dienst voor elektronische handtekeningen *"ook zal dienen om de handtekeningfunctie aan te bieden via de Belgische digitale portemonnee voor identiteit (dat wil zeggen de MyGov.be-app)"*[2].

II. ONDERZOEK VAN HET ONTWERP

Dit advies is als volgt opgebouwd:

[1] Zie advies nr. 14/2025 van 27 februari 2025 van de Autoriteit betreffende een wetsvoorstel tot delen van data uit authentieke bronnen met erkende dienstverleners voor elektronische identificatiemiddelen (DOC56 0330/001) en een daarmee verband houdend amendement (DOC56 0330/002) (CO-A-2025-003).

[2] Zie punt 8.

II.1 Motivering van het ontwerp en de uiteindelijke bestemming van het handtekeningcertificaat op de identiteitskaart

4. Het ontwerp wordt gemotiveerd door de volgende overwegingen uit de memorie van toelichting bij het ontwerp:

> *"De herziening van de eIDAS-verordening (de zogenaamde "eIDAS 2.0") legt* ***nieuwe certificeringsvoorwaarden op voor middelen voor het aanmaken van handtekeningen (Qualified Signature Creation Device QSCD).*** *Deze voorwaarden* ***stellen de geldigheid ter discussie van elektronische handtekeningen die worden geplaatst via de chips op de eIDkaarten****, waarvan de geldigheidsduur niet langer in overeenstemming is met de* ***nieuwe Europese vereisten (QSCD-certificering maximaal 5 jaar geldig, tegenover 10 jaar geldigheid voor een eID-kaart).*** *Vanaf 2026 zullen identiteitskaarten die vóór mei 2021 zijn uitgegeven (enkele miljoenen) hun mogelijkheid verliezen om gekwalificeerde elektronische handtekeningen te plaatsen. Vanuit deze problematiek is het onderhavige wetsontwerp opgesteld, om* ***de continuïteit van de toegang tot de gekwalificeerde elektronische handtekening voor alle burgers en inwoners van België te waarborgen****.* (vetgedrukt door de Autoriteit)
>
> *"Het gebruik van een dergelijke dienst maakt het o****ok mogelijk om in te spelen op de gebruikssituaties die zijn vastgesteld in het kader van de digitale transformatie van de overheid****: dematerialisatie van procedures, toegankelijkheid op mobiele apparaten, afwezigheid van een kaartlezer, behoefte aan handtekeningen op afstand voor ambtenaren, enz."* (vetgedrukt door de Autoriteit)

5. In dit verband heeft de Autoriteit de aanvrager allereerst verzocht haar **precies aan te geven welke relevante regels en normen** van toepassing zijn (en deze mee te delen indien ze niet openbaar toegankelijk zijn) met betrekking tot de certificering van "**QSCD's**" ("**Qualified Signature Creation Device**"), zowel wat betreft de huidige elektronische identiteitskaart als wat betreft de nieuwe regels (certificering met een geldigheidsduur van vijf jaar) van de eIDAS-verordening. Ze vroeg hem ook om toe te lichten waarom, vanuit juridisch en technisch oogpunt, de (te lange) geldigheidsduur van de certificering van de chips van de Belgische eID[3] niet ook een probleem zou vormen voor de dienst voor elektronische handtekeningen die in het kader van het ontwerp wordt ingevoerd, aangezien de toegankelijkheid en het gebruik van deze dienst berusten op een identificatie en authenticatie[4] die zelf op de Belgische eID-kaart zijn gebaseerd. En tot slot vroeg ze haar te bevestigen dat het QSCD dat voortaan zou worden gebruikt, een informatiesysteem van de FOD Binnenlandse Zaken en/of de FOD Beleid en Ondersteuning zou zijn (een systeem waarop dus de privésleutels van de betrokkenen zouden worden opgeslagen).

6. Hij antwoordde het volgende: [NvdV]

> *"In **artikel 30** van de **eIDAS-verordening** worden de eisen voor de certificering van QSCD's vastgesteld. In bijlage II bij de eIDAS-verordening worden de eisen voor QSCD's vastgesteld.*
>
> *Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market* [5] stelt de specifieke normen vast voor de beveiligingsbeoordeling van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen." (vetgedrukt en hyperliinks weggelaten door de Autoriteit)
>
> "*Het gebruik van een QSCD is een van de drie wettelijke vereisten voor een gekwalificeerde elektronische handtekening, zoals bepaald in artikel 3, waarin de definities van de eIDAS-verordening worden vastgelegd:*
> *"gekwalificeerde elektronische handtekening":*

---

[3] Zie https://repository.eidpki.belgium.be/, voor het laatst geraadpleegd op 20/01/2026.

[4] Zie artikel 3, § 2, van het ontwerp.

[NvdV] [alle antwoorden van de aanvrager in dit advies zijn vertaald uit het Frans]

[5] Uitvoeringsbesluit (EU) 2016/650 van de Commissie van 25 april 2016 tot vaststelling van normen inzake de veiligheidsbeoordeling van gekwalificeerde middelen voor het aanmaken van handtekeningen en zegels overeenkomstig artikel 30, lid 3, en artikel 39, lid 2, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

- *een geavanceerde elektronische handtekening*
- *die is aangemaakt met behulp van een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen*
- *en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen;"*

Op grond van artikel 51 Overgangsmaatregelen, vervalt de erkenning van beveiligde middelen voor het aanmaken van handtekeningen die op basis van de Europese Richtlijn 1999/93/EG als QSCD zijn erkend, met ingang van 21/05/2027, waardoor dus niet langer wordt voldaan aan de tweede vereiste voor een gekwalificeerde elektronische handtekening.

[…]

Ter aanvulling en ter informatie: gekwalificeerde certificaten die zijn afgegeven overeenkomstig Richtlijn (EG) nr. 1999/93 worden vanaf 21/05/2026 niet langer als gekwalificeerde certificaten erkend en voldoen dan niet meer aan vereiste 3 van de definitie.
"Artikel 51 Overgangsmaatregelen 2. […]"

Chips van vóór 2021 worden niet langer als QSCD erkend en kunnen dus geen gekwalificeerde handtekening meer aanmaken. ***Voor authenticatie is het gebruik van een QSCD geen vereiste.***

De QSCD-certificering is dus alleen van toepassing op het QSCD dat de gekwalificeerde elektronische handtekening zelf genereert. *In de nieuwe oplossing zal dit middel altijd QSCD-gecertificeerd zijn.*
Om het gekwalificeerde certificaat af te geven, moet de vertrouwensdienstverlener de ***identiteit van de aanvrager controleren volgens een van de vier methoden die worden genoemd in artikel 24, lid 1 bis****, van de eIDAS-verordening. In onze nieuwe oplossing is een van de methoden die zal worden gebruikt de combinatie van de federale authenticatiedienst en het authenticatiecertificaat op identiteits- en verblijfskaarten, wat een genotificeerd elektronisch identificatiemiddel van hoog niveau vormt.*
Er moet ook worden opgemerkt dat ***de nieuwe geldigheidsduur van de QSCD-certificering louter administratief van aard is. Het eventuele verstrijken van de certificering duidt niet op een onderliggend technisch probleem of een veiligheidsrisico****."*
(vetgedrukt door de Autoriteit)

"Het remote QSCD ***wordt <u>beheerd</u> door de QTSP (vertegenwoordigd door de FOD BOSA en de FOD IBZ) en <u>geëxploiteerd</u> door een dienstverlener****, ZETES NV.*

*Het **remote QSCD** bestaat uit de Cryptomathic Signer SAM v6.0-module in combinatie met de Utimaco Cryptoserver CP5 v5.1.0.0 Hardware Security Module (HSM) als cryptografische module voor het genereren en beveiligen van gegevens voor het aanmaken van handtekeningen. **HSM's[6] bieden een veilig beveiligingsmechanisme voor de opslag van de privésleutels van de houder buiten de HSM, in gecodeerde vorm in een databank**.*
*De Signature Activation Module (**SAM** [7]) is een softwaremodule die ervoor zorgt dat gebruikers (dat wil zeggen ondertekenaars) de exclusieve controle over hun ondertekeningssleutels behouden. Deze wordt als lokale toepassing op de HSM's geladen. Het QSCD wordt in een beveiligde omgeving gebruikt.*
***De privésleutels van de houder worden uitsluitend in het QSCD opgeslagen voor zover dat voor het gebruik nodig is.** Wanneer een sleutel niet langer nodig is, wordt deze uit het QSCD verwijderd. De privésleutel wordt bewaard in een beveiligd formaat dat garandeert dat deze alleen binnen het QSCD kan worden gebruikt om ondertekeningshandelingen uit te voeren.* (vetgedrukt en onderstreept door de Autoriteit)

7. De Autoriteit heeft de aanvrager opnieuw ondervraagd naar aanleiding van zijn antwoord ("*…de opslag van de privésleutels van de houder buiten de HSM, in gecodeerde vorm in een databank*") om te laten bevestigen dat de sleutels uitsluitend door de HSM zelf worden verwerkt en daar niet toegankelijk zijn. Hij antwoordde het volgende: *"Het is niet mogelijk om alle actieve sleutels in het QSCD zelf op te slaan, omdat het er voor zo'n apparaat te veel zijn. Bovendien beschikt een rQSCD over meer dan één operationele HSM. **De sleutels worden door de HSM versleuteld, zodat niemand anders ze kan opvragen of gebruiken.**"* (vetgedrukt door de Autoriteit)

8. Op basis van de door de aanvrager verstrekte antwoorden **gaat dit advies uit van het volgende.** Artikel 30, 3 bis, van de eIDAS-verordening bepaalt dat de geldigheidsduur van een certificering van middelen voor het aanmaken van gekwalificeerde elektronische handtekeningen niet langer mag zijn dan vijf jaar. Om een gekwalificeerd certificaat af te geven, moet de verlener van vertrouwensdiensten de identiteit van de betrokkene verifiëren op basis van een identificatiemiddel als bedoeld in artikel 24, 1 bis, van de eIDAS-verordening, namelijk bijvoorbeeld een aangemeld elektronisch identificatiemiddel dat voldoet aan de in artikel 8 vastgestelde eisen met betrekking tot het hoge betrouwbaarheidsniveau. De identificatie en authenticatie via de Belgische elektronische identiteitskaart voldoen aan deze vereisten en het is hiervoor niet nodig om gebruik te maken van een QSCD. Het *"remote QSCD"*valt onder de verantwoordelijkheid van de FOD Binnenlandse Zaken en de FOD BOSA, die een beroep doen op de diensten van het bedrijf Zetes om dit aan hun gebruikers aan te bieden. De privésleutels worden daar tijdens het gebruik opgeslagen en mogen niet toegankelijk zijn. Wanneer ze niet worden gebruikt,

[6] "Hardware Security Module".

[7] "Signature Activation Module".

worden ze versleuteld en door de HSM zelf in een externe databank opgeslagen. Ze worden alleen door de HSM verwerkt, na authenticatie van de betrokkenen voor het plaatsen van elektronische handtekeningen, blijven ontoegankelijk en worden uit de databank verwijderd zodra ze niet meer nodig zijn. **In deze context is het ingevoerde middel geschikt om het nagestreefde doel te bereiken, namelijk het aanmaken van gekwalificeerde elektronische handtekeningen op afstand.**

9. Voorts **kan een burger momenteel zijn elektronische identiteitskaart gebruiken om documenten te ondertekenen zonder dat hij daarvoor via internet een beroep hoeft te doen op een dienstverlener**[8]. Wel vereist de controle van de geldigheid van een certificaat door de ontvanger van een ondertekend document het gebruik van een online dienst (**OCSP/CRL, oftewel Online Certificate Status Protocol/Certificate Revocation List**[9]). De Autoriteit heeft de aanvrager gevraagd wat er op termijn met deze technische mogelijkheid zal gebeuren: **is het de bedoeling om deze af te schaffen of om de voorwaarden voor de verstrekking van elektronische identiteitskaarten te herzien**, zodat deze mogelijkheid behouden blijft in de herziene context van de eIDAS-verordening? De aanvrager antwoordde het volgende:

> *"Er is nog geen formele beslissing genomen, maar door de snelle ontwikkeling van de wettelijke en normatieve context zal het wellicht onmogelijk worden om een oplossing voor het ondertekenen via een handtekeningcertificaat op de elektronische identiteitskaart te handhaven.*
>
> ***De nieuwe oplossing is dus geen tijdelijke oplossing, maar een volledige herziening van onze bestaande dienst voor handtekeningen.*** *Artikel 5 bis, lid 5, g), van de eIDAS-verordening bepaalt bovendien dat burgers via de Europese portemonnee voor digitale identiteit de mogelijkheid moet worden geboden om kosteloos hun handtekening te plaatsen.* ***Deze oplossing zal dus ook dienen om de functionaliteit voor ondertekening via de Belgische digitale identiteitsportefeuille (dat wil zeggen de MyGov.be-app) aan te bieden.****"* (vetgedrukt en onderstreept door de Autoriteit)

---

[8] Lees in dit verband ook het antwoord van de FOD Economie op de vraag: "Moet ik in alle gevallen een beroep doen op een dienstverlener om een gekwalificeerde elektronische handtekening te plaatsen?", beschikbaar via https://economie.fgov.be/nl/themas/online/elektronische-handel/elektronische-handtekening-en, voor het laatst geraadpleegd op 20/01/26. Voor lijsten met gekwalificeerde verleners van vertrouwensdiensten, zie https://economie.fgov.be/nl/themas/online/elektronische-handel/elektronische-handtekening-en en https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls, voor het laatst geraadpleegd op 20/01/2026.

[9] Zie https://repository.eid.belgium.be/index.php?lang=nl, voor het laatst geraadpleegd op 20/01/2026; *"Vertrouwende partijen moeten, om de status van certificaten te controleren, gebruikmaken van online hulpmiddelen die de CA ter beschikking stelt via het archief, alvorens deze certificaten te vertrouwen. De CA werkt de OCSP, de webinterface voor verificatie van de certificaatstatus, de CRL's en de Delta-CRL's dienovereenkomstig bij. CRL's worden regelmatig bijgewerkt, met een minimuminterval van drie uur."* Certipost, "Belgisch Certificaatbeleid & Verklaring met betrekking tot de Praktijk voor eID PKI-infrastructuur Citizen CA", versie 5.0, 03/09/2024, blz. 30, beschikbaar via https://repository.eid.belgium.be/downloads/citizen/nl/CPS_CitizenCA_BRCA34.pdf, voor het laatst geraadpleegd op 20/01/2026.

10. De Autoriteit neemt nota van dit antwoord en is van mening dat de **reikwijdte van het ontwerp** (*"volledige herziening van onze bestaande dienst voor handtekeningen"*, het aanbieden van *"de functionaliteit voor ondertekening via de Belgische digitale identiteitsportefeuille"* en zeer waarschijnlijk het verdwijnen van de mogelijkheid voor de burger om op gekwalificeerde wijze elektronisch te ondertekenen door middel van een certificaat voor elektronische ondertekeningen op zijn elektronische identiteitskaart) **beter moet worden benadrukt in de inleiding, in de memorie van toelichting bij het ontwerp**.

11. Wat gegevensbescherming betreft, en **vanuit het oogpunt van evenredigheid en minimale gegevensverwerking**, **vereist** de in het ontwerp voorziene oplossing namelijk **extra verwerkingen van persoonsgegevens in vergelijking met de oplossing voor elektronische handtekeningen die momenteel nog beschikbaar is via de elektronische identiteitskaart**, en vereist deze a priori systematisch een internetverbinding: verbinding met een externe dienstverlener; het aanmaken van een specifiek gebruikersaccount; identificatie en authenticatie via dit account; het regelmatig genereren van elektronische handtekeningcertificaten met een geldigheidsduur van maximaal 24 uur; extra loggegevens die bij de dienstverleners worden gegenereerd[10].

12. In dit verband is de Autoriteit van mening dat het **raadzaam is om de mogelijkheid te overwegen om een oplossing voor gekwalificeerde elektronische handtekeningen te handhaven van het type dat momenteel bestaat** – een handtekening via een gekwalificeerd certificaat voor elektronische handtekeningen dat de gebruiker op de chip van zijn elektronische identiteitskaart heeft –, met dien verstande dat het aan de aanvrager is om na te gaan of dit al dan niet mogelijk is in het kader van de eIDAS-verordening zoals gewijzigd door de eIDAS2-verordening. In dit verband begrijpt de Autoriteit dat een oplossing op basis van de elektronische identiteitskaart, om redenen van de certificering van de elektronische chip, zou vereisen dat de geldigheidsduur van de elektronische kaarten wordt teruggebracht tot vijf jaar. Dit betekent een ingrijpende wijziging van de huidige praktijk in België, waarvan de reikwijdte en de kosten het best door de aanvrager kunnen worden ingeschat. Het gaat er met name om te bepalen of het haalbaar is om de geldigheidsduur van elektronische identiteitskaarten systematisch te verkorten, of dat het beter is om de burger de keuze te laten (met de bijbehorende gevolgen) tussen een elektronische identiteitskaart met of zonder certificaat van een gekwalificeerde elektronische handtekening. Voor het overige is de Autoriteit er zich terdege van bewust dat de eIDAS-verordening ook voorziet in de verplichting om **Europese portemonnees voor digitale identiteit** in te voeren, die met name alle natuurlijke personen de mogelijkheid bieden om

[10] Zie punt 53.

standaard en kosteloos te ondertekenen met behulp van gekwalificeerde elektronische handtekeningen[11]. Een **andere mogelijkheid** die de aanvrager wellicht zou kunnen overwegen, is om **na vijf jaar te voorzien in een nieuwe certificering van de chip van de elektronische identiteitskaart (het QSCD)**, zodat de levensduur ervan kan worden verlengd als deze certificering kan worden toegekend. Daartoe zouden twee handtekeningcertificaten op de elektronische identiteitskaart kunnen worden geplaatst: een actief certificaat voor een eerste periode van vijf jaar (van t tot t+5); een tweede, inactief certificaat, dat alleen kan worden geactiveerd voor een tweede periode van vijf jaar (t+5 tot t+10) (er moet nog worden bepaald hoe dit tweede certificaat bij de bevoegde gemeente kan worden geactiveerd)[12]. De keuze die hier moet worden gemaakt (al dan niet handhaven van een certificaat voor elektronische handtekeningen op de chip van de identiteitskaart), moet worden onderworpen aan een **gegevensbeschermingseffectbeoordeling**, die, in voorkomend geval en onder andere, zou aantonen dat er op het vlak van gegevensbescherming geen meerwaarde is bij het behoud van een oplossing voor elektronische handtekeningen op basis van de chip van de Belgische elektronische identiteitskaart, ondanks de beschikbaarheid van Europese portemonnees voor digitale identiteit.

II.2 De dienst voor gekwalificeerde elektronische handtekeningen zoals voorzien in het ontwerp

13. Het ontwerp voorziet in de invoering van een **"dienst voor gekwalificeerde elektronische handtekeningen"** die door de FOD Binnenlandse Zaken en de FOD BOSA ter beschikking wordt gesteld. Artikel 2, § 1, 5°, van het ontwerp definieert deze dienst als *"dienst via de welke een gekwalificeerde handtekening in de zin van artikel 3.12 van de eIDAS-verordening via een handtekening**certificaat op afstand kan geplaatst** worden".* (vetgedrukt en onderstreept door de Autoriteit) Deze bepaling definieert de gekwalificeerde elektronische handtekening als *"een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen"*. Artikel 2, § 3, van het ontwerp bepaalt op zijn beurt: *"Voor het **op afstand aanmaken van gekwalificeerde elektronische handtekeningen via de dienst voor gekwalificeerde elektronische***

[11] Artikel 5 bis, lid 5, g), van de eIDAS-verordening.

[12] De mogelijkheid dat er een inactief certificaat op de elektronische identiteitskaart staat, is al in het positieve recht vastgelegd (zie artikel 6, § 7, laatste lid, van de wet van 19 juli 1991 *betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten*). In de praktijk lijkt het, zonder dat de Autoriteit deze mogelijkheid heeft onderzocht, technisch haalbaar om deze certificaten te activeren: zie bijvoorbeeld

https://www.waasmunster.be/activering-handtekeningcertificaat-eid-vanaf-16-jaar;

https://www.berlaar.be/nieuws/activeer-het-handtekeningcertificaat-van-jouw-eid;

https://www.dalhem.be/ma-commune/services-communaux/population/demarches-administratives/carte-didentite;

https://www.lommel.be/handtekencertificaat-activeren, voor het laatst geraadpleegd op 04/03/2026.

handtekeningen *stellen de Federale Overheidsdienst Binnenlandse Zaken en de Federale Overheidsdienst Beleid en Ondersteuning gekwalificeerde handtekening****certificaten ter beschikking*** *van de burgers*". (vetgedrukt en onderstreept door de Autoriteit)

14. Deze activiteiten komen neer op het **verlenen van ten minste drie vertrouwensdiensten** in de zin van de eIDAS-verordening, namelijk in ieder geval: *"het uitgeven van certificaten voor elektronische handtekeningen"*[13], *"het aanmaken van elektronische handtekeningen"*[14] en *"het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische handtekeningen"*[15]. De Autoriteit heeft de aanvrager verzocht dit te bevestigen en in dit verband aan te geven wie een dienst voor validering van elektronische handtekeningen zou aanbieden[16] (en hoe) (Zal er software van het type eID-viewer ter beschikking worden gesteld aan de gebruikers? Is het de FOD Binnenlandse Zaken, die krachtens artikel 2, § 6, 1°, van het ontwerp verantwoordelijk is voor de certificaten, die de nodige middelen (OCSP/CRL[17]) online ter beschikking zal stellen?).

15. De aanvrager antwoordde het volgende:

> *"'Belgium Federal Government' is vandaag al een* ***QTSP voor de volgende vertrouwensdiensten****:*
>
> - ***Qualified certificate for electronic signature***
> - *Qualified timestamp*
>
> *In de nabije toekomst zullen de volgende vertrouwensdiensten hieraan worden toegevoegd:*
>
> - *Qualified certificate for electronic seal*
> - ***Qualified management of remote QSCDs****."*
>
> *"****De handtekeningcertificaten voor burgers in de nieuwe dienst zullen een geldigheidsduur van 24 uur hebben, waardoor een statusdienst zoals OCSP en CRL overbodig wordt.*** *Deze zeer korte geldigheidsduur verkort de tijd waarin misbruik kan plaatsvinden bij een beveiligingsincident aanzienlijk, beperkt de risico's die gepaard gaan met een te late intrekking en draagt zo bij aan een algeheel hoger beveiligingsniveau.*
> *De eID-viewer dient om de eID te lezen en staat dus los van de nieuwe oplossing.*
> ***De eID-middleware wordt bijgewerkt zodat ondertekening via de nieuwe dienst mogelijk wordt met behulp van applicaties voor ondertekening die op de eigen pc***

[13] Artikel 3, punt 16, a), van de eIDAS-verordening.
[14] Artikel 3, punt 16, c), van de eIDAS-verordening.
[15] Artikel 3, punt 16, f), van de eIDAS-verordening.
[16] Artikel 3, punt 16, d) van de eIDAS verordening.
[17] Zie voetnoot 9.

zijn geïnstalleerd. *Deze eID-middleware wordt aangeboden door de FOD BOSA: Downloaden | eID-software downloaden | eID-software.*
Daarnaast zal de ***FOD BOSA tegelijkertijd zijn ondertekeningsplatform (SigningBox) aanpassen*** *zodat handtekeningen via de nieuwe dienst voor ondertekening op afstand kunnen worden geplaatst. SigningBox zal gebruikmaken van de nieuwe dienst."* (vetgedrukt en onderstreept door de Autoriteit)

Naar aanleiding van verdere vragen heeft de aanvrager het volgende bevestigd: "*Het is* ***standaard om certificaten die slechts één dag geldig zijn te gebruiken voor ondertekeningen op afstand****. In dat geval zijn* ***het OCSP of de CRL niet langer nodig: als het certificaat bestaat, is het geldig****. In overeenstemming met ons bestaande beleid en de ETSI-normen inzake eID moeten eID-certificaten zo nodig binnen 24 uur worden ingetrokken."* (vetgedrukt door de Autoriteit)

16. De Autoriteit neemt er nota van dat een dienst die via **het OCSP en de CRL's** beschikbaar is, **niet langer relevant is in het kader van certificaten met een geldigheidsduur van 24 uur** (op dit punt merkt de Autoriteit echter op dat de gegenereerde certificaten zelfs een **geldigheidsduur van minder** dan 24 uur zouden kunnen hebben – de geldigheidsduur zou beperkt kunnen zijn tot één handtekening of een korte sessie) en daarom niet beschikbaar zullen zijn in het kader van het ontwerp. Het volstaat dan ook om te controleren of het certificaat op het betreffende tijdstip daadwerkelijk door de betrokken verlener van vertrouwensdiensten is afgegeven[18]. In ieder geval bepaalt bijlage I bij de eIDAS-verordening dat een gekwalificeerd certificaat met name gegevens ter validatie van de elektronische handtekening moet bevatten die overeenkomen met de gegevens voor het aanmaken van de elektronische handtekening, de geavanceerde elektronische handtekening of de geavanceerde elektronische zegel van de gekwalificeerde verlener van vertrouwensdiensten die het certificaat afgeeft, en de informatie of de locatie van de diensten die kunnen worden gebruikt om de geldigheidsstatus van het gekwalificeerde certificaat te vernemen.

17. De Autoriteit heeft de aanvrager opnieuw ondervraagd, met name over de volgende punten: hoever staat het met het **aanmaken van de elektronische handtekening** op zich; zal de betrokkene via de nieuwe dienst eenvoudigweg een gekwalificeerd certificaat voor elektronische handtekeningen kunnen verkrijgen om elders te gebruiken, via een applicatie waarover de betrokkene zal beschikken (of is het de bedoeling om het systeem voor elektronische handtekeningen op afstand in deze andere applicaties te integreren?). De Autoriteit heeft hem ook vragen gesteld over de handeling van het

[18] Zie met name de List of Trusted Lists ("LOTL"), die door de Europese Commissie ter beschikking wordt gesteld. https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/887386519/TLv6+is+coming+Upgrade+now+to+avoid+signature+validation+failures; https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109149/eSignature+List+of+Trusted+Lists; https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls; voor het laatst geraadpleegd op 16/02/2026.

"**plaatsen**" van de elektronische handtekening *"op afstand"* (in plaats van "het plaatsen" van een elektronische handtekening spreekt de eIDAS-verordening van *"ondertekenen met gekwalificeerde elektronische handtekeningen"*). Technisch gezien houdt **de elektronische ondertekening van een document in dat dit document wordt verwerkt** (het toepassen van een cryptografische functie op het document – het genereren van een hash –, het toevoegen van gegevens aan het document). De Autoriteit vroeg de aanvrager te bevestigen of deze verwerkingshandelingen wel degelijk zullen worden uitgevoerd via het informatiesysteem van de FOD Binnenlandse Zaken/FOD Strategie en Ondersteuning, dat daartoe het te ondertekenen document zal ontvangen. Na bevestiging, heeft de Autoriteit de aanvrager gevraagd naar de bewaartermijn van het aldus verwerkte document.

18. De aanvrager antwoordde het volgende:

> *"**Er is geen gekwalificeerde dienst voor het plaatsen van handtekeningen, en de burger is vrij om zelf te kiezen welke hij wil gebruiken (Adobe Reader is bijvoorbeeld ook een programma waarmee handtekeningen kunnen worden geplaatst).** We nemen het plaatsen van handtekeningen daarom niet mee in de door de CAB uitgevoerde audit."*[19] (vetgedrukt en onderstreept door de Autoriteit)
>
> [...[20]]
>
> *"De gebruiker **kan de ondertekeningsfunctie van het rQSCD** (uiteraard in combinatie met het certificaat) in andere toepassingen **gebruiken**, maar **het certificaat wordt alleen in combinatie met het rQSCD gebruikt**. Wij verstrekken dus geen certificaten aan derden of voor andere doeleinden dan dit specifieke gebruik."* (vetgedrukt en onderstreept door de Autoriteit)
>
> "*De eID-middleware is nodig om de eID-kaart (authenticatiecertificaat) te raadplegen. Deze software wordt al gebruikt en wordt momenteel uitgebreid om ook de volgende handelingen te kunnen uitvoeren: het aanmaken van een account, het op afstand aanmaken van een certificaat, het ophalen en gebruiken van een certificaat op afstand, en rekeying. Deze handelingen worden uitgevoerd via de FOD BOSA en de FOD IBZ, maar de software maakt het mogelijk om ze toegankelijk te maken op de computer van de gebruiker."*

---

[19] De Autoriteit heeft de aanvrager hierover opnieuw vragen gesteld. Het ontwerp definieert de "dienst voor gekwalificeerde elektronische handtekeningen" zelf als "dienst via de welke een gekwalificeerde handtekening via een handtekeningcertificaat kan geplaatst worden". Op een bepaald moment (na de aanmaak van een certificaat) moet een dienst de elektronische handtekening aanmaken. Artikel 3, punt 16, c), van de eIDAS-verordening heeft het over dit soort vertrouwensdiensten. En artikel 2, § 3, van het ontwerp heeft ook duidelijk betrekking op het op afstand aanmaken van elektronische handtekeningen. In principe is het een QTSP die deze handtekening moet aanmaken, en dit moet gedaan worden door het *remote* QSCD. Zou er dan niet een QTSP moeten zijn die wordt aangewezen voor dit deel van het proces van de door het ontwerp voorziene ondertekeningsdienst?

[20] Zie punt 15, laatste alinea.

Toen hem opnieuw vragen werden gesteld over het <u>plaatsen</u> of <u>aanmaken</u> van handtekeningen, antwoordde de aanvrager het volgende:

"Er kunnen **drie** verschillende elementen worden onderscheiden:

1. ***De dienst die het certificaat aanmaakt****: dit is een gekwalificeerde dienst die wordt geleverd door de QTSP Kingdom of Belgium.*
2. *De dienst die de handtekening aanmaakt: er **<u>bestaat geen specifieke gekwalificeerde dienst onder eIDAS voor deze dienst</u>**.*
    - *In het kader van eID-kaarten wordt de handtekening geplaatst door het QSCD (dat wil zeggen de contactchip) dat zich in de kaart bevindt.*
    - *In het kader van de "Remote Signing"-oplossing wordt de handtekening aangemaakt door het rQSCD-systeem, dat (zoals u al aangaf) door Zetes wordt geëxploiteerd voor de QTSP van het Koninkrijk België. Onder de eerste versie van de regelgeving bestond er geen dergelijke **gekwalificeerde** dienst. Onder de nieuwe versie **bestaat er nu de gekwalificeerde dienst "beheer van QSCD's." <u>De QTSP zal gekwalificeerd zijn om deze dienst te verlenen</u>** vóór de uiterste datum die wordt opgelegd door eIDAS art. 51 (3).*
3. « **3. *De dienst die de handtekening plaatst****, dat wil zeggen een dienst zoals SigningBox, aangeboden door de FOD BOSA, of een platform van een derde partij zoals Adobe: **<u>dit is geen dienst die onder eIDAS valt</u>.***

    *Om de handtekening aan te maken met behulp van de dienst voor handtekeningen op afstand, ondersteunen we daarom applicaties zoals Adobe Reader (gebruikservaring vergelijkbaar met het ondertekenen met eID) en de **Signingbox die wordt aangeboden door de FOD BOSA.***

    *Adobe Reader of soortgelijke applicaties zijn lokale applicaties die door de gebruiker worden geïnstalleerd, terwijl **Signingbox een <u>webapplicatie</u>** is die toegankelijk is via https://signing.fts.bosa.belgium.be/. Deze laatste maakt gebruik van de componenten van de dienst voor digitale handtekeningen die door de Europese Commissie wordt aangeboden (https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/).*

    *In beide gevallen wordt het document door de gebruiker bekeken en wordt hem gevraagd de ondertekening van het document te bevestigen. **Deze applicaties communiceren met de dienst voor ondertekening op afstand** en sturen alleen de hash van het document naar de dienst voor ondertekening op afstand om de hash te ondertekenen.* Adobe Reader of Signingbox ontvangt de ondertekende hash van de

dienst voor ondertekening op afstand en **voegt op basis daarvan de elektronische handtekening toe aan het document**." (vetgedrukt en onderstreept door de Autoriteit)

19. De door de aanvrager verstrekte antwoorden geven aanleiding tot de volgende opmerkingen van de Autoriteit.

20. **Ten eerste moet het ontwerp, in overeenstemming met de in de eIDAS-verordening gedefinieerde begrippen, duidelijk aangeven op welke diensten het van toepassing is, en het dispositief** (voorwaarden voor toegang tot de dienst; logregistratie; verwerkingsverantwoordelijken) **afstemmen op elk van de betrokken diensten.** In dit verband blijkt uit de memorie van toelichting en de door de aanvrager verstrekte antwoorden duidelijk dat het ontwerp van toepassing is op **de volgende vertrouwensdiensten**: *"Het uitgeven van certificaten voor elektronische handtekeningen"* [21], het *"aanmaken van elektronische handtekeningen"* [22] (dit gebeurt via het door Zetes namens de FOD Binnenlandse Zaken en de FOD BOSA geleverde *remote* QSCD) en *"het beheer van apparatuur voor het op afstand aanmaken van elektronische handtekeningen"* (dat wil zeggen het beheer door de FOD Binnenlandse Zaken en de FOD BOSA van het door Zetes geleverde *remote* QSCD)[23].

21. **Ten tweede** heeft de Autoriteit, wat betreft de dienst waarmee een **elektronische handtekening** op een document kan worden **geplaatst**, terecht opgemerkt en vastgesteld dat een dergelijke dienst i**n de eIDAS-verordening niet wordt gedefineerd als vertrouwensdienst**. Uit de tekst van het ontwerp en de memorie van toelichting **blijkt echter niet duidelijk of het ontwerp al dan niet tot doel heeft deze specifieke dienst in te voeren en te reglementeren.** Met name op dit punt, tenzij de Autoriteit zich vergist, verwijzen de documenten die bij het dossier zijn gevoegd niet expliciet naar de oplossing "Signingbox" waarnaar de aanvrager verwijst in de antwoorden die hij aan de Autoriteit heeft verstrekt in het kader van de voorbereiding van het dossier, en zijn de definitie van het begrip *"dienst voor gekwalificeerde elektronische handtekeningen"* [24] zoals vastgelegd in artikel 2, § 1, 5°, van het ontwerp, en de wijze waarop dit begrip in het dispositief van het ontwerp wordt gebruikt, dubbelzinnig[25]. Daarom moet deze bepaling van het ontwerp in ieder geval worden aangepast. **Indien het de bedoeling van de aanvrager is om met zijn ontwerp een dienst voor het plaatsen van handtekeninge**n (een webapplicatie) **aan te bieden**, moet deze **dienst** allereerst **worden**

[21] Artikel 3, punt 16, a) van de eIDAS-verordening.

[22] Artikel 3, punt 16, c) van de eIDAS-verordening.

[23] Artikel 3, punt 16, f) van de eIDAS-verordening.

[24] Namelijk de "dienst via de welke een gekwalificeerde handtekening [...] kan **geplaatst** worden". (vetgedrukt door de Autoriteit)

[25] Hoewel deze dienst wordt omschreven als de dienst waarmee een handtekening kan worden **geplaatst**, heeft artikel 2, § 3, van het ontwerp bijvoorbeeld betrekking op *"het **op afstand aanmaken** van gekwalificeerde elektronische handtekeningen via de dienst voor gekwalificeerde elektronische handtekeningen".* (vetgedrukt door de Autoriteit)

gedefinieerd en moeten de werking en de levering ervan vervolgens op dezelfde wijze worden geregeld als de andere betrokken vertrouwensdiensten. Afgezien van de volgende opmerking **doet de Autoriteit geen verdere uitspraken over deze dienst**.

22. **Ten derde moet het ontwerp duidelijkheid bieden over het aanbod van de betrokken diensten aan de burgers: welke diensten kunnen afzonderlijk worden gebruikt en welke diensten moeten op geïntegreerde wijze worden gebruikt.** Wat dit punt betreft: als het de bedoeling van de aanvrager is om de dienst voor **het plaatsen van elektronische handtekeningen** te reguleren, moet uit het ontwerp ook duidelijk blijken dat het **gebruik van deze dienst optioneel** is (hoewel, zo veronderstelt de Autoriteit, gekoppeld aan het gebruik van de andere (vertrouwens)diensten waarin het ontwerp voorziet), en dat de andere aangeboden (vertrouwens)diensten bijgevolg kunnen worden gebruikt zonder dat er systematisch gebruik wordt gemaakt van de dienst voor het plaatsen van handtekeningen. Met name op het gebied van gegevensbescherming is de impact van een dergelijke dienst duidelijk, aangezien de levering ervan technisch gezien toegang tot (en verwerking van) het te ondertekenen document zelf zou kunnen inhouden, en dus ook de verwerking van de gegevens, met inbegrip van persoonsgegevens, die het document bevat. In dit verband is **de Autoriteit van mening** dat, in het kader van **de dienst voor het plaatsen van elektronische handtekeningen**, de verwerking van het document (het genereren van de hash; het toevoegen van de handtekening in de vorm van een ondertekende hash, het openbare certificaat en eventueel een visuele weergave) in ieder geval **volledig lokaal (*client-side*) moet plaatsvinden**. Voor het overige begrijpt de Autoriteit dat **de betrokkene op grond van het ontwerp alleen een certificaat voor elektronische handtekeningen kan verkrijgen indien hij ook gebruik wil maken van de dienst voor het aanmaken van elektronische handtekeningen** via het door Zetes geleverde *remote* QSCD, onder de verantwoordelijkheid van de FOD Binnenlandse Zaken en de FOD BOSA.

23. **Ten vierde** neemt de Autoriteit nota van dit antwoord van de aanvrager met betrekking tot het **aanmaken van de elektronische handtekening zelf**: het document dat de betrokkene ondertekent, **mag niet worden doorgestuurd** naar de FOD BOSA, de FOD Binnenlandse Zaken of Zetes (met andere woorden, de hash ervan wordt lokaal – *client-side* – gegenereerd via de terminal (software en hardware) van de betrokkene (computer of ander apparaat). Dit is een aanpak die **in overeenstemming is met de beginselen van doelbinding en minimale gegevensverwerking**.

24. **Ten vijfde** geeft de aanvrager aan[26] dat er **geen specifieke gekwalificeerde dienst in de zin van de eIDAS-verordening bestaat voor het aanmaken van elektronische handtekeningen.** In het onderhavige geval is het echter, in tegenstelling tot het scenario van elektronische ondertekening via het ondertekeningscertificaat op de chip van de elektronische identiteitskaart, wel aangewezen

[26] Zie punt 17.

om gebruik te maken van een dergelijke dienst. De Autoriteit merkt op dat in dit geval de gekwalificeerde dienst, **de dienst voor het beheer van apparatuur voor het aanmaken van gekwalificeerde elektronische handtekeningen op afstand** is.

II.3 Verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens

25. Artikel 2, § 6, van het ontwerp regelt de verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens. Deze bepaling luidt als volgt:

> "*1° wat betreft de persoonsgegevens voor de inhoud en het beheer van de gekwalificeerde handtekeningcertificaten is de Federale Overheidsdienst Binnenlandse Zaken de verwerkingsverantwoordelijke en garandeert de identiteit van de gebruiker en de identificatie van de ondertekenaar in geval van geschil;*
>
> *2° de Federale Overheidsdienst Binnenlandse Zaken en de Federale Overheidsdienst Beleid en Ondersteuning zijn gezamenlijke verwerkingsverantwoordelijken voor de persoonsgegevens verwerkt ten behoeve van de aanmaak, de actualisatie, het beheer en de bewaring van de gebruikersaccounts bedoeld in artikel 3 in het register van gebruikersaccounts bedoeld in artikel 3 §6;*
>
> *3° de Federale Overheidsdienst Beleid en Ondersteuning is de verwerkingsverantwoordelijke voor de persoonsgegevens verwerkt voor het bijhouden van de* ***logbestanden*** [27] *met betrekking tot de* ***gebruikersaccounts*** *bedoeld in artikel 3;*
>
> *4° de Federale Overheidsdienst Binnenlandse Zaken is de verwerkingsverantwoordelijke voor de persoonsgegevens verwerkt voor het bijhouden van de* ***logbestanden*** [28] *met betrekking tot het* ***beheer van de gekwalificeerde handtekeningcertificaten****.*" (vetgedrukt door de Autoriteit)

26. De Autoriteit benadrukt meteen dat **het ontwerp terecht tot doel heeft de verantwoordelijkheden te verduidelijken met betrekking tot de verwerking van persoonsgegevens in dit kader**[29]**.** Daarom moet de aanvrager er altijd goed op letten dat de aanwijzing van een entiteit als verwerkingsverantwoordelijke in overeenstemming is met de taken en opdrachten die haar in het kader

[27] (niet van toepassing hier)

[28] (niet van toepassing hier)

[29] Zie ook de recente ontwikkelingen in Advies nr. 08/2026 van 20 januari 2026 met betrekking tot een voorontwerp van wet tot wijziging van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid en de wet van 17 juli 2001 betreffende de machtiging voor de federale overheidsdiensten om zich te verenigen met het oog op

van het betreffende normatieve kader zijn toegewezen. In haar adviespraktijk redeneert de Autoriteit dat een entiteit in het algemeen verwerkingsverantwoordelijke is voor de verwerking van persoonsgegevens die nodig is voor de uitvoering van deze opdrachten/taken. Deze benadering maakt het in principe ook mogelijk om systematisch een verantwoordelijkheid toe te wijzen. **In het kader van het ontwerp is het van belang dat duidelijk kan worden vastgesteld wie verantwoordelijk is voor de gegevensverwerking die nodig is voor de uitvoering van de verschillende aangeboden vertrouwensdiensten[30]. En in principe zou deze verantwoordelijkheid moeten berusten bij de entiteit – de gekwalificeerde verlener van vertrouwensdiensten[31] die door het ontwerp is aangewezen om de betreffende vertrouwensdienst aan te bieden[32]**. Deze aanpak is in overeenstemming met de eIDAS-verordening, die een reeks verplichtingen oplegt aan dit specifieke type dienstverleners, die logischerwijs op dit gebied een eigen verantwoordelijkheid dragen[33].

27. De aanpak die in het ontwerp wordt gevolgd, vertoont echter een zekere mate van hybriditeit, aangezien er taken en verantwoordelijkheden worden toegewezen met betrekking tot de verwerking van gegevens zonder dat er systematisch een overeenkomst tussen beide bestaat. Concreet wordt dit geïllustreerd door de volgende ontwikkelingen.

28. De "**aanmaak**"en het "**beheer**" van gekwalificeerde handtekening**certificaten** vallen onder de verantwoordelijkheid van de FOD Binnenlandse Zaken wat gegevensverwerking betreft. Overeenkomstig artikel 2, § 3, van het ontwerp zijn de FOD Binnenlandse Zaken en de FOD Beleid en Ondersteuning echter belast met het "**ter beschikking stellen**" (een handeling die dus losstaat van het "beheer" van de certificaten) van de certificaten aan de burgers. Met andere woorden, wat de verwerking van persoonsgegevens betreft, **lijkt** de verantwoordelijkheid voor het ter beschikking stellen van de certificaten **een gezamenlijke verantwoordelijkheid te zijn** van de FOD Binnenlandse Zaken en de FOD Beleid en Ondersteuning.

29. De Autoriteit begrijpt dat de FOD Binnenlandse Zaken zal optreden als Certificate Authority (**CA**) die verantwoordelijk is voor de aanmaak van gekwalificeerde certificaten voor elektronische handtekeningen, en dat het met name aan haar is om certificaten eventueel in te trekken en de nodige informatie over de geldigheid van de certificaten (OCSP/CRL) ter beschikking te stellen. De aanvrager heeft **echter** in de antwoorden die hij in het kader van de voorbereiding van de zaak aan de Autoriteit heeft

---

de uitvoering van werkzaamheden inzake informatiebeheer en informatieveiligheid (CO-A-2025-207), punt 14 en de geciteerde referenties.

[30] Of gewoon "dienst ", wanneer het gaat om de dienst waarmee een gekwalificeerde elektronische handtekening kan worden geplaatst, voor zover het ontwerp tot doel heeft deze dienst te reguleren; zie punt 21.

[31] Of de verlener van een ander soort dienst, *ibid.*

[32] Of een andere dienst, zie voetnoot 27.

[33] Zie artikel 13 van de EIDAS-verordening.

verstrekt, benadrukt dat OCSP/CRL niet langer relevant waren gezien de beperkte geldigheidsduur van de certificaten – zie punten 15-16. Maar **het ontwerp bevat geen dergelijke bepaling** (deze conclusie volgt uit de toekenning van verantwoordelijkheid met betrekking tot de gegevensverwerking).

30. Welke entiteit is verantwoordelijk voor de gegevensverwerking die noodzakelijk is voor het verlenen van de dienst voor elektronische handtekeningen op afstand zelf (dat wil zeggen: de dienst voor het aanmaken van elektronische handtekeningen)? Artikel 2, § 6, vermeldt dit niet, maar artikel 2, § 2, bepaalt: *"Deze wet heeft betrekking op de dienst voor [...] elektronische handtekeningen,* ***ter beschikking gesteld*** *door de Federale Overheidsdienst Binnenlandse Zaken en de Federale Overheidsdienst Strategie en Ondersteuning*" (door de Autoriteit vetgedrukt), onverminderd de eerder gemaakte opmerkingen over de dubbelzinnigheid van de definitie van de "*dienst voor elektronische handtekeningen*"[34]. Het **lijkt er dus op** dat de levering van de dienst voor elektronische handtekeningen, wat de gegevensverwerking betreft, onder de gezamenlijke verantwoordelijkheid valt van de FOD Binnenlandse Zaken en de FOD BOSA.

31. Wat betreft de **gegevensverwerking in het kader van de logregistratie**, kan in het ontwerp inderdaad worden vermeld dat de FOD BOSA verwerkingsverantwoordelijke is voor de *logging* met betrekking tot de **gebruikersaccounts** (aangezien de FOD Beleid en Ondersteuning en de FOD Binnenlandse Zaken in dit geval *gezamenlijke* verwerkingsverantwoordelijken zijn, zodat de bepaling in ontwerp een meerwaarde biedt). De Autoriteit ziet daarentegen niet in waarom het nodig zou zijn om bovendien aan te geven dat de FOD Binnenlandse Zaken verantwoordelijk is voor de *logging* in verband met het "**beheer**" van de certificaten, aangezien deze reeds is aangewezen als verwerkingsverantwoordelijke voor de gegevensverwerking in verband met het beheer van de certificaten. Dit gezegd zijnde, heeft de memorie van toelichting betrekking op de logs die verband houden met het "**gebruik**" van de certificaten, wat weer een andere vorm van gegevensverwerking is. Het ontwerp moet verduidelijken of het gebruik van de certificaten het voorwerp moet zijn van een specifieke logregistratie en onder de verantwoordelijkheid van welke entiteit dan. Bovendien is het ontwerp onvolledig, omdat het niet gericht is op de "**aanmaak**" van de certificaten. Wie anders dan de FOD Binnenlandse Zaken zou belast zijn met de logging met betrekking tot de aanmaak van de certificaten? *Quid* met de registratie van het gebruik van de dienst voor elektronische handtekeningen?

32. **Aangezien het ontwerp ingaat op de kwestie van de logregistratieverplichtingen en de verantwoordelijkheid ten aanzien van de gegevensverwerkingen die hiermee gepaard gaat, moet het op dit gebied een coherente en alomvattende aanpak hanteren.**

[34] Zie punt 21.

33. Wat de gevallen van **gezamenlijke verantwoordelijkheid**[35] betreft, heeft de Autoriteit zich ook afgevraagd of er eventueel via een koninklijk besluit kan worden overwogen om de respectieve verplichtingen van de FOD Binnenlandse Zaken en de FOD Beleid en Ondersteuning nader te omschrijven[36].

34. Toen hem hierover vragen werden gesteld (zij het in enigszins andere bewoordingen), legde de aanvrager het volgende uit:

> *"De 'Kingdom Belgium Federal Government' is vandaag al een Qualified Trust Service Provider voor handtekeningdiensten en wordt vertegenwoordigd door de FOD IBZ en de FOD BOSA.*
> *De FOD IBZ en de FOD BOSA hebben een **contract met de verwerker ZETES NV** voor het **aanmaken, beheren en bewaren** van gekwalificeerde elektronische handtekeningcertificaten, **en ook met CERTIPOST** voor het beheer en de bewaring van reeds afgegeven gekwalificeerde elektronische handtekeningcertificaten (er worden in het kader van dit contract geen nieuwe certificaten meer aangemaakt).*
> *De **certificaten van de nieuwe oplossing** zullen worden afgegeven door de 'Kingdom Belgium Federal Government' QTSP De entiteit die verantwoordelijk is voor de afgifte, het beheer en de bewaring van de certificaten is dus de 'Kingdom Belgium Federal Government' QTSP, vertegenwoordigd door de FOD BOSA en de FOD IBZ, die een beroep doen op **verwerker ZETES NV, die optreedt als Certificate Authority (CA).***
>
> *Technisch gezien is het **een systeem van de FOD BOSA dat de gebruikersaccounts verwerkt en dat de aanvraag voor een certificaat van een burger doorstuurt naar de CA,** die technisch wordt geëxploiteerd door ZETES NV, **nadat de burger door de FOD BOSA via de FAS is geauthenticeerd en nadat de FOD BOSA de geldigheid van zijn gebruikersaccount heeft gecontroleerd.***
> *De controle van de naam en voornamen en van de handtekeningbevoegdheid ("CanSign") gebeurt op basis van de gegevens uit de authentieke gegevensbron, het Rijksregister van de FOD IBZ.*
> ***Er vindt geen validiteitscontrole plaats via OCSP/CRL, aangezien het om certificaten met een geldigheidsduur van 24 uur gaat.***
> ***De logregistratie en audit van de gebruikersaccounts** gebeurt door de **FOD BOSA** en **de logregistratie en audit van de certificaten gebeurt door de verwerker van de***

[35] Wat bijvoorbeeld het beheer van accounts betreft, bepaalt artikel 3, § 4, van het ontwerp dat de FOD Binnenlandse Zaken en de FOD Beleid en Ondersteuning de in § 3 vermelde voorwaarden moeten controleren, zowel bij het aanmaken van het account als tijdens de levensduur ervan.

[36] Zie artikel 26.1 van de AVG.

FOD IBZ en de FOD BOSA. *Meer informatie vindt u in het antwoord op vraag 18.*" (vetgedrukt door de Autoriteit)

Wat betreft de **gezamelijke verantwoordelijkheid**, antwoordde de aanvrager het volgende: *"Er zal een overeenkomst worden gesloten tussen de FOD IBZ en de FOD BOSA."*

35. Het ontwerp **moet op basis van de voorgaande uiteenzettingen nader worden uitgewerkt om duidelijk vast te stellen welke entiteiten (al dan niet gezamenlijk) verantwoordelijk zijn voor welke verwerkingen van persoonsgegevens in het kader van de verificatie van de identificatie/authenticatie van gebruikers, en het leveren van de verschillende vertrouwensdiensten[37] waarin het ontwerp voorziet.** Deze aanpak moet in overeenstemming zijn met de taken en opdrachten die het ontwerp aan deze entiteiten toekent. Deze verantwoordelijkheden moeten door het ontwerp worden toegewezen aan de betrokken verwerkingsverantwoordelijken. De AVG staat het gebruik van verwerkers toe, zodat het, afhankelijk van de omstandigheden, niet uitgesloten is dat Zetes als verwerker van de FOD Binnenlandse Zaken en de FOD BOSA kan optreden, voor zover de activiteiten van Zetes in de praktijk daadwerkelijk beperkt blijven tot die van een verwerker. Theoretisch zou het ontwerp ook een andere aanpak kunnen volgen en bepalen dat de FOD Binnenlandse Zaken en de FOD BOSA, volgens procedures en voorwaarden die door het ontwerp moeten worden vastgesteld, de gekwalificeerde verlener van vertrouwensdiensten aanwijzen die belast is met het verlenen van een van de in het ontwerp voorziene vertrouwensdiensten (toewijzing van een taak van algemeen belang aan een particuliere entiteit). Het ontwerp zou dan deze dienstverlener verantwoordelijk kunnen stellen voor de verwerking van persoonsgegevens. **Het is in het onderhavige geval aan de aanvrager om de aanpak en de juridische kwalificaties te kiezen die het beste aansluiten bij de feiten.**

36. Wat betreft de in het ontwerp voorziene gezamenlijke verantwoordelijkheden met betrekking tot de verwerking, neemt de Autoriteit nota van de keuze van de aanvrager om de respectieve verplichtingen van de FOD Binnenlandse Zaken en de FOD BOSA niet in het ontwerp of in een koninklijk besluit ter uitvoering daarvan vast te leggen, maar deze autoriteiten in plaats daarvan een overeenkomst te laten sluiten. De Autoriteit wijst erop dat de betrokkene in elk geval altijd zijn rechten kan uitoefenen ten aanzien van en tegen elk van de verwerkingsverantwoordelijken, overeenkomstig artikel 26.3 van de AVG. De "*hoofdlijnen*" van deze overeenkomst moeten eveneens ter beschikking worden gesteld van de betrokkene, overeenkomstig artikel 26.2 van de AVG. **Als aanvullende waarborg op het gebied van transparantie verzoekt de Autoriteit de aanvrager na te gaan of het ontwerp niet zou kunnen voorzien in de publicatie van de overeenkomst die zal worden gesloten.**

[37] Of andere, zie voetnoot 30.

II.4 Gebruikersaccount, certificaat en verwerkte gegevens

II.4.1 Gebruikersaccount en register van gebruikersaccounts

37. Artikel 3, § 5, van het ontwerp bepaalt dat het register van gebruikersaccounts voor elk gebruikersaccount de volgende gegevens bevat: de naam van de houder van het gebruikersaccount; de eerste twee voornamen en, in voorkomend geval, de eerste letter van de derde voornaam; het rijksregisternummer van de houder van het gebruikersaccount; en het gebruikersaccountnummer van de houder van het gebruikersaccount.

38. De Autoriteit merkt op dat de "**status**" van het account – "actief" of "gedeactiveerd" – eveneens een gegeven is dat in het register van gebruikersaccounts moet worden verwerkt. Daarnaast heeft zij de aanvrager gevraagd of de verwerking van "*de eerste twee voornamen en, in voorkomend geval, de eerste letter van de derde voornaam*" van de gebruiker noodzakelijk is, aangezien het rijksregisternummer deze gegevens overbodig lijkt te maken (dezelfde vraag doet zich *mutatis mutandis* voor met betrekking tot het elektronische handtekening**certificaat** zelf[38]) (**opmerking**: dit doet geen afbreuk aan de volgende uiteenzettingen betreffende de aanwezigheid van het rijksregisternummer in het gekwalificeerde certificaat voor elektronische handtekeningen). Daarover ondervraagd, antwoordde de aanvrager het volgende:

> "**De naam van de houder moet worden opgenomen, aangezien deze in het certificaat moet worden vermeld.**
>
> *De wijze waarop de naam in het certificaat is opgenomen,* ***voldoet aan de eisen van de norm ETSI EN 319 412-2 V2.3.1 (2023-09)****:*
>
> • *NAT-4.2.4-10: In case of the (givenName and/or surname) alternative, if the* ***given name*** *of the subject is known, then the givenName attribute* ***shall be present****.*
> *NOTE 1: Some natural persons do not have both a given name and a surname.*
>
> • *NAT-4.2.4-11: In case of the (givenName and/or surname) alternative, if the* ***surname*** *of the subject is known, then the surname attribute* ***shall be present****.*
> *NOTE 1: Some natural persons do not have both a given name and a surname*
>
> • *NAT-4.2.4-12: The givenName with surname shall contain* ***formal representation*** *of the user's identity,* ***such as indicated on a user's official identity document****.*
>
> ***De naam komt dus overeen met de naam zoals die op de identiteits- en verblijfskaarten staat afgedrukt."*** (Engelse tekst vetgedrukt door de aanvrager, Nederlandse tekst vetgedrukt door de Autoriteit)

[38] Zie punt 43.

39. De Autoriteit neemt nota van dit antwoord en begrijpt dus dat de bijkomende voornamen (die niet nodig zijn wanneer ook een unieke identificator wordt gebruikt) uiteindelijk moeten worden opgenomen in het certificaat (en het register van gebruikersaccounts), **a priori vanwege de in België gemaakte keuze** (de Autoriteit **sluit niet uit** dat er in dit verband andere internationale verplichtingen voor België van toepassing kunnen zijn en voert hierover geen analyse uit) **om deze voornamen op de elektronische identiteitskaart zelf te vermelden.** De Autoriteit **trekt deze keuze/deze stand van het recht niet in twijfel.** In het kader van het onderhavige advies kan en behoort zij deze kwestie niet grondig te analyseren.

40. Zij wijst de aanvrager er echter in principe op dat, **indien een technische norm krachtens het Europees recht verplicht wordt gesteld, het aan de wetgever is om, voor zover mogelijk, het Belgisch recht zodanig aan te passen dat deze norm kan worden toegepast in overeenstemming met het in de AVG vastgelegde beginsel van minimale gegevensverwerking.**

41. De aanvrager heeft ook verduidelijkt dat "*overeenkomstig artikel 2, § 5, een actief account vereist is: 'Om gekwalificeerde elektronische handtekeningen te plaatsen via de dienst voor gekwalificeerde elektronische handtekeningen dient de gebruiker een actiefve gebruikersaccount te hebben en een geldig gekwalificeerd handtekeningcertificaat.' **Dit is geen gegeven in het register, maar veeleer een eigenschap van het account."***Bovendien wordt in het ontwerp niets vermeld over de gegevens die via het **gebruikersaccount** zelf zouden worden verwerkt. Op vragen hierover en over de relevantie van het onderscheid tussen het gebruikersaccount en het register van gebruikersaccounts, verklaarde de aanvrager het volgende: "***De verwerkte gegevens worden vermeld in artikel 3, § 5, van het ontwerp***." (vetgedrukt door de Autoriteit) **De Autoriteit neemt derhalve kennis van het feit dat er geen andere gegevens worden verwerkt in het gebruikersaccount en het register van gebruikersaccounts.** Opmerking: deze vaststelling doet geen afbreuk aan de verdere uiteenzettingen in dit advies met betrekking tot de logregistratie.

42. Wat het gebruik van het gebruikersaccount betreft, bepaalt artikel 3, § 2, dat een gebruiker zich via zijn eID (of de federale portemonnee voor digitale identiteit) moet authenticeren om het account **aan te maken**. Het ontwerp **vermeldt daarentegen niet dat voor het verdere gebruik van het account** (om een certificaat voor elektronische handtekeningen te verkrijgen en/of documenten te ondertekenen) **dezelfde identificatie en authenticatie vereist zijn**. Artikel 4, § 2, bepaalt enkel: "*Telkens wanneer de **uitgifte van een gekwalificeerd handtekeningcertificaat** wordt gevraagd, **controleren** de Federale Overheidsdienst Binnenlandse Zaken en de Federale Overheidsdienst Beleid en Ondersteuning **eerst de identiteit van de gebruiker en de geldigheid van het gebruikersaccount**."* (vetgedrukt door de Autoriteit) Het gebruikte controlemiddel wordt niet vermeld. Het ge-

bruik van de dienst voor **elektronische handtekeningen** wordt overigens niet genoemd. De Autoriteit gaat ervan uit dat al deze gevallen eenzelfde betrouwbaarheidsniveau voor identificatie en authenticatie vereisen als voor het aanmaken van een account. Op vragen hierover antwoordde de aanvrager het volgende:

> "Het ontwerp vermeldt in artikel 4, § 2: *Telkens wanneer de uitgifte van een gekwalificeerd handtekeningcertificaat wordt gevraagd, controleren de Federale Overheidsdienst Binnenlandse Zaken en de Federale Overheidsdienst Beleid en Ondersteuning eerst de identiteit van de gebruiker en de geldigheid van het gebruikersaccount.*
> *Het gebruik van de dienst is mogelijk via de streng beveiligde identificatiemiddelen, zoals* ***bijvoorbeeld*** *de Belgische portemonnee voor digitale identiteit (d.w.z. de MyGov.be-app) of de federale authenticatiedienst (CSAM FAS) in combinatie met het authenticatiecertificaat van identiteitskaarten en vreemdelingenkaarten."* (vetgedrukt door de Autoriteit)

43. De Autoriteit stelt vast dat **de identiteit van de betrokkene moet worden gecontroleerd wanneer deze via zijn gebruikersaccount gebruikmaakt van de in het ontwerp voorziene vertrouwensdiensten[39], overeenkomstig artikel 24, lid 1 bis, van de eIDAS-verordening[40].**

II.4.2 Gekwalificeerd handtekeningcertificaat en rijksregisternummer

44. Wat het **gekwalificeerd handtekeningcertificaat** betreft, bepaalt **artikel 4, § 4**, van het ontwerp dat het de volgende gegevens bevat: het rijksregisternummer van de houder van het gebruikersaccount, de naam van de houder van het gebruikersaccount, de eerste voornaam en, indien van toepassing, de tweede voornaam en de eerste letter van de derde voornaam, en het serienummer van het gekwalificeerde handtekeningcertificaat. **Paragraaf 5** van datzelfde artikel machtigt de vertrouwende partijen[41] *"om het rijksregisternummer te* ***bewaren*** *zolang als nodig is om een* ***bewijs van de elektronische handtekening of authenticatie*** *te verkrijgen, en* ***het te gebruiken met als enig doeleinde de verificatie*** *van de elektronische handtekening van de gebruiker"*.

45. Om te beginnen, en zonder afbreuk te doen aan de meer fundamentele toelichting die hierna volgt (punten nrs. 48 e.v.), **geeft artikel 4, § 5, van het ontwerp aanleiding tot de volgende drie opmerkingen**. Ten eerste merkt de Autoriteit op dat de vertrouwende partij **zich niet noodzakelijkerwijs zal kunnen beperken tot het "bewaren"** van het rijksregisternummer. Zodra dit nummer

---

[39] Met inbegrip van de dienst voor het aanbrengen van handtekeningen, voor zover deze niet beschikbaar lijkt te zijn buiten de elektronische handtekening via het in het ontwerp bedoelde QSCD op afstand.

[40] Zie de punten 6-8.

[41] Namelijk *"een natuurlijke of rechtspersoon die vertrouwt op elektronische identificatie, Europese portemonnees voor digitale identiteit of andere elektronische identificatiemiddelen, of op een vertrouwensdienst"*, artikel 3, punt 6, van de eIDAS-verordening.

is opgenomen in het certificaat dat in het ondertekende document is geïntegreerd, zal elke **mededeling van dit document waarbij een document moet worden verstrekt dat gelijkwaardig is aan het origineel** (dat wil zeggen een mededeling van het document die niet kan plaatsvinden zonder het document te bewerken om de elektronische handtekening en het certificaat te verwijderen), ook een mededeling van het rijksregisternummer aan de entiteit waaraan het wordt verstrekt, inhouden. Met andere woorden, de verwerking van het rijksregisternummer gaat waarschijnlijk verder dan louter het bewaren ervan. Het is aan de aanvrager om terminologie te gebruiken die is aangepast aan de praktijken die ook op het gebied van de uitwisseling van ondertekende documenten moeten worden toegestaan.

46. Ten tweede: als deze bepaling ook tot gevolg heeft dat **de verdere verwerking van het rijksregisternummer wordt verboden**, verdient een nog explicietere formulering de voorkeur. Zonder de toepassing van een eventuele wettelijke verplichting (wat in de ontwerpbepaling als voorbehoud moet worden opgenomen, anders zou deze als *lex posterior* de toepassing van eventuele wettelijke verplichtingen kunnen verhinderen), ziet de Autoriteit geen legitieme reden waarom het rijksregisternummer voor een ander doel zou mogen worden verwerkt dan het vaststellen (het bewijzen en verifiëren) van de elektronische handtekening. Met andere woorden, het verbod op elke andere verdere verwerking van het rijksregisternummer, onverminderd een eventuele wettelijke verplichting, zou moeten worden voorzien als passende waarborg in de zin van artikel 87 van de AVG.

47. Ten derde begreep de Autoriteit niet goed waarom het certificaat voor elektronische handtekeningen volgens het ontwerp ook bewaard zou moeten worden als bewijs van een "**authenticatie**"(in principe wordt het authenticatiecertificaat gebruikt wanneer het gaat om identificatie en niet om ondertekening), en heeft zij de aanvrager hierover ondervraagd. Deze antwoordde het volgende: *"Het bewaren dient inderdaad om het bewijs van de elektronische handtekening te verzamelen, uitsluitend om de elektronische handtekening van de gebruiker te verifiëren. Authenticatie maakt hier deel van uit, maar is in dit geval geen afzonderlijk doel. De bepaling moet worden gewijzigd".* De Autoriteit neemt er nota van dat het ontwerp in die zin zal worden gewijzigd.

48. Hoe dan ook, **het ontwerp brengt meer in het algemeen en fundamenteel <u>de kwestie aan de orde van het gebruik van het rijksregisternummer in gekwalificeerde certificaten</u>** voor elektronische handtekeningen. Dit is een bekend onderwerp in het Belgische recht. Ter herinnering: de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen* (hierna de "**RR-wet**") moest al worden hervormd om rekening te houden met het feit dat in België, **de elektronische identificatie en de gekwalificeerde elektronische handtekening, die gebaseerd zijn op de authenticatie- en handtekeningcertificaten op de Belgische elektronische iden-**

titeitskaart, de verwerking van het rijksregisternummer in deze context vereisen, aangezien dit nummer rechtstreeks op deze certificaten is opgenomen[42]. Dit betekent dat in een maatschappij waarin het gebruik van elektronische handtekeningen en identificatie voortdurend toeneemt, **er steeds meer particuliere partijen zijn waarmee de betrokkenen hun rijksregisternummer delen.**

49. In deze context, met het oog op de beoogde nieuwe dienst voor het aanmaken van elektronische handtekeningen, en gezien het bestaan van een bijkomend(e) identificator/nummer (namelijk *"het gebruikersaccountnummer van de houder van het gebruikersaccount",* en in de veronderstelling dat dit nummer niet is afgeleid van het rijksregisternummer), **heeft de Autoriteit de aanvrager gevraagd of er is overwogen om het rijksregisternummer niet langer te gebruiken in de certificaten voor elektronische handtekeningen**, en waarom een dergelijke oplossing in voorkomend geval zou zijn afgewezen. De Autoriteit ondervroeg de aanvrager hierover een eerste keer en deze antwoordde het volgende:

---

[42] Zie artikel 8, §§ 2-3, van de RR-wet:

" […]

§ 2. Bij het lezen van een elektronische identiteitskaart voor Belgen of een vreemdelingenkaart of ***bij de ontvangst van een elektronisch handtekeningcertificaat*** *of een elektronisch authenticatiecertificaat, wordt de kennisneming van het Rijksregisternummer op zich niet beschouwd als een gebruik van het nummer waarvoor een voorafgaande machtiging vereist is.*

§ 3. Een machtiging tot gebruik van het Rijksregisternummer is niet vereist indien het Rijksregisternummer uitsluitend gebruikt wordt met het oog op de identificatie en authenticatie van een natuurlijk persoon in het kader van een informaticatoepassing aangeboden door een private of openbare instelling van Belgisch recht of door de overheden, instellingen en personen, bedoeld in artikel 5, § 1.

Een machtiging tot gebruik van het Rijksregisternummer is niet vereist indien het Rijksregisternummer uitsluitend gebruikt wordt met het oog op de identificatie en authenticatie van een natuurlijke persoon in het kader van een informaticatoepassing aangeboden door een buitenlandse onderneming indien het gebruik voor dit doeleinde is gemachtigd door of krachtens een wet, een decreet of een ordonnantie, door de minister bevoegd voor Binnenlandse Zaken of door een andere bevoegde instantie.

De aanbieder van een informaticatoepassing mag het Rijksregisternummer niet gebruiken voor andere doeleinden, tenzij hij hiertoe gemachtigd is door of krachtens een wet, een decreet of een ordonnantie, door de minister bevoegd voor Binnenlandse Zaken.

De elektronische handtekening- en/of authenticatiecertificaten die het Rijksregisternummer bevatten, mogen zonder voorafgaande toestemming bewaard worden zolang het nodig is om het bewijs te leveren van de elektronische handtekening of van de authenticatie.

De aanbieder van een informaticatoepassing zoals bedoeld in het eerste en het tweede lid legt in een geëncrypteerd conversiebestand een link tussen het Rijksregisternummer en een identificatienummer eigen aan de aanbieder. De informatie uit dat conversiebestand mag enkel gebruikt worden voor het terugvinden van het identificatienummer eigen aan de aanbieder van de natuurlijke persoon die toegang wenst te krijgen tot de informaticatoepassing van de aanbieder van de informaticatoepassing of waarvan de gegevens worden uitgewisseld met een andere aanbieder van een informaticatoepassing.

[…]

§ 5. Een machtiging om het Rijksregisternummer te gebruiken is niet vereist wanneer het Rijksregisternummer gebruikt wordt voor de identificatie van een natuurlijke persoon door een aanbieder van een dienst voor elektronische identificatie van het niveau hoog of substantieel zoals bedoeld in de Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/ EG, die erkend is overeenkomstig het koninklijk besluit van 22 oktober 2017 tot vaststelling van de voorwaarden, de procedure en de gevolgen van de erkenning van diensten voor elektronische identificatie voor overheidstoepassingen of door een overheidsdienst die door of krachtens een wet, een decreet of een ordonnantie de opdracht heeft om een dienst voor gebruikers- en toegangsbeheer aan te bieden, uitsluitend voor de identificatie en authenticatie van een natuurlijke persoon die van op afstand toegang wenst te krijgen tot een informaticatoepassing van een aanbieder van een informaticatoepassing bedoeld in § 3." (vetgedrukt door de Autoriteit)

"*Als antwoord op deze bezorgdheid zullen i**n de toekomst beroepscertificaten worden afgegeven** aan personen die voor de federale overheid werken en een specifieke functie uitoefenen. In dat geval wordt niet **de werkelijke identiteit van de persoon achter het certificaat vermeld, maar wel de rol van die persoon**. Zo zal een boete bijvoorbeeld geldig elektronisch worden ondertekend door een ambtenaar, maar ziet de burger in het certificaat niet de naam en het rijksregisternummer van de ambtenaar die heeft ondertekend. Het is daarentegen noodzakelijk dat de registratie-instantie (in dit geval de politie) altijd de werkelijke identiteit van de ambtenaar kent en weet wie een handtekening heeft geplaatst. Indien nodig zal de registratie-instantie deze informatie in bepaalde situaties moeten vrijgeven. De registratie-instantie zal het beroepscertificaat moeten intrekken wanneer de ambtenaar deze functie niet langer vervult (in geval van ontslag, pensionering, schorsing, enz.).*"
(vetgedrukt door de Autoriteit)

De Autoriteit heeft **de aanvrager hierover opnieuw ondervraagd**, aangezien haar vraag veel verder reikt. Hij antwoordde het volgende:

"*Hieronder vindt u onze reactie op het gebruik van het rijksregisternummer in de certificaten (in aansluiting op wat is uiteengezet in het dossier met referentie **DOS-2021-06312***[43]):

***De optie** om het rijksregisternummer te vervangen door een alternatieve identificator (bijvoorbeeld een uniek serienummer) **is onderzocht**.*
In de context van de Belgische overheidsdiensten vormt het rijksregisternummer de unieke administratieve identificator** waarmee op duidelijke wijze de link met een natuurlijke persoon kan worden gelegd, **met name in de relaties met overheidsinstanties en met bepaalde particuliere instellingen die onderworpen zijn aan wettelijke identificatieverplichtingen en verplicht zijn het rijksregisternummer te gebruiken.
*Het gebruik van een **alternatieve identificator** zou de invoering van een **koppelingsdienst** vereisen om **de link** tussen deze identificator en het rijksregisternummer **te leggen.***
*Een dergelijk mechanisme zou **onmisbaar zijn voor overheidsinstanties en organisaties die wettelijk verplicht zijn** om een persoon formeel te **identificeren**.*
*Aangezien een elektronisch ondertekend document **rechtsgevolgen heeft ten aanzien van derden,** moet de ontvanger de ondertekenaar **op duidelijke en ondubbelzinnige wijze kunnen identificeren. In het Belgische rechtssysteem berust deze duidelijke***

[43] [Dit dossier heeft geleid tot Beslissing ten gronde 65/2025 van 3 april 2025 van de Geschillenkamer van de Autoriteit, beschikbaar op https://gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr. -65-2025.pdf, laatstelijk geraadpleegd op 16/02/2026. Het betreft een beslissing tot seponering waarin de Geschillenkamer zich niet rechtstreeks uitspreekt over de kwestie die in dit advies aan de orde wordt gesteld ("*De litigieuze verwerking in onderhavige zaak is de onrechtmatige publicatie van ongeveer 40.000 handtekening- en authenticatiecertificaten van Belgische burgers in één van de CT-logs van Google waardoor de vertrouwelijkheid van de persoonsgegevens geschonden werd. De vraag rijst wie als verwerkingsverantwoordelijke moet worden aangeduid voor deze litigieuze verwerking.*")].

identificatie op de unieke administratieve identificator*, namelijk het rijksregisternummer.*

De vervanging van het rijksregisternummer zou de verwerking ervan dus niet opheffen, maar ***het gebruik ervan verplaatsen naar een bijkomende koppelingsinfrastructuur****, wat* ***extra technische complexiteit en een bijkomend centraal punt voor gegevensverwerking*** *met zich meebrengt, met een* ***structurele afhankelijkheid*** *van deze intermediaire dienst.*

Onder deze omstandigheden biedt deze optie ***geen echte meerwaarde in het licht van de beginselen van de AVG****, met name wat betreft minimale gegevensverwerking en gegevensbeveiliging, terwijl ze wel* ***aanzienlijke operationele en organisatorische nadelen*** *met zich meebrengt. Daarom is er niet voor gekozen*." (vetgedrukt en onderstreept door de Autoriteit)

50. De Autoriteit neemt akte van het antwoord van de aanvrager, dat haar **in de huidige vorm echter niet volledig overtuigend** lijkt, en wel om de volgende redenen:

- Er moet een **onderscheid worden gemaakt tussen de gekwalificeerde elektronische handtekening en de identificatie/authenticatie van de betrokkenen als zodanig**, met name wanneer deze identificatie/authenticatie op een wettelijke verplichting berust. Het ontwerp zelf is op dit onderscheid gebaseerd[44], aangezien het authenticatiecertificaat op de chip van de Belgische elektronische identiteitskaart altijd kan worden gebruikt voor identificatie en authenticatie, en door de gebruiker ook daadwerkelijk zal worden gebruikt om een account aan te maken en zo gebruik te maken van de in het ontwerp voorziene dienst[45]. Met andere woorden: het feit dat het rijksregisternummer niet wordt gebruikt in het gekwalificeerde certificaat voor elektronische handtekeningen, sluit de mogelijkheid van identificatie met behulp van het rijksregisternummer niet uit in gevallen waarin, zoals de aanvrager aangeeft, sprake is van contact met een **overheidsinstantie** of een **particuliere entiteit** die een **specifieke wettelijke verplichting** heeft **tot identificatie** van haar "klanten"[46]. Dit is mogelijk via het authenticatiecertificaat. Wat de identificatie betreft, zou het dus niet nodig zijn om een eventuele *"koppelingsdienst"* op te zetten;

[44] Zie de punten 4-8.

[45] Opmerking: de Autoriteit neemt hier geen standpunt in over de kwestie van het meedelen van het rijksregisternummer aan particuliere entiteiten die om identificatie vragen, aangezien er geen specifieke wettelijke verplichting op dit gebied bestaat. Het onderhavige advies heeft geen betrekking op de kwestie van identificatie/authenticatie als zodanig.

[46] Opgemerkt moet worden dat particuliere entiteiten in sommige van deze gevallen zelfs het recht hebben om het Rijksregister te raadplegen (in het kader van de strijd tegen het witwassen van geld, zie Advies nr. 14/2025 van 27 februari 2025 betreffende een wetsvoorstel tot delen van data uit authentieke bronnen met erkende dienstverleners voor elektronische identificatiemiddelen (DOC56 0330/001) en een daarmee verband houdend amendement (DOC56 0330/002) (CO-A-2025-003), punt nr. 50). Dat geeft wel aan hoezeer deze situatie verschilt van louter het gebruik van een elektronische handtekening, zelfs als die gekwalificeerd is.

- De aanvrager geeft aan dat *"aangezien een elektronisch ondertekend document rechtsgevolgen heeft ten aanzien van derden, de ontvanger de ondertekenaar op duidelijke en ondubbelzinnige wijze moet kunnen identificeren. In het Belgische rechtsstelsel berust deze duidelijke identificatie op het unieke administratieve identificatienummer, namelijk het rijksregisternummer".* Allereerst zijn er **talrijke situaties waarin een handeling met rechtsgevolgen voor derden kan plaatsvinden zonder dat het rijksregisternummer** van de betrokkenen wordt verwerkt, en zonder dat dit overigens moet (of kan) gebeuren[47] (talrijke transacties in de elektronische handel/digitale economie illustreren dit). De identificatie van een persoon is, met name in de relaties tussen particulieren[48], een relatief begrip dat moet worden beoordeeld in het licht van het doel van de betreffende gegevensverwerking. Bijlage I van de eIDAS-verordening bepaalt dat het gekwalificeerde certificaat (c) *"op zijn minst de naam van de ondertekenaar [bevat] of een pseudoniem; als er een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven"*. Maar nog fundamenteler is dat **een gekwalificeerde elektronische handtekening, per definitie en overeenkomstig de eIDAS-verordening, inhoudt dat de identiteit van de betrokkene door de gekwalificeerde verlener van vertrouwensdiensten is gecontroleerd via een van de methoden bedoeld in artikel 24, lid 1 bis, van de eIDAS-verordening.** Met andere woorden: in een dergelijke situatie is het in principe niet nodig dat de partij aan wie het ondertekende document wordt meegedeeld, het rijksregisternummer van de betrokkenen kent, aangezien het gebruik van een gekwalificeerde elektronische handtekening al inhoudt dat de betrokkene met een hoge mate van betrouwbaarheid is geïdentificeerd;

- De aanvrager merkt verder op: *"De vervanging van het rijksregisternummer zou de verwerking ervan dus niet opheffen, maar het gebruik ervan verplaatsen naar een bijkomende koppelingsinfrastructuur, wat extra technische complexiteit en een bijkomend centraal punt voor gegevensverwerking met zich meebrengt, met een structurele afhankelijkheid van deze intermediaire dienst".* Ten eerste voorziet het ontwerp juist in de invoering van een nieuwe dienst en daarmee de facto een nieuwe infrastructuur, in het kader waarvan overigens **gebruikersaccounts** zullen worden aangemaakt en beheerd waaraan een identificator wordt toegekend (binnen een register van gebruikersaccounts). Ten tweede geeft de aanvrager zelf aan dat de mogelijkheid wordt overwogen om **beroepscertificaten[49]** aan te maken voor personen die voor de federale overheid werken en een specifieke functie uitoefenen (zou er niet ook een specifiek handtekeningcertificaat kunnen worden aangemaakt voor relaties met

---

[47] Over de noodzaak van identificatie, zie advies nr. 69/2025 van 26 augustus 2025 met betrekking tot de "*Nationale Cybersecurity Strategie* 3.0, 2026-2030" (CO-A-2025-108), punten 16-19.

[48] Ook bij contacten met een overheidsinstantie is identificatie op basis van het rijksregisternummer niet altijd vereist (een burger kan bijvoorbeeld gewoon een algemene vraag stellen aan een overheidsinstantie).

[49] De Autoriteit neemt in dit advies geen standpunt in ten aanzien van deze piste en de informatie die de aanvrager hierover heeft verstrekt.

de publieke sector?) (**<u>opmerking</u>**: de Autoriteit wijst er terloops op dat organisaties in het kader van de eIDAS-verordening gebruik kunnen maken van **gekwalificeerde elektronische zegels**). Ten derde blijft, zoals reeds opgemerkt, een **authenticatiecertificaat** in ieder geval elders beschikbaar. Kortom, **de Autoriteit beschikt niet over overtuigende concrete informatie om te concluderen dat de bijkomende complexiteit** die gepaard gaat met de afgifte van gekwalificeerde certificaten voor elektronische handtekeningen zonder het rijksregisternummer, **in de praktijk onoverkomelijk is of qua kosten onhaalbaar is in het licht van het comparatieve voordeel** dat gekwalificeerde certificaten voor elektronische handtekeningen zonder rijksregisternummer op het gebied van gegevensbescherming zouden opleveren;

- Ten slotte, en dit is een onderwerp dat buiten de reikwijdte van dit advies valt, **zou men ook kunnen overwegen dat het rijksregisternummer, oorspronkelijk een instrument van de publieke sector, in feite en voortaan als een persoonsgegeven moet worden beschouwd, waarbij de voorwaarden voor de verwerking ervan door particuliere entiteiten in het kader van de digitale economie in het algemeen moeten worden versoepeld**[50]**.** Een dergelijke hervorming van de manier waarop particuliere entiteiten omgaan met het rijksregisternummer zou op zich moeten worden onderzocht, met name in het kader van een gegevensbeschermingseffectbeoordeling. De Autoriteit wijst er in dit verband alleen op dat een nationaal identificatienummer een bijzonder soort persoonsgegeven is dat, overeenkomstig artikel 87 van de AVG *"alleen gebruikt [wordt] met passende waarborgen voor de rechten en vrijheden van de betrokkene uit hoofde"* van de AVG. Het Belgische recht heeft het gebruik van het rijksregisternummer specifiek geregeld. Het handhaven van een technische oplossing waarbij het rijksregisternummer een gegeven is dat is opgenomen in het gekwalificeerde certificaat voor elektronische handtekeningen, heeft tot gevolg dat de rijksregisternummers van de Belgische bevolking op grote schaal worden verspreid en verwerkt, temeer daar er in de huidige samenleving steeds vaker gebruik zal worden gemaakt van elektronische handtekeningen. **Tenzij er een paradigmaverschuiving plaatsvindt, levert het op het gebied van gegevensbescherming dus wel degelijk een reële meerwaarde op** om te voorzien in gekwalificeerde certificaten voor elektronische handtekeningen zonder rijksregisternummer.

[50] Als we deze redenering verder doortrekken, in omgekeerde richting, zou het gebruik van *<u>enkel</u>* het rijksregisternummer om de betrokkene te identificeren, de uitwisseling van persoonsgegevens over de betrokkene tot een minimum kunnen beperken, aangezien het zeker is dat er wereldwijd slechts één persoon is die door een Belgisch rijksregisternummer wordt geïdentificeerd. Maar dit is een scenario dat niet wordt overwogen en dat bovendien niet is voorzien (toegestaan) in het normatieve kader van de eIDAS-verordening (zie artikel 12, 3, d), van de eIDAS-verordening en de bijlage bij Uitvoeringsverordening (EU) nr. 2015/1501 van de Commissie van 8 september 2015 *betreffende het interoperabiliteitskader bedoeld in artikel 12, lid 8, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt*).

51. Samenvattend is de Autoriteit van mening dat **de argumenten die de aanvrager heeft aangevoerd om niet te voorzien in het aanmaken van gekwalificeerde certificaten voor elektronische handtekeningen zonder het rijksregisternummer, niet volledig overtuigend zijn.** De keuze die op dit gebied wordt gemaakt, **moet in elk geval worden onderworpen aan een grondige gegevensbeschermingseffectbeoordeling.** De aanvrager vermeldt in zijn aanvraagformulier echter dat een dergelijke analyse niet is uitgevoerd. Het is belangrijk dat dit alsnog gebeurt. (Opmerking: de Autoriteit is zich ervan bewust dat **identificatie** in private verhoudingen soortgelijke vragen oproept, die echter niet in dit advies aan de orde komen).

II.4.3 Logregistratie - logging

52. Wat betreft het **loggen – de logregistratie**, wat eveneens een verplichting is die voortvloeit uit de uitvoering van de AVG zelf, met betrekking tot de verwerking van persoonsgegevens, heeft de Autoriteit de aanvrager verzocht haar te verduidelijken welke bepalingen van het normatieve kader van **eIDAS** (uitvoeringshandelingen van de Commissie, toepasselijke normen) voorzien in specifieke logregistratie (met het oog op de levering van vertrouwensdiensten), teneinde de categorieën van gegevens te kunnen identificeren die in deze context zullen worden verwerkt. Wanneer een betrokkene bijvoorbeeld gebruikmaakt van de dienst voor het aanmaken van elektronische handtekeningen of via de in het kader van het ontwerp ter beschikking gestelde dienst een handtekening op een document "plaatst", welke sporen worden dan bewaard met betrekking tot deze handeling (worden bijvoorbeeld ook de titel en de eigenschappen van het ondertekende document geregistreerd?)? De aanvrager antwoordde het volgende: *"Wat het gebruik van de dienst voor elektronische handtekeningen betreft, wordt* ***het activeren van de privésleutel om een handtekening te plaatsen geregistreerd, maar er is geen enkel spoor van het document dat wordt ondertekend****."* (vetgedrukt door de Autoriteit). De Autoriteit neemt hier akte van.

53. Toen hem werd gevraagd naar de bewaartermijn van de loggegevens, verklaarde de aanvrager ook het volgende

> *"De* ***FOD BOSA*** *registreert en controleert de* ***gebruikersaccounts*** *en* ***bewaart de volgende gegevens gedurende 10 jaar****:*
> - *Naam;*
> - *Voornaam;*
> - *CanSign (true or false);*
> - *Datum van aanmaak van het account;*
> - *Datum van wijziging van het account;*
> - *Reden van stopzetting van het account;*
> - *Ondertekening van de algemene voorwaarden;*

- *Actie om de privésleutel te activeren voor het plaatsen van een handtekening (zonder het document).*

*Wat de **logs met betrekking tot de certificaten** betreft, bevat de databank niets meer dan de gegevens die in het certificaat zijn opgenomen, evenals de gebeurtenissen die verband houden met de levenscyclus van het certificaat: ontvangst van de certificaataanvraag, aanmaak en beheer van het certificaat. De gegevens op het certificaat worden door ZETES NV, de verwerker van de FOD BOSA en de FOD IBZ, gedurende 7 jaar bewaard, **in overeenstemming met de vereisten van de eIDAS-verordening.***

eIDAS -> CIR 2025/1943 -> ETSI 319 411-2 6.4.6 -> ETSI 319 411-1 6.4.6:

6.4.6 Records archival

NOTE: ETSI TS 119 511 [i.22] suggests provisions on how to preserve digital data objects.

OVR-6.4.6-01: The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:

a) log of all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA (see requirement **GEN-6.4.5-08**);

b) documentation as identified in clause 6.3.4.

***De raadplegingslogs van het Rijksregister worden geregeld door artikel 17 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van natuurlijke personen**.*" (door de Autoriteit vetgedrukt).

54. De Autoriteit neemt akte van dit antwoord. Het is echter mogelijk onvolledig: wat geldt er voor de logregistratie met betrekking tot de dienst voor het **plaatsen** van elektronische handtekeningen, ervan uitgaande dat het doel van het ontwerp inderdaad is om ook deze dienst te reguleren[51]? Gezien het belang van logregistratie in het kader van het ontwerp en de levering van de betreffende gekwalificeerde vertrouwensdiensten, is de Autoriteit van mening dat **de aanvrager zou kunnen overwegen** om in het ontwerp, of liever gezegd in een uitvoeringsbesluit daarvan, **de te implementeren logregistratie** (gegevens en bewaartermijn daarvan) **vast te leggen, voor zover deze niet reeds is gedefinieerd in het normatieve kader** (met inbegrip van de toepasselijke technische normen) **van de eIDAS-verordening zelf**. Het is aan de aanvrager om na te gaan en te motiveren of er al dan niet een aanvullend normatief kader nodig is voor het reguleren van de verwerkingen van loggegevens die nodig zijn voor de uitvoering van het ontwerp.

[51] Zie punt 21.

II.5 Bewaartermijn van de gegevens

55. Artikel 3, § 5, van het ontwerp bepaalt dat de gegevens uit het register van gebruikersaccounts[52] worden bewaard *"gedurende 30 jaar na stopzetting"* van het account. De memorie van toelichting vermeldt: *"Deze termijn werd vastgesteld met inachtneming van de maximale verjaringstermijn die mogelijk is in het Belgische recht."* De Autoriteit heeft de aanvrager gevraagd om aan te geven om welke verjaringstermijn het ging (wettelijke basis). Hij antwoordde het volgende:

> *"We hebben gekozen voor deze termijn van 30 jaar omdat dit de termijn is die geldt voor gegevens die zijn opgenomen in het Rijksregister van natuurlijke personen.*
> *Om te voorkomen dat dezelfde informatie die in verschillende databanken is opgeslagen, in de ene wordt gewist en in de andere toch wordt bewaard, leek het ons noodzakelijk de bewaartermijnen van de informatie op elkaar af te stemmen, aangezien deze termijn overeenkomt met de maximale verjaringstermijn (weliswaar voornamelijk op strafrechtelijk gebied) die van toepassing is in het nationale recht."*

56. De bewaartermijn van de gegevens **moet door het ontwerp worden vastgesteld in het licht van het door het ontwerp nagestreefde doel**. Het feit dat dezelfde gegevens voor verschillende termijnen kunnen worden bewaard in verschillende systemen die verschillende doelen dienen, is logisch vanuit het oogpunt van de AVG en artikel 8 van het EVRM en artikel 22 van de Grondwet. Het in het ontwerp voorziene register van gebruikersaccounts heeft niet hetzelfde doel als het Rijksregister van natuurlijke personen. Voor elk doeleinde van de verwerking moet worden beoordeeld hoe lang de gegevens moeten worden bewaard. Bovendien ziet de Autoriteit niet direct het logische verband tussen de bewaartermijn van de gegevens in het register van gebruikersaccounts en de maximale verjaringstermijn volgens het Belgische recht (hoewel de Autoriteit deze analyse niet maakt, kan men zich zelfs afvragen wat de concrete meerwaarde is van deze gegevens, die op zichzelf eigenlijk alleen een persoon aan een gebruikersaccount en het bijbehorende nummer koppelen).

57. **Het is aan de aanvrager om in de memorie van toelichting bij het ontwerp de bewaartermijn te motiveren die hij in zijn ontwerp vaststelt en deze termijn, in voorkomend geval, aan te passen indien deze niet in overeenstemming is met de hierboven genoemde beginselen.**

58. Meer fundamenteel gezien worden in artikel 3, § 5, van het ontwerp slechts weinig gegevens genoemd, en het is duidelijk dat andere categorieën van persoonsgegevens door de FOD Binnenlandse Zaken en

[52] Zie punt 37.

de FOD Beleid en Ondersteuning zullen worden verwerkt, zoals bijvoorbeeld loggegevens met betrekking tot het aanmaken en beheren van certificaten of met betrekking tot het beheer van accounts en het gebruik van de dienst voor elektronische handtekeningen, en bovendien, gegevens ter controle van de voorwaarden waaraan moet worden voldaan in verband met de gebruikersaccounts. De Autoriteit heeft de aanvrager hierover ondervraagd en deze heeft de in punt 53 genoemde antwoorden verstrekt, waarover de Autoriteit haar standpunt in punt 54 heeft uiteengezet. Uiteindelijk zal het, in de huidige stand van het ontwerp, aan de verwerkingsverantwoordelijken zijn om de bewaartermijn voor loggegevens vast te stellen, met name in overeenstemming met de technische normen die krachtens de eIDAS-verordening van toepassing zijn.

II.6 Diverse

59. In artikel 3, § 1, van het ontwerp staat dat de burger, om een gebruikersaccount aan te maken, akkoord moet gaan met de **algemene voorwaarden** die beschikbaar zijn via de website van de Algemene Directie Identiteit en Burgerzaken van de Federale Overheidsdienst Binnenlandse Zaken en van de Federale Overheidsdienst Beleid en Ondersteuning. De Autoriteit merkt op dat deze fase van het aanmaken van het gebruikersaccount ook nuttig kan worden gebruikt om de gebruiker naar behoren te informeren over de verwerkingen van persoonsgegevens door de FOD Binnenlandse Zaken en de FOD Beleid en Ondersteuning in uitvoering van het ontwerp, overeenkomstig de artikelen 12 en 13 van de AVG. In deze fase is het ook belangrijk om de betrokkenen duidelijk te informeren over de aangeboden diensten en over de mogelijkheid om elk van deze diensten afzonderlijk in te schakelen[53].

OM DEZE REDENEN,
is de Autoriteit de volgende mening toegedaan:

1. Op basis van de hypothese die is opgesteld aan de hand van de door de aanvrager verstrekte antwoorden, is het ingevoerde instrument geschikt om het nagestreefde doel te bereiken (het aanmaken van een gekwalificeerde elektronische handtekening op afstand) (**punten 4-8**);

2. De reikwijdte van het ontwerp (*"volledige herziening van onze bestaande dienst voor handtekeningen"*, het aanbieden van *de functionaliteit voor ondertekening via de Belgische portemonnee voor digitale identiteit"* en zeer waarschijnlijk het verdwijnen van de mogelijkheid voor de burger om op gekwalificeerde wijze elektronisch te ondertekenen door middel van een certificaat voor elektronische ondertekeningen op zijn elektronische

[53] Zie de punten 21-22.

identiteitskaart) moet beter worden benadrukt in de inleiding, in de memorie van toelichting bij het ontwerp.

Het verdient aanbeveling om de mogelijkheid te overwegen om een oplossing voor gekwalificeerde elektronische handtekeningen te handhaven van het type dat momenteel bestaat (ondertekening via een gekwalificeerd certificaat voor elektronische handtekeningen op de chip van de elektronische identiteitskaart), met dien verstande dat het aan de aanvrager is om na te gaan of dit al dan niet mogelijk is binnen het normatieve en technische kader van de eIDAS-verordening, zoals gewijzigd bij de eIDAS2-verordening. De keuze die op dit gebied wordt gemaakt, moet worden onderworpen aan een gegevensbeschermingseffectbeoordeling (**punten 9-12**);

3. Het ontwerp moet, in overeenstemming met de in de eIDAS-verordening gedefinieerde begrippen, duidelijk aangeven op welke diensten het van toepassing is, en het dispositief (voorwaarden voor toegang tot de dienst; logregistratie; verwerkingsverantwoordelijken) afstemmen op de betreffende diensten. Indien het de bedoeling van de aanvrager is om met zijn ontwerp een dienst voor het plaatsen van handtekeningen (een webapplicatie) aan te bieden, moet deze dienst worden gedefinieerd en moeten de werking en de levering ervan vervolgens op dezelfde wijze worden geregeld als de andere betrokken vertrouwensdiensten. Onverminderd hetgeen hierna volgt, wordt de analyse met betrekking tot dit punt niet voortgezet. Het ontwerp moet duidelijkheid verschaffen over het aanbod van de betreffende diensten aan de burgers: welke diensten kunnen afzonderlijk worden gebruikt en welke diensten moeten geïntegreerd worden gebruikt (**punten 17-24**);

4. Het ontwerp moet nader worden uitgewerkt om duidelijk vast te stellen welke entiteiten (al dan niet gezamenlijk) verantwoordelijk zijn voor welke verwerkingen van persoonsgegevens in het kader van de identificatie en authenticatie van gebruikers, en het leveren van de verschillende vertrouwensdiensten (of gewoon diensten) waarin het ontwerp voorziet. Wat betreft de gezamenlijke verantwoordelijkheden met betrekking tot de verwerking zoals voorzien in het ontwerp, zou de aanvrager, als aanvullende waarborg op het gebied van transparantie, moeten nagaan of het ontwerp niet zou kunnen voorzien in de publicatie van de overeenkomst die zal worden gesloten (**punten 25-36**);

5. In principe geldt dat indien een technische norm krachtens het Europees recht verplicht wordt gesteld, het aan de wetgever is om, voor zover mogelijk, het Belgisch recht zodanig aan te passen dat deze norm kan worden toegepast in overeenstemming met het in de AVG vastgelegde beginsel van minimale gegevensverwerking (**punt 40**);

6. Voor het gebruik van de in het ontwerp voorziene diensten door de betrokkene is een identiteitscontrole vereist, zoals bedoeld in artikel 24, lid 1 bis, van de eIDAS-verordening (**punten 42-43**).

7. Onverminderd het volgende punt moet artikel 4, § 5, van het ontwerp worden aangepast (**punten 44-47**);

8. De argumenten die worden aangevoerd om geen gekwalificeerde certificaten voor elektronische handtekeningen zonder het rijksregisternummer in te voeren, zijn niet helemaal overtuigend. Het handhaven van een technische oplossing waarbij het rijksregisternummer een gegeven is dat in het gekwalificeerde certificaat voor elektronische handtekeningen is opgenomen, houdt een aanzienlijke verspreiding en verwerking van de rijksregisternummers van de Belgische bevolking in, temeer omdat elektronische handtekeningen in de hedendaagse samenleving steeds vaker zullen worden gebruikt. De keuze die op dit gebied wordt gemaakt, moet in elk geval het voorwerp uitmaken van een gegevensbeschermingseffectbeoordeling (**punten 44-51**);

9. De aanvrager zou kunnen overwegen om in het ontwerp, of liever gezegd in een uitvoeringsbesluit daarvan, de te implementeren logregistratie vast te leggen (gegevens en bewaartermijn daarvan), voor zover deze niet reeds is gedefinieerd in het normatieve kader (met inbegrip van de toepasselijke technische normen) van de eIDAS-verordening. Het is aan de aanvrager om na te gaan en te motiveren of er al dan niet een aanvullend normatief kader nodig is voor het reguleren van de verwerkingen van loggegevens die nodig zijn voor de uitvoering van het ontwerp (**punten 52-54 en 59**);

10. Het is aan de aanvrager om in de memorie van toelichting bij het ontwerp de bewaartermijn te motiveren die hij in zijn ontwerp vaststelt en deze termijn, in voorkomend geval, aan te passen indien deze niet in overeenstemming is met de hierboven genoemde beginselen (**punten 55-57**).

Voor de Autorisatie- en Adviesdienst,
(get.) Alexandra Jaspar, Directeur