Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 36/2026 du 04 mars 2026

Objet : Avis concernant un avant-projet de loi créant un service de signatures électroniques qualifiées (CO-A-2026-002).

Mots-clés : signature électronique qualifiée ; Règlement EIDAS ; carte d'identité, eID.

Version originale

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier ses articles 23 et 26 (ci-après « LCA ») ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD ») ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD ») ;

Vu la demande d'avis de Madame Vanessa Matz, Ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'Etat, du Numérique et de la Politique Scientifique, recevable le 13 janvier 2025 ;

Vu la demande d'informations complémentaires adressée au demandeur le 22 janvier 2026 ;

Vu les informations complémentaires communiquées par le demandeur le 6 février 2026 ;

Vu la demande d'informations complémentaires adressée au demandeur le 9 février 2026 ;

Vu les informations complémentaires communiquées par le demandeur le 11 et le 13 février 2026 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 4 mars 2026, l'avis suivant :

L'Autorité ne publie en français et en néerlandais que les avis concernant les projets ou propositions de textes de rang de loi émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale ou de la Commission Communautaire Commune. La « Version originale » est la version qui a été validée.

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le demandeur a introduit auprès de l'Autorité, une demande d'avis concernant **un avant-projet de loi *créant un service de signatures électroniques qualifiées*** (ci-après « **le Projet** »). Le Projet s'inscrit dans le contexte normatif du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE* (ci-après, « **Règlement EIDAS** »), tel que modifié par le Règlement (UE) n° 2024/1183 du Parlement Européen et du Conseil du 11 avril 2024 *modifiant le Règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique* (ci-après, « **le Règlement EIDAS2** »[1]).

2. L'exposé des motifs du Projet indique que celui-ci « *vise à **créer un service de signatures électroniques qualifiées, mis à disposition des citoyens par le Gouvernement fédéral**. Ce service, opérationnalisé par le SPF Intérieur et le SPF Stratégie et Appui, permet*[trait] *aux citoyens de signer, en utilisant un certificat de signature activé à distance, avec une signature électronique qualifiée, au sens de l'article 3, 12° du* [Règlement EIDAS] » (mis en gras par l'Autorité). Pour accéder à ce service, le citoyen devra, moyennant authentification via sa carte d'identité électronique, créer un compte utilisateur dans un système d'information dont en substance, la responsabilité conjointe relèvera du SPF Stratégie et Appui et du SPF Intérieur.

3. Dans le cadre de la mise en état du dossier, le Demandeur a également indiqué à l'Autorité que ce service de signature électronique servira « *également à offrir la fonctionnalité de signature via le portefeuille belge pour l'identité numérique (c'est-à-dire l'application MyGov.be)* »[2].

II. EXAMEN DU PROJET

Le présent avis est structuré comme suit :

[1] Sur le sujet, voir l'Avis de l'Autorité n° 14/2025 du 27 février 2025 concernant une proposition de loi relative au partage de données provenant de sources authentiques avec les prestataires de services d'identification électronique agréés (DOC56 0330/001) et un amendement y lié (DOC56 0330/002) (CO-A-2025-003).

[2] Voir le considérant n° 9.

II.1. Motivation du Projet et sort, à terme, du certificat de signature électronique présent sur la carte d'identité

4. Le Projet est motivé par les considérations suivantes, extraites de son exposé des motifs :

> « […] *la révision du règlement eIDAS (dite "eIDAS 2.0") impose de* ***nouvelles conditions de certification pour les dispositifs de création de signature (Qualified Signature Creation Device - QSCD****). Ces conditions* ***remettent en question la validité des signatures électroniques apposées via les puces embarquées sur les eID****, dont la durée de validité n'est plus alignée sur les* ***nouvelles exigences européennes*** *(****certification QSCD valable 5 ans maximum, contre 10 ans de validité pour une carte eID****). Dès lors, à compter de 2026, les cartes d'identité émises avant mai 2021 (plusieurs millions) perdront leur capacité à produire des signatures électroniques qualifiées. C'est à l'origine de cette problématique qu'a été conçu le présent projet de loi, afin de* ***garantir la continuité de l'accès à la signature électronique qualifiée pour l'ensemble des citoyens et résidents en Belgique*** » (mis en gras par l'Autorité).
>
> « *Le recours à un tel service permet* ***également de répondre aux cas d'usages identifiés dans le cadre de la transformation numérique de l'administration*** *: dématérialisation des procédures, accessibilité sur appareils mobiles, absence de lecteur de carte, besoins de signature à distance pour les agents publics, etc.* » (mis en gras par l'Autorité).

5. Dans ce contexte, l'Autorité a tout d'abord invité le demandeur à lui **indiquer précisément les règles et normes pertinentes** (et à les communiquer si elles ne sont pas publiquement accessibles) concernant la certification des « **QSCD** » (« **Qualified Signature Creation Device** »), tant concernant la carte d'identité électronique actuelle que concernant les nouvelles règles (certification valable 5 ans) du Règlement EIDAS. Elle lui a également demandé de préciser pour quelles raisons, sur les plans juridique et technique, la validité (trop longue) de la certification des puces de l'eID belge[3] ne poserait pas également un problème dans le cadre du service de signature électronique mis en œuvre en vertu du Projet, dès lors que l'accessibilité et l'utilisation de ce service repose sur une identification et une

[3] Voir https://repository.eidpki.belgium.be/, dernièrement consulté le 20/01/2026.

authentification[4] fondée elle-même sur la carte eID belge. Et enfin, elle l'a invité à lui confirmer que le QSCD désormais utilisé serait alors un système d'information du SPF Intérieur et/ou du SPF Stratégie et Appui (système sur lequel se trouveront donc les clés privées des personnes concernées).

6. Celui-ci a répondu ce qui suit :

> « *Le **règlement eIDAS** définit à **l'article 30** les exigences relatives à la certification des QSCD. L'annexe II du règlement eIDAS définit les exigences relatives aux QSCD.*
>
> *La 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] *établit les normes spécifiques relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique* » (hyperliens omis et mis en gras par l'Autorité).
>
> « *L'utilisation d'un QSCD est l'une des trois exigences légales pour une signature électronique qualifiée, comme le stipule l'article 3 qui détermine les définitions du Règlement eIDAS :*
> *"signature électronique qualifiée" :*
> - *une signature électronique avancée*
> - *qui a été créée à l'aide d'un dispositif qualifié pour la création de signatures électroniques*
> - *et qui est basée sur un certificat qualifié pour les signatures électroniques ; " ;*
>
> *En vertu de l'article 51 Mesures transitoires, la reconnaissance de dispositifs sécurisés de création de signature reconnus sur la base de la directive européenne 1999/93/CE en tant que QSCD expire à compter du 21/05/2027 et donc la deuxième exigence pour une signature électronique qualifiée n'est plus remplie.*
>
> […]
>
> *À titre complémentaire et à titre d'information, les certificats qualifiés délivrés conformément à la directive 1999/93/CE ne seront plus reconnus comme certificats qualifiés à partir du 21/05/2026 et ne satisferont plus à l'exigence 3 de la définition.*
> *"Article 51 Mesures transitoires 2.* […]"

[4] Voir l'article 3, § 2, du Projet.

[5] Soit Décision d'exécution (UE) n° 2016/650 du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Les puces datant d'avant 2021 ne sont plus reconnues comme QSCD et ne peuvent donc plus créer de signature qualifiée. ***Pour l'authentification, l'utilisation d'un QSCD n'est pas une exigence****.*

La certification QSCD n'est donc pertinente que pour le QSCD qui génère la signature électronique qualifiée proprement dite*. Dans la nouvelle solution, ce dispositif sera toujours certifié QSCD.*
Pour délivrer le certificat qualifié, le prestataire de services de confiance doit ***vérifier l'identité du demandeur conformément à l'une des quatre méthodes mentionnées à l'article 24, paragraphe 1 bis,*** *du règlement eIDAS. Dans notre nouvelle solution, une des méthodes qui sera utilisée est la combinaison du service fédéral d'authentification et du certificat d'authentification figurant sur les cartes d'identité et de séjour, qui constitue un moyen d'identification électronique notifié de niveau élevé.*
Il convient également de noter que ***la nouvelle limite de validité de la certification QSCD est une limite purement administrative. L'expiration éventuelle de la certification n'indique aucun problème technique sous-jacent ni aucun risque pour la sécurité*** » (mis en gras par l'Autorité).

« *Le remote QSCD est* ***géré par le QTSP (représenté par le SPF BOSA et le SPF IBZ) et exploité par un prestataire de services****, ZETES SA.*
Le ***remote QSCD*** *est constitué du module Cryptomathic Signer SAM v6.0 associé au Hardware Security Module (HSM) Utimaco Cryptoserver CP5 v5.1.0.0 en tant que module cryptographique pour la génération et la protection des données de création de signature.* ***Les HSM***[6] ***fournissent un mécanisme de protection sécurisé pour le stockage des clés privées du titulaire à l'extérieur du HSM, sous forme chiffrée dans une base de données****.*
*Le Module d'Activation de Signature (****SAM***[7]*) est un module logiciel garantissant que les utilisateurs (c'est-à-dire les signataires) conservent le contrôle exclusif de leurs clés de signature. Il est chargé sur les HSM en tant qu'application locale. Le QSCD est exploité dans un environnement sécurisé.*
Les clés privées du titulaire sont stockées dans le QSCD uniquement selon les nécessités d'utilisation. *Lorsqu'une clé n'est plus nécessaire, elle est supprimée du QSCD. La clé privée est conservée dans un format sécurisé garantissant qu'elle ne peut être utilisée qu'à*

[6] Soit « Hardware Security Module ».
[7] Soit « Signature Activation Module ».

l'intérieur du QSCD pour effectuer des opérations de signature » (mis en gras et souligné par l'Autorité).

7. L'Autorité a réinterrogé le Demandeur à l'aune de sa réponse (« …*le stockage des clés privées du titulaire à l'extérieur du HSM, sous forme chiffrée dans une base de données* ») afin que celui-ci confirme bien que les clés sont uniquement traitées par le HSM en son sein, et qu'elles n'y sont pas accessibles. Celui-ci a répondu ce qui suit : « *Il n'est pas possible de conserver toutes les clés actives dans le QSCD lui-même, car elles sont trop nombreuses pour un tel appareil. De plus, un rQSCD dispose de plus d'un HSM opérationnel.* ***Les clés sont cryptées par le HSM afin que personne d'autre ne puisse les récupérer ou les utiliser*** » (mis en gras par l'Autorité).

8. Sur la base des réponses communiquées par le Demandeur, **le présent Avis se fonde sur l'hypothèse suivante**. L'article 30, 3*bis*., du Règlement EIDAS prévoit que la validité d'une certification des dispositifs de création de signatures électroniques qualifiées ne peut pas excéder 5 ans. Pour délivrer un certificat qualifié, le prestataire de service de confiance doit vérifier l'identité de la personne concernée sur la base d'un moyen d'identification prévu à l'article 24, 1*bis*., du Règlement EIDAS, à savoir par exemple, un moyen d'identification électronique notifié satisfaisant aux exigences énoncées à l'article 8 en ce qui concerne le niveau de garantie élevé. L'identification et l'authentification via la carte d'identité électronique belge répondent à ces exigences et il n'est pas nécessaire à cette fin, de recourir à un QSCD. Le « *remote QSCD* » relève de la responsabilité du SPF Intérieur et du SPF BOSA qui recourent afin de l'offrir à ses utilisateurs, aux services de l'entreprise Zetes. Les clés privées y sont stockées lors de leur utilisation et ne peuvent pas être accessibles. Non utilisées, elles sont chiffrées et stockées dans une banque de données externe par le HSM lui-même. Elles ne sont traitées que par le HSM, après authentification de la personne concernée pour la réalisation de signatures électroniques, demeurent inaccessibles et en sont supprimées dès qu'elles ne sont plus nécessaires. **Dans ce contexte, le dispositif mis en place est apte à accomplir l'objectif poursuivi, soit la création de signatures électroniques qualifiées à distance**.

9. Ensuite, à ce jour, un citoyen **peut utiliser sa carte d'identité électronique afin de signer des documents sans devoir recourir à un prestataire de service via internet**[8] à cette fin. Certes, la vérification de la validité d'un certificat par le destinataire d'un document signé nécessite quant à

[8] Dans le même sens, lire la réponse du SPF Economie à la question « Dois-je, dans tous les cas, faire appel à un prestataire de service pour réaliser une signature électronique qualifiée ? », disponible sur https://economie.fgov.be/fr/themes/line/commerce-electronique/signature-electronique-et, dernièrement consulté le 20/01/2026. Pour les listes de prestataires de services de confiances qualifiés, voir https://economie.fgov.be/fr/themes/line/commerce-electronique/signature-electronique-et et https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls, dernièrement consultés le 20/01/2026.

elle l'utilisation d'un service en ligne (**OCSP/CRL**, soit **Online Certificate Status Protocol/Certificate Revocation List**[9]). L'Autorité a interrogé le demandeur quant à la question de savoir ce qu'il en serait à terme de cette possibilité technique : **est-il envisagé de l'abandonner ou de revoir les conditions de mise à disposition des cartes d'identité électroniques** afin de maintenir cette possibilité dans le contexte réformé du Règlement EIDAS. Le demandeur a répondu ce qui suit :

> « *Il n'y a pas de décision formelle prise mais l'évolution rapide du contexte juridique et normatif rendra potentiellement impossible le maintien d'une solution de signature via un certificat de signature sur la carte d'identité électronique.*
> ***La nouvelle solution n'est en effet pas une solution temporaire, mais une refonte complète de notre service de signature existant****. L'article 5 bis, 5(g) du Règlement eIDAS stipule en outre qu'une fonctionnalité de signature gratuite doit être offerte aux citoyens via le portefeuille européen pour l'identité numérique.* ***Cette solution servira donc également à offrir la fonctionnalité de signature via le portefeuille belge pour l'identité numérique (c'est-à-dire l'application MyGov.be)*** » (mis en gras et souligné par l'Autorité).

10. L'Autorité prend acte de cette réponse et est d'avis que **la portée du Projet** (« *refonte complète de notre service de signature existant* », offre de « *la fonctionnalité de signature via le portefeuille belge pour l'identité numérique* » et fort probable disparition de la possibilité pour le citoyen, de signer électroniquement de manière qualifiée au moyen d'un certificat de signature électronique présent sur sa carte d'identité électronique) **devrait être mieux mise en évidence à titre introductif, dans l'exposé des motifs du Projet**.

11. En effet, sur le plan de la protection des données, **du point de vue de la proportionnalité et de la minimisation des données**, la solution prévue par le Projet **nécessite des traitements de données à caractère personnel supplémentaires par rapport à la solution de signature électronique encore actuellement disponible via la carte d'identité électronique**, et requiert *a priori* systématiquement une connexion à internet : connexion à un prestataire de service à distance ; création d'un compte utilisateur spécifique ; identification et authentification via ce compte ; génération fréquente de certificats de signature électronique à la validité limitée à 24 heures ; données de journalisation supplémentaires générées auprès des prestataires de service[10].

---

[9] Voir https://repository.eid.belgium.be/index.php?item=docs&lang=fr, dernièrement consulté le 20/01/2026 ; « *Les parties se fiant au certificat doivent utiliser les ressources en ligne que la CA met à leur disposition via son référentiel afin de vérifier l'état des certificats avant de s'y fier. La CA met à jour en conséquence l'OCSP, le service de vérification du statut de la certification par interface web, les CRL et les Delta CRL. Les CRL sont actualisées fréquemment, au minimum toutes les trois heures* », Certipost, « Politique belge de Certification et Déclaration de Pratique pour l'infrastructure PKI eID Citizen CA », version 5.0, 03/09/2024, p. 30, disponible sur https://repository.eid.belgium.be/downloads/citizen/fr/CPS_CitizenCA_BRCA34.pdf, dernièrement consulté le 20/01/2026.

[10] Voir le considérant n° 53.

12. Dans ce contexte, l'Autorité est d'avis qu'il est **recommandé d'envisager la possibilité de maintenir une solution de signature électronique qualifiée du type de celle qui existe actuellement** – signature via un certificat de signature électronique qualifié dont l'utilisateur dispose sur la puce de sa carte d'identité électronique –, étant entendu qu'il appartient au Demandeur de vérifier si cela est ou pas possible dans le cadre du Règlement EIDAS tel que réformé par le Règlement EIDAS2. A cet égard, l'Autorité comprend qu'une solution fondée sur la **carte d'identité électronique** nécessiterait, pour des raisons de certification de la puce électronique, de diminuer à 5 ans la validité des cartes électroniques. Ce qui représente une modification significative de la pratique actuellement en vigueur en Belgique dont la portée et le coût peuvent au mieux être évaluées par le Demandeur. Il s'agirait notamment de déterminer s'il est envisageable de systématiquement raccourcir la durée de validité des cartes d'identité électroniques ou plutôt, de **laisser au citoyen le choix (avec les conséquences y liées) d'une carte d'identité électronique avec ou sans certificat qualifié de signature électronique**. Pour le reste, l'Autorité est bien consciente du fait que le Règlement EIDAS prévoit également l'obligation de mettre en place des **portefeuilles européens d'identité numérique** qui notamment, offrent à toutes les personnes physiques la possibilité de signer, par défaut et gratuitement, au moyen de signatures électroniques qualifiées[11]. Une **autre possibilité** pourrait peut-être être envisagée par le Demandeur, à savoir de prévoir **après cinq ans, une nouvelle certification de la puce de la carte d'identité électronique (le QSCD)** de manière telle que la durée de vie de celle-ci puisse être prolongée si cette certification peut être octroyée. A cette fin, deux certificats de signature pourraient être placés sur la carte d'identité électronique : un actif pour une première période de cinq ans (de t à t+5) ; un second, inactif, qui pourrait uniquement être activé pour une seconde période de 5 ans (t+5 à t+10) (resterait à déterminer comment ce second certificat pourrait être activé auprès de la commune compétente)[12]. Le choix posé en la matière (maintien ou non d'un certificat de signature électronique sur la puce de la carte d'identité) doit être l'objet d'une **analyse d'impact relative à la protection des données**, qui le cas échéant et entre autres, démontrerait l'absence de plus-value, sur le plan de la protection des données, du maintien d'une solution de signature électronique basée sur la puce de la carte d'identité électronique belge, malgré la disponibilité de portefeuilles européens d'identité numérique.

[11] Article 5bis, 5., g), du Règlement EIDAS.

[12] L'hypothèse d'un certificat inactif présent sur la carte d'identité électronique existe déjà en droit positif (voir l'article 6, § 7, dernier alinéa, de la Loi du 19 juillet 1991 *relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour*. Et en pratique, sans que l'Autorité investigue cette possibilité, l'activation de ces certificats paraît techniquement faisable : voir par exemple,

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, dernièrement consultés le 04/03/2026.

II.2. Le service de signatures électroniques qualifiées prévu par le Projet

13. Le Projet prévoit la mise en place d'un « **service de signatures électroniques qualifiées** » mis à la disposition par le SPF Intérieur et le SPF BOSA. L'article 2, § 1er, 5°, du Projet définit ce service comme le « *service permettant **d'apposer** **via un certificat** de signature **à distance** une signature qualifiée au sens de l'article 3.12 du règlement eIDAS* » (mis en gras et souligné par l'Autorité). Cette dernière disposition définit la signature électronique qualifiée comme étant « *une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique* ». L'article 2, § 3, du Projet prévoit quant à lui que pour la « ***création à distance de signatures électroniques qualifiées via le service de signatures électroniques** qualifiées le Service public fédéral Intérieur et le Service public fédéral Stratégie et Appui **mettent à la disposition** des citoyens **des certificats** qualifiés de signature électronique* » (mis en gras et souligné par l'Autorité).

14. Ces activités correspondent à la **prestation d'au moins trois services de confiance** au sens du Règlement EIDAS, à savoir en tout cas : « *la délivrance de certificats de signature électronique* »[13], la « *création de signatures électroniques* »[14] et « *la gestion de dispositifs de création de signature électronique à distance* »[15]. L'Autorité a invité le demandeur à le confirmer et à lui indiquer dans ce contexte qui (et comment) offrirait un service de validation de la signature électronique[16] (un logiciel du type eID viewer sera-t-il mis à disposition des utilisateurs ? ; est-ce le SPF Intérieur, responsable des certificats en vertu de l'article 2, § 6, 1°, du Projet, qui mettra à disposition en ligne les ressources nécessaires (OCSP/CRL[17]) ?

15. Le demandeur a répondu ce qui suit :

> « *'Belgium Federal Government' est déjà aujourd'hui **QTSP pour les services de confiance suivants** :*
>
> - ***Qualified certificate for electronic signature***
> - *Qualified timestamp*
>
> *Dans un avenir proche, les services de confiance suivants viendront s'y ajouter :*
>
> - *Qualified certificate for electronic seal*
> - ***Qualified management of remote QSCDs*** ».

[13] Article 3, 16., a), du Règlement EIDAS.
[14] Article 3, 16., c), du Règlement EIDAS.
[15] Article 3, 16., f), du Règlement EIDAS.
[16] Article 3, 16., d), du Règlement EIDAS.
[17] Voir note de bas de page n° 9.

« ***Les certificats de signature pour les citoyens dans le nouveau service seront des certificats d'une durée de validité de 24 heures, ce qui rend inutile un service de statut tel que OCSP et CRL****. Cette durée de vie très courte réduit significativement la fenêtre d'exploitation en cas d'incident de sécurité, limite les risques liés à une révocation tardive et contribue ainsi à un niveau de sécurité globalement renforcé.*
Le eID viewer sert à lire l'eID et n'est donc pas lié à la nouvelle solution.
Le middleware eID sera mis à jour afin de permettre la signature via le nouveau service à l'aide d'applications de signature installées sur son propre PC*. Ce middleware eID est publié par le SPF BOSA : Télécharger | Logiciel eID Télécharger | Logiciel eID*
Par ailleurs, le ***SPF BOSA adaptera en parallèle sa plateforme de signature (SigningBox)*** *afin que les signatures puissent être apposées via le nouveau service de signature à distance. Le SigningBox utilisera le nouveau service* » (mis en gras et souligné par l'Autorité).

À la suite d'un questionnement subséquent, le Demandeur a confirmé ce qui suit : « *C'est un* ***standard d'utiliser des certificats valables un jour seulement pour les signatures à distance****. Dans ce cas,* ***l'OCSP ou la CRL ne sont plus nécessaires : si le certificat existe, il est valable.*** *Conformément à nos politiques existantes et les standards ETSI en matière d'eID, les certificats eID doivent être révoqués dans les 24 heures si nécessaire* » (mis en gras par l'Autorité) ;

16. L'Autorité prend acte du fait qu'un service disponible via **OCSP et les CRL ne sont plus pertinents dans le cadre de certificats d'une durée de validité de 24 heures** (sur ce point néanmoins, l'Autorité observe que les certificats générés pourraient même avoir une **durée de validité plus courte** que 24 heures – la durée de validité pourrait être limitée à une signature ou à une courte session) et ne seront donc pas disponibles dans le cadre du Projet. La vérification du fait que le certificat a bien été émis au moment concerné par le prestataire de service de confiance concerné suffira par conséquent[18]. En tout état de cause, l'Annexe I du Règlement EIDAS prévoit qu'un certificat qualifié doit notamment contenir des données de validation de la signature électronique correspondant aux données de création de la signature électronique, la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat et les informations ou l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

[18] Voir notamment la List of Trusted Lists (« LOTL ») mise à disposition par la Commission européenne, 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 ; dernièrement consultés le 16/02/2026.

17. L'Autorité a réinterrogé le Demandeur notamment quant aux points suivants : ce qu'il en est de la **<u>création</u> de signature électronique** en tant que telle ; le nouveau service permettra-t-il à la personne concernée de simplement obtenir un certificat de signature électronique qualifié à utiliser par ailleurs, via une application dont disposerait la personne concernée (ou s'agit-il d'intégrer le système de signature électronique à distance à ces autres applications ?). L'Autorité l'a également interrogé quant à l'opération consistant à **« apposer »** la signature électronique « *à distance* » (plutôt que « apposer » une signature électronique, le Règlement EIDAS utilise les termes « *signer au moyen de signatures électroniques qualifiées* »). Techniquement, **la signature électronique d'un document implique un traitement de ce document** (application au document d'une fonction cryptographique – création d'un hash –, ajout de données au document). En l'occurrence, l'Autorité a invité le demandeur à confirmer si ces opérations de traitement seront bien réalisées via le système d'information du SPF Intérieur/SPF Stratégie et Appui qui a cette fin, recevra par conséquent le document à signer. Dans l'affirmative, l'Autorité a interrogé le demandeur quant à la durée de conservation du document ainsi traité. Le demandeur a précisé ce qui suit :

18. Le Demandeur a répondu ce qui suit :

> « ***Il n'existe pas de service qualifié <u>pour l'apposition de signatures</u>, et le citoyen est libre de choisir celui qu'il souhaite (Adobe Reader est par exemple également une application permettant <u>d'apposer</u> des signatures)***. *Nous n'incluons donc pas l'apposition de signatures dans l'audit réalisé par le CAB* »[19] (mis en gras et souligné par l'Autorité).
>
> [...[20]]
>
> « *L'utilisateur **peut utiliser la <u>fonction de signature</u> du rQSCD** (en combinaison avec le certificat, bien sûr) dans d'autres applications, mais **le certificat n'est utilisé qu'en combinaison avec le rQSCD**. Nous ne délivrons donc pas de certificat à des tiers ou à des fins autres que cette utilisation spécifique* » (mis en gras et souligné par l'Autorité).
>
> « *Le middleware eID est nécessaire pour consulter la carte eID (certificat d'authentification). Ce logiciel est déjà utilisé et est actuellement étendu afin de pouvoir également effectuer les*

[19] L'Autorité a réinterrogé le Demandeur sur ce point précis. Le Projet définit lui-même le « service de signatures électroniques qualifiées » comme étant le « service permettant d'apposer via un certificat de signature à distance une signature électronique qualifiée ». A un moment donné (au-delà de la création d'un certificat), un service doit créer la signature électronique. L'article 3, 16., c), du Règlement EIDAS vise bien cette hypothèse de service de confiance. Et l'article 2, § 3, du Projet vise bien aussi la création à distance de signatures électroniques. Or c'est *a priori* un QTSP qui doit créer cette signature et celle-ci devrait être créée par le *remote* QSCD. Ne devrait-il par conséquent pas y avoir un QTSP qui est identifié pour cette partie du processus du service de signature prévu par le Projet ?

[20] Voir le considérant n° 15, dernier alinéa.

actions suivantes : création d'un compte, création d'un certificat à distance, récupération et utilisation d'un certificat à distance, rekeying. Ces actions sont effectuées via le SPF BOSA et le SPF IBZ, mais le logiciel permet de les rendre accessibles sur l'ordinateur de l'utilisateur ».

Réinterrogé à propos de <u>l'apposition</u> ou de <u>la création</u> de signatures, le Demandeur a répondu ce qui suit :

« *On peut distinguer **trois** éléments différents :*

1. ***Le service qui crée le certificat** : Il s'agit d'un service qualifié fourni par le QTSP Kingdom of Belgium.*
2. ***Le service qui crée la signature** : Il **<u>n'existe pas de service qualifié spécifique sous eIDAS pour ce service</u>**.*
    - *Dans le contexte des cartes eID, la signature est faite par le QSCD (c'est-à-dire la puce à contact) qui réside dans la carte.*
    - *Dans le contexte de la solution « Remote Signing », la signature est créée par le système rQSCD, qui est (comme vous le disiez) opéré par Zetes pour le QTSP Kingdom of Belgium. Sous la première version de la réglementation, il n'existait pas un tel service **qualifié**. Sous la nouvelle version, **<u>il existe maintenant le service qualifié de « management of QSCDs ». Le QTSP sera qualifié pour fournir ce service</u>** avant la date limite imposée par eIDAS art. 51 (3).*
3. « ***3. Le service qui appose la signature**, c'est-à-dire un service comme le Signing-Box offert par le SPF BOSA ou une plateforme tierce telle qu'Adobe : **Ceci n'est <u>pas un service qualifiable sous eIDAS</u>.***

    *Pour créer la signature à l'aide du service de signature à distance, nous soutenons donc des applications comme Adobe Reader (expérience utilisateur similaire à la signature avec eID) ainsi que le **Signingbox offert par le SPF BOSA.***
    *Adobe Reader ou les applications semblables sont des applications locales installées par l'utilisateur et **Signingbox est une <u>application web</u>** accessible via https://signing.fts.bosa.belgium.be/. Cette dernière utilise les composants du service de signature numérique proposés par la Commission européenne (https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/).*
    *Dans les deux cas, le document est visualisé par l'utilisateur et celui-ci est invité à confirmer la signature du document. **Ces applications communiquent avec le service de signature à distance** et ne transmettent que le hash du document au service de signature à distance afin de signer le hash. Adobe Reader ou Signingbox*

*reçoit le hash signé du service de signature à distance **et ajoute la signature électronique au document sur cette base*** » (mise en gras modifiée et soulignement ajouté par l'Autorité).

19. Les réponses communiquées par le Demandeur appellent les commentaires suivants de la part de l'Autorité.

20. **Premièrement, le Projet doit identifier clairement, en s'alignant sur les concepts définis dans le Règlement EIDAS, les services auxquels il s'applique**, **et articuler son dispositif** (conditions d'accès au service ; journalisation ; responsables du traitement) **en fonction de chacun des services concernés**. A cet égard, sur la base de l'exposé des motifs et des réponses communiquées par le Demandeur, il est clair que le Projet s'applique aux **services de confiances suivants** : « *la délivrance de certificats de signature électronique* »[21], la « *création de signatures électroniques* »[22] (celle-ci est réalisée via le *remote* QSCD fourni par Zetes pour le compte du SPF Intérieur et du SPF BOSA) et « *la gestion de dispositifs de création de signature électronique à distance* » (soit la gestion par le SPF Intérieur et le SPF BOSA du *remote* QSCD fourni par Zetes)[23].

21. **Deuxièmement**, s'agissant du service permettant **d'apposer une signature électronique** sur un document, l'Autorité a bien observé et noté qu'un tel service n'était **pas défini par le Règlement EIDAS en tant que service de confiance**. Or la lecture du Projet et de son exposé des motifs **ne permet pas de comprendre clairement si le Projet a pour objectif ou pas de mettre en place et réglementer ce service particulier**. Sur ce point notamment, sauf erreur de l'Autorité, les documents communiqués avec le dossier n'identifient d'ailleurs pas dénommée comme telle la solution « Signingbox » évoquée par le Demandeur dans les réponses communiquées à l'Autorité dans le cadre de la mise en état du dossier, et la définition du concept de « *service de signatures électroniques qualifiées* »[24] tel que consacrée dans l'article 2, § 1er, 5°, du Projet ainsi que la manière dont ce concept est utilisé dans le dispositif du Projet sont ambigus[25]. Par conséquent, en tout état de cause, cette disposition du Projet doit être adaptée. **Si l'intention du Demandeur est d'encadrer par son Projet un service d'apposition de signature** (une application web) mise à disposition, il convient alors avant tout, de **définir ce service**, et ensuite, d'en encadrer le fonctionnement et la fourniture à la manière dont sont encadrés les autres services de confiance concernés. Sous réserve du commentaire suivant, **l'Autorité ne se prononce pas plus à propos de ce service**.

---

[21] Article 3, 16., a), du Règlement EIDAS.

[22] Article 3, 16., c), du Règlement EIDAS.

[23] Article 3, 16., f), du Règlement EIDAS.

[24] Soit le « service permettant **d'apposer** via un certificat de signature à distance une signature qualifiée […] » (mis en gras par l'Autorité).

[25] Alors que ce service est défini comme le service permettant **d'apposer** une signature, l'article 2, § 3, du Projet par exemple, vise la « ***création à distance** de signatures électroniques qualifiées via le service de signatures électroniques qualifiées* » (mis en gras par l'Autorité).

22. **Troisièmement**, **le Projet doit être clair quant à l'offre des services concernés aux citoyens : quels services peuvent être utilisés séparément ou quels services doivent être utilisés de manière intégrée.** Sur ce point, si l'intention du Demandeur est de réglementer le service **d'apposition de signature électronique**, il doit également se dégager clairement du Projet que le **recours à ce service est optionnel** (mais bien, l'Autorité présume, lié à l'utilisation des autres services (de confiance) prévus par le Projet), et que les autres services (de confiance) mis à disposition peuvent par conséquent être utilisés sans qu'il soit systématiquement recouru au service d'apposition de signature. Notamment, sur le plan de la protection des données, l'impact d'un tel service est distinct dès lors que techniquement, la fourniture d'un tel service pourrait impliquer l'accès au (et le traitement du) document à signer lui-même et donc le traitement des données, y compris à caractère personnel, qu'il contient. A cet égard, **l'Autorité est d'avis qu'en tout état de cause,** dans le cadre du **service d'apposition de signature électronique, le traitement du document** (création du hash ; ajout de la signature sous la forme d'un hash signé, du certificat public et éventuellement, d'une représentation visuelle) **doit être totalement exécuté localement (*client-side*)**. Pour le reste, l'Autorité comprend qu'en vertu du Projet, **la personne concernée ne pourra obtenir la délivrance d'un certificat de signature électronique que dans l'hypothèse où elle entend également recourir au service de création de signature électronique** via le *remote* QSCD fourni par Zetes sous la responsabilité du SPF Intérieur et du SPF BOSA.

23. **Troisièmement**, l'Autorité prend acte de cette réponse du Demandeur concernant la **création de la signature électronique elle-même** : le document que signe la personne concernée **ne peut pas être transmis** au SPF BOSA, au SPF Intérieur ou à Zetes (autrement dit, son *hash* est réalisé localement – *client-side*, via le terminal (*software* et *hardware*) de la personne concernée (ordinateur ou autre). Ce qui constitue une approche **conforme aux principes de finalité et de minimisation des données**.

24. **Quatrièmement** enfin, le Demandeur indique[26] **qu'il n'existe pas de service qualifié spécifique en vertu du Règlement EIDAS pour le service de création de signature électronique**. Bien qu'en l'occurrence, contrairement au scénario de la signature électronique via le certificat de signature présent sur la puce de la carte d'identité électronique, il convienne bien de recourir à un tel service. L'Autorité note que dans ce cas, le service qualifié est **le service de gestion de dispositifs de création de signature électronique qualifiés à distance**.

[26] Voir le considérant n° 17.

II.3. Responsabilités au regard des traitements de données à caractère personnel

25. L'article 2, § 6, du Projet fixe les responsabilités au regard des traitements de données à caractère personnel. Cette disposition est rédigée comme suit :

> « *1° en ce qui concerne les données personnelles pour* ***la création et la gestion des certificats*** *qualifiés de signature, le Service public fédéral Intérieur est le responsable de traitement des données à caractère personnel garantit notamment l'identité de l'utilisateur et l'identification du signataire en cas de litige ;*
>
> *2° le Service public fédéral Intérieur et le Service public fédéral Stratégie et Appui sont les responsables* ***conjoints*** *des traitements de données à caractère personnel traitées pour la* ***création, l'actualisation, la gestion et la conservation des comptes utilisateurs*** *visés à l'article 3* ***dans le registre des comptes utilisateurs*** *visé à l'article 3 §6 ;*
>
> *3° le Service public fédéral Stratégie et Appui est le responsable de traitement des données à caractère personnel traitées en vue de la tenue* ***des fichiers de journalisation*** *(loging*[27]*) relatifs à la* ***gestion des comptes utilisateurs*** *visés à l'article 3* ;
>
> *4° le Service public fédéral Intérieur est responsable de traitement des données à caractère personnel traitées en vue de la tenue des* ***fichiers de journalisation*** *(loging*[28]*) relatifs à la* ***gestion des certificats qualifiés de signature électronique*** » (mis en gras par l'Autorité).

26. L'Autorité souligne d'emblée que **c'est à juste titre que le Projet entend clarifier les responsabilités au regard des traitements de données à caractère personnel réalisés dans son contexte**[29]. A cette fin, le Demandeur doit toujours bien veiller à ce que la désignation d'une entité comme responsable du traitement soit cohérente à l'égard des tâches et missions qui lui sont attribuées en vertu du contexte normatif concerné. Dans sa pratique d'avis, le raisonnement de l'Autorité est qu'en général une entité est responsable du traitement de données à caractère personnel nécessaire à l'exécution de ces missions/tâches. Cette approche permet aussi, en principe, que soit systématiquement attribuée une responsabilité. **Dans le cadre du Projet, il importe de pouvoir clairement identifier qui est responsable des traitements de données nécessaires à la mise en œuvre des**

---

[27] Logging.

[28] Logging.

[29] Voir encore récemment les développements dans l'Avis n° 08/2026 du 20 janvier 2026 concernant un avant-projet de loi portant modification de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale et de la loi du 17 juillet 2001 relative à l'autorisation pour les services publics fédéraux de s'associer en vue de l'exécution de travaux relatifs à la gestion et à la sécurité de l'information (CO-A-2025-207), considérant n° 14 et les références citées.

différents services de confiance[30] offerts. Et en principe, cette responsabilité devrait incomber à l'entité – le prestataire de service de confiance qualifié[31] qui est chargée par le Projet d'offrir le service de confiance concerné[32]. Cette approche est cohérente au regard du Règlement EIDAS qui fixe une série d'obligations à charge de ce type particulier de prestataires de service qui ont logiquement une responsabilité propre en la matière[33].

27. L'approche suivie dans le Projet comporte néanmoins une certaine hybridité dans la mesure où elle attribue des missions et des responsabilités au regard du traitement de données sans systématiquement une correspondance entre les deux. Plus concrètement, les développements suivants l'illustrent.

28. La « **création** » et la « **gestion** » des **certificats** qualifiés de signature relève de la responsabilité au regard du traitement de données du SPF Intérieur. Cependant, conformément à l'article 2,§ 3, du Projet, c'est le SPF Intérieur et le SPF Stratégie et Appui qui sont chargés de la « **mise à disposition** » (action par conséquent distincte de la « gestion » des certificats) des citoyens des certificats. Autrement dit, sur le plan du traitement de données à caractère personnel, la responsabilité au regard de la mise à disposition des certificats **semblerait être une responsabilité conjointe** des SPF Intérieur et SPF Stratégie et Appui.

29. L'Autorité comprend que le SPF Intérieur sera Certificate Authority (**CA**) responsable de la création des certificats qualifiés de signature électronique et qu'il lui appartiendra notamment de procéder à l'éventuelle révocation des certificats et de mettre à disposition les informations nécessaires concernant la validité des certificats (OCSP/CRL). **Mais** le Demandeur a toutefois souligné dans les réponses communiquées à l'Autorité dans le cadre de la mise en état du dossier qu'OCSP/CRL n'étaient plus pertinents compte-tenu de la durée de validité limitée des certificats – voir les considérants nos 15-16). Mais **le Projet ne le prévoit pas** en tant que tel (cette déduction résulte de l'attribution d'une responsabilité au regard du traitement de données).

30. Quelle entité est responsable du traitement de données nécessaire à la fourniture du **service de signature électronique à distance** lui-même (entendu comme le service de **création** de signature électronique) ? L'article 2, § 6, ne le précise pas mais l'article 2, § 2, indique que la présente loi concerne le « *service des signatures électroniques, **mis à la disposition** par le Service public fédéral Intérieur et le Service public fédéral Stratégie et Appui* » (mis en gras par l'Autorité), sans préjudice

[30] Ou simplement « service », s'agissant du service permettant d'apposer une signature électronique qualifiée, pour autant que le Projet ait pour objectif d'encadrer ce service, voir le considérant n° 21.

[31] Ou le prestataire d'un autre type de service, *ibid*.

[32] Ou autre service, voir la note de bas de page n° 27.

[33] Voir l'article 13 du Règlement EIDAS.

des commentaires émis précédemment concernant l'ambiguïté de la définition du « *service de signatures électroniques* »[34]. De telle sorte **qu'il semblerait** que la fourniture du service de signature électronique relève de la responsabilité conjointe, au regard du traitement de données, du SPF Intérieur et du SPF BOSA.

31. S'agissant des **traitements de données effectués dans le cadre de la journalisation**, le Projet peut effectivement indiquer que c'est le SPF BOSA qui est responsable du *logging* en relation avec les **comptes utilisateurs** (car le SPF Stratégie et Appui *et* le SPF Intérieur sont responsables *conjoints* du traitement dans ce cas, de telle sorte que la disposition en Projet présente par conséquent une plus-value). En revanche, l'Autorité ne perçoit pas pourquoi il serait nécessaire d'indiquer en outre que le SPF Intérieur est responsable du *logging* lié à la « **gestion** » des certificats, dès lors qu'il est déjà désigné comme responsable des traitements de données liés à la gestion des certificats. Cela étant dit, l'exposé des motifs vise lui les logs liés à « ***l'utilisation*** » des certificats, ce qui constitue encore un autre traitement de données. Le Projet doit clarifier si l'utilisation des certificats doit être l'objet d'une journalisation particulière et sous la responsabilité de quelle entité. Par ailleurs, le projet serait partiel dès lors qu'il ne viserait pas la « **création** » des certificats. Qui d'autre que le SPF Intérieur serait chargé du *logging* concernant la création des certificats ? *Quid* encore de la journalisation du recours au service de signature électronique ?

32. **Dès lors qu'il aborde la question des obligations de journalisation et la responsabilité au regard des traitements de données que celle-ci implique, le Projet doit adopter une approche cohérente et exhaustive en la matière**.

33. Dans les hypothèses de **responsabilités conjointes[35]**, l'Autorité s'est également demandé si par arrêté royal, il serait le cas échéant envisagé d'identifier plus en détail les obligations respectives du SPF Intérieur et du SPF Stratégie et Appui[36].

34. Interrogé à ce sujet (dans des termes néanmoins partiellement différents), le demandeur a expliqué ce qui suit :

> « *Le 'Kingdom Belgium Federal Government' est déjà aujourd'hui Qualified Trust Service Provider pour les services de signature et est représenté par le SPF IBZ et le SPF BOSA.*
> *Le SPF IBZ et le SPF BOSA ont un* ***contrat avec le sous-traitant ZETES SA*** *pour la* ***création, la gestion*** *et* ***la conservation*** *des certificats qualifiés de signature électronique* ***et***

[34] Voir le considérant n° 21.

[35] Par exemple, s'agissant de la gestion des comptes, l'article 3, § 4, du Projet, prévoit que le SPF Intérieur et le SPF Stratégie et Appui doivent vérifier les conditions du § 3 tant lors de la création du compte que durant la durée de vie de ce dernier.

[36] Voir l'article 26, 1., du RGPD.

encore avec CERTIPOST *pour la gestion et la conservation des certificats qualifiés de signature électronique déjà délivrés (il n'y a plus de création de nouveaux certificats sous ce contrat).*
Les ***certificats de la nouvelle solution*** *seront délivrés sous le 'Kingdom Belgium Federal Government' QTSP. L'entité qui est responsable de la délivrance, la gestion et de la conservation des certificats est donc le 'Kingdom Belgium Federal Government' QTSP, représenté par le SPF BOSA et le SPF IBZ qui font appel au* ***sous-traitant ZETES SA qui opère comme Certificate Authority (CA)****.*

Techniquement, c'est ***un système du SPF BOSA qui traite les comptes d'utilisateur et qui transmettra la demande d'un certificat d'un citoyen au CA*** *exploitée techniquement par ZETES SA* ***après authentification du citoyen via le FAS par le SPF BOSA et après vérification par le SPF BOSA de la validité de son compte d'utilisateur****.*
La vérification du nom et des prénoms et de la capacité de signature ("CanSign") se fait sur base des données de la source authentique Registre National du SPF IBZ.
Il n'y a pas de vérification de la validité via OCSP/CRL, car il s'agit de certificats d'une durée de validité de 24 heures*.*
La journalisation et audit des comptes d'utilisateur *se fait par le* ***SPF BOSA*** *et* ***la journalisation et audit des certificats*** *se fait par le* ***sous-traitant du SPF IBZ et du SPF BOSA****. Veuillez trouver plus d'information dans la réponse à la question 18* » (mis en gras par l'Autorité).

En ce qui concerne les **responsabilités conjointes**, le Demandeur a répondu ce qui suit : « *Une convention entre le SPF IBZ et le SPF BOSA sera conclue* ».

35. Le Projet **doit être précisé sur la base des développements précédents afin d'identifier clairement quelles entités sont responsables (conjointes ou pas) de quels traitements de données à caractère personnel dans le cadre de la vérification de l'identification/authentification des utilisateurs ainsi que de la fourniture des différents services de confiance[37] prévus par le Projet**. Cette approche doit être cohérente en fonction des tâches et missions qui sont attribuées par le Projet à ces entités. Ces responsabilités doivent être allouées par le Projet aux responsables du traitement concernés. Le RGPD autorise le recours à la sous-traitance de telle sorte que selon les hypothèses, il n'est pas exclu que Zetes puisse agir comme sous-traitant du SPF Intérieur et du SPF BOSA, pour autant qu'en pratique, l'action de Zetes soit bien limitée à celle d'un sous-traitant. Sur le plan théorique, le Projet pourrait également suivre une autre approche et prévoir que, selon une procédure et des conditions à déterminer par le Projet, le SPF Intérieur et le SPF BOSA désignent le

[37] Ou autre, voir la note de bas de page n° 30.

prestataire de service de confiance qualifié chargé de fournir l'un ou l'autre service de confiance prévu par le Projet (attribution d'une mission d'intérêt public à une entité privée). Dans une telle hypothèse, une responsabilité au regard du traitement de données à caractère personnel pourrait être imputée à ce prestataire par le Projet. **Il appartient en l'espèce au demandeur de choisir l'approche et les qualifications juridiques qui reflètent au mieux les faits**.

36. S'agissant des **responsabilités conjointes** au regard du traitement prévues par le Projet, l'Autorité prend acte du choix du demandeur de ne pas définir dans le Projet ou un arrêté royal pris en exécution de celui-ci les obligations respectives du SPF Intérieur et du SPF BOSA et de plutôt laisser ces autorités conclure une convention. L'Autorité rappelle qu'en tout état de cause, la personne concernée peut toujours exercer ses droits à l'égard de et contre chacun des responsables du traitement, conformément à l'article 26, 3., du RGPD. Les « *grandes lignes* » de cette convention devront également être mises à la disposition de la personne concernée, conformément à l'article 26, 2., du RGPD. **A titre de garantie complémentaire en matière de transparence, l'Autorité invite le Demandeur à vérifier si le Projet ne pourrait pas prévoir la publication de la convention qui sera conclue**.

II.4. Compte utilisateur, certificat et données traitées

II.4.1. Compte utilisateur et Registre des comptes utilisateurs

37. L'article 3, § 5, du Projet prévoit que le **Registre des comptes utilisateurs** contient les données suivantes pour chaque compte utilisateur : le nom du titulaire du compte utilisateur ; les deux premiers prénoms et, le cas échéant, la première lettre du troisième prénom ; le numéro de Registre national du titulaire du compte utilisateur et le numéro de compte utilisateur du titulaire du compte utilisateur.

38. L'Autorité observe que le « **statut** » du compte, « actif » ou désactivé constitue également une donnée qui doit être traitée dans le Registre des comptes utilisateurs. Par ailleurs, elle a interrogé le demandeur quant à la nécessité d'y traiter également « *les deux premiers prénoms et, le cas échéant, la première lettre du troisième prénom* » de l'utilisateur dès lors que le numéro de Registre national paraît rendre ces données superflues (la même question se posant *mutatis mutandis* concernant le **certificat** de signature lui-même[38]) (**remarque** : ceci est sans préjudice des développements suivants concernant la présence du numéro de Registre national dans le certificat qualifié de signature électronique). Interrogé à ce sujet, le demandeur a notamment répondu ce qui suit :

« ***Le nom du titulaire doit être intégré car il doit figurer dans le certificat***.

[38] Voir le considérant n° 43.

*La manière dont le nom a été intégré dans le certificat est **conforme aux exigences de la norme 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**.*

Le nom correspond donc au nom tel qu'il est imprimé sur les cartes d'identité et de séjour » (texte en anglais mis en gras par le demandeur, texte en français mis en gras par l'Autorité).

39. L'Autorité prend acte de cette réponse et comprend par conséquent qu'en fin de compte, les prénoms additionnels (non nécessaires dès lors qu'un identifiant unique est également utilisé) doivent être intégrés dans le certificat (et le Registre des comptes utilisateurs) **en raison *a priori* du choix posé en Belgique** (l'Autorité **n'exclut pas** que d'autres obligations internationales de la Belgique puissent s'appliquer en la matière et ne mène pas d'analyse à ce sujet) **de faire apparaître ces prénoms sur la carte d'identité électronique elle-même**. L'Autorité **ne remet pas en cause ce choix/cet état du droit**. Elle ne peut et il ne lui appartient pas dans le cadre du présent Avis d'analyser ce questionnement en profondeur.

40. Elle attire cependant l'attention du Demandeur, sur le plan des principes, sur le fait que **si une norme technique est rendue obligatoire en vertu du droit européen, il appartient au législateur, lorsque cela est possible, d'adapter le droit belge de manière telle que cette norme puisse être mise en œuvre conformément au principe de minimisation des données consacré dans le RGPD**.

41. Le Demandeur a également précisé que « *Conformément l'article 2 § 5 il faut un compte actif : 'Pour pouvoir utiliser le service de signatures électroniques qualifiées l'utilisateur doit avoir un compte utilisateur actif et un certificat qualifié de signature valable.' **Ce n'est pas une donnée dans le registre mais plutôt une propriété du compte*** ». Par ailleurs, le Projet n'indique rien quant aux données qui seraient traitées via le **compte utilisateur** lui-même. Interrogé à ce sujet et quant à la pertinence de la distinction entre le compte utilisateur et le registre des comptes utilisateurs, le demandeur a précisé ce qui suit : « ***Les données traitées sont indiquées à l'article 3 § 5 du projet de loi*** » (mis en gras par l'Autorité). **L'Autorité prend en conséquence acte du fait qu'aucune autre donnée n'est traitée dans le compte utilisateur et le Registre des comptes**. Remarque : cette

constatation est sans préjudice des développements ultérieurs du présent Avis concernant la journalisation.

42. S'agissant de l'utilisation du compte utilisateur, l'article 3, § 2, prévoit bien la nécessité pour un utilisateur, de s'authentifier via son eID (ou le portefeuille fédéral d'identité numérique) pour **créer** le compte. Le Projet **ne précise en revanche pas que l'utilisation ultérieure du compte** (afin d'obtenir un certificat de signature électronique et/ou de signer des documents) **nécessite les mêmes identification et authentification**. L'article 4, § 2, prévoit seulement que « *A chaque demande de **délivrance d'un certificat qualifié de signature**, le Service public fédéral Intérieur et le Service public fédéral Stratégie et Appui **vérifient au préalable l'identité de l'utilisateur et la validité du compte utilisateur*** » (mis en gras par l'Autorité), sans préciser le moyen de vérification utilisé. L'hypothèse du recours au service de **signature électronique** n'est par ailleurs pas visée. L'Autorité part du principe que toutes ces hypothèses nécessitent un même niveau de garantie d'identification et authentification que celle qui est nécessaire pour la création d'un compte. Interrogé à ce sujet, le demandeur a répondu ce qui suit :

> « *Le projet mentionne dans l'article 4 § 2 : A chaque demande de délivrance d'un certificat qualifié de signature, le Service public fédéral Intérieur et le Service public fédéral Stratégie et Appui vérifient au préalable l'identité de l'utilisateur et la validité du compte utilisateur.*
> *L'utilisation du service est possible via les moyens d'identification hautement sécurisés qui sont **par exemple** le portefeuille belge pour l'identité numérique (c'est-à-dire l'application MyGov.be) ou et le service fédéral d'authentification (CSAM FAS) combiné avec le certificat d'authentification des cartes d'identité et des cartes d'étranger* » (mis en gras par l'Autorité).

43. L'Autorité retient que **l'identité de la personne concernée doit être vérifiée, lorsqu'elle recourt via son compte utilisateur aux services de confiance prévus par le Projet[39], conformément à l'article 24, 1*bis*., du Règlement EIDAS[40]**.

II.4.2. Certificat qualifié de signature et numéro de Registre national

44. S'agissant du **certificat qualifié de signature**, **l'article 4, § 4,** du Projet prévoit que les données le composant sont les suivantes : le numéro de Registre national du titulaire du compte utilisateur, le nom du titulaire du compte utilisateur, le premier prénom et , le cas échéant, le deuxième prénom et

[39] Y compris également, le service d'apposition de signature dans la mesure où celui-ci ne semble pas pouvoir être disponible en dehors de la signature électronique via le *remote* QSCD visé par le Projet.

[40] Voir les considérants nos 6-8.

la première lettre du troisième prénom, le numéro de série du certificat de signature qualifié. Le **paragraphe 5** du même article autorise toute partie utilisatrice[41] « *à **conserver** le numéro de Registre national, aussi longtemps qu'il est nécessaire pour recueillir la **preuve de la signature électronique ou de l'authentification**, et **à l'utiliser uniquement pour vérifier** la signature électronique de l'utilisateur* ».

45. D'emblée et sans préjudice du commentaire plus fondamental qui suit (considérants nos 48 et s.), **l'article 4, § 5, du Projet appelle les trois commentaires suivants**. Premièrement, l'Autorité observe que la partie utilisatrice **ne va pas nécessairement pouvoir se limiter à « conserver »** le numéro de Registre national. A partir du moment où celui-ci est repris dans le certificat intégré au document signé, toute **communication de ce document qui nécessite la communication d'un document équivalent à l'original** (c'est-à-dire, une communication du document qui ne peut pas être réalisée sans l'édition du document en vue de la suppression de la signature électronique et du certificat) impliquera également une communication du numéro de Registre national à l'entité à laquelle il est communiqué. Autrement dit, le traitement du numéro de Registre national est bien susceptible d'aller au-delà de sa simple conservation. Il appartient au Demandeur d'utiliser une terminologie adaptée aux pratiques qui doivent être permises en matière également d'échanges de documents signés.

46. Deuxièmement, si cette disposition a également pour effet **d'interdire le traitement ultérieur du numéro de Registre national**, une formulation encore plus explicite devrait être privilégiée. Effectivement, en l'absence de l'application d'une éventuelle obligation légale (hypothèse qui doit être réservée par la disposition en projet, sauf à risquer, en tant que *lex posterior*, d'empêcher l'application d'éventuelles obligations légales), l'Autorité ne voit pas pour quelle raison légitime le numéro de Registre national devrait pouvoir être traité à une autre fin que celle de l'établissement (la preuve et la vérification) de la signature électronique. Autrement dit, l'interdiction de tout autre traitement ultérieur du numéro de Registre national, sans préjudice d'une éventuelle obligation légale, devrait être prévue à titre de garantie appropriée au sens de l'article 87 du RGPD.

47. Troisièmement, l'Autorité n'étant pas sûre de percevoir pourquoi, en vertu du Projet, le certificat de signature électronique devrait être également conservé pour la preuve d'une « **authentification** » (en principe, lorsqu'il s'agit de s'identifier et non de signer, le certificat d'authentification est utilisé), elle a interrogé le demandeur qui a répondu ce qui suit : « *En effet, la conservation sert à recueillir la preuve de la signature électronique, à utiliser uniquement pour vérifier la signature électronique de l'utilisateur. L'authentification en fait partie mais n'est pas une finalité séparée dans ce cas. La disposition devra être modifiée* ». **L'Autorité prend acte du fait que le Projet sera modifié en ce sens**.

[41] Soit « *une personne physique ou morale qui se fie à une identification électronique, aux portefeuilles européens d'identité numérique ou à d'autres moyens d'identification électronique, ou à un service de confiance* », article 3, 6., du Règlement EIDAS.

48. Quoi qu'il en soit, **le Projet soulève plus globalement et fondamentalement <u>la problématique de l'utilisation du numéro de Registre national dans les certificats qualifiés</u>** de signature électronique. C'est un sujet connu du droit belge. Pour rappel, la Loi du 8 août 1983 *organisant un registre national des personnes physiques* (ci-après, la « **Loi RN** ») a déjà dû être réformée pour prendre en compte le fait qu'en Belgique, **l'identification électronique et la signature électronique qualifiée reposant sur la base des certificats d'authentification et de signature présents sur la carte d'identité électronique** belge nécessitent de permettre le traitement du numéro de Registre national dans ce contexte, dès lors que ce dernier est directement repris sur ces certificats[42]. De telle sorte que, dans une société dans laquelle le recours à la signature et l'identification électroniques s'accroissent constamment, **il existe toujours plus de parties privées avec lesquelles les personnes concernées partagent leur numéro de Registre national**.

49. Dans ce contexte, au regard du nouveau service de création de signature électronique envisagé, compte-tenu d'ailleurs, de l'existence d'un identifiant/numéro supplémentaire (à savoir, « *le numéro de compte utilisateur du titulaire du compte utilisateur* », et en supposant que ce numéro n'est pas une fonction du numéro de Registre national), **l'Autorité a interrogé le demandeur quant à la**

---

[42] Voir l'article 8, §§ 2-3, de la Loi RN selon lesquels :

« […]

§ 2. Lors de la lecture d'une carte d'identité électronique pour Belge ou d'une carte pour étranger, ou ***lors de la réception d'un certificat de signature électronique*** *ou d'un certificat d'authentification électronique, la seule prise de connaissance du numéro de Registre national ne constitue pas une utilisation dudit numéro requérant une autorisation préalable.*

§ 3. Une autorisation d'utilisation du numéro de Registre national n'est pas requise si le numéro de Registre national est exclusivement utilisé à des fins d'identification et d'authentification d'une personne physique dans le cadre d'une application informatique offerte par une institution privée ou publique de droit belge ou par les autorités, institutions et personnes visées à l'article 5, § 1er.

Une autorisation d'utilisation du numéro de Registre national n'est pas non plus requise lorsque le numéro de Registre national est exclusivement utilisé à des fins d'identification et d'authentification d'une personne physique dans le cadre d'une application informatique offerte par une entreprise étrangère lorsque l'utilisation est autorisée à cette fin par ou en vertu d'une loi, d'un décret ou d'une ordonnance, par le ministre ayant l'Intérieur dans ses attributions ou par une autre instance compétente.

Le fournisseur d'une application informatique ne peut pas utiliser le numéro de Registre national à d'autres fins sauf s'il y est autorisé par ou en vertu d'une loi, d'un décret ou d'une ordonnance, par le ministre ayant l'Intérieur dans ses attributions.

Les certificats de signature et/ou d'authentification électroniques, comprenant le numéro de Registre national, peuvent être conservés sans autorisation préalable aussi longtemps qu'il est nécessaire pour recueillir la preuve de la signature électronique ou de l'authentification.

Le fournisseur d'une application informatique tel que visé aux alinéas 1er et 2, consigne, dans un fichier de conversion crypté, une relation entre le numéro de Registre national et un numéro d'identification propre au fournisseur. Les informations issues de ce fichier de conversion ne peuvent être utilisées que pour retrouver le numéro d'identification propre au fournisseur de la personne physique qui souhaite avoir accès à l'application informatique du fournisseur de l'application informatique ou dont les données sont échangées avec un autre fournisseur d'application informatique.

[…]

§ 5. Une autorisation d'utilisation du Registre national n'est pas requise lorsque le numéro de Registre national est utilisé pour l'identification d'une personne physique par un fournisseur de service d'identification électronique de niveau élevé ou substantiel tel que visé dans le Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la Directive 1999/93/CE, qui est agréé conformément à l'arrêté royal du 22 octobre 2017 fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification électronique pour applications publiques ou par un service public qui, par ou en vertu d'un loi, d'un décret ou d'une ordonnance, a pour mission de fournir un service de gestion des utilisateurs et des accès, exclusivement à des fins d'identification et d'authentification d'une personne physique qui souhaite obtenir un accès à distance à une application informatique d'un fournisseur d'une application informatique visée au § 3 » (mis en gras par l'Autorité).

question de savoir s'il avait été envisagé de ne plus recourir à l'utilisation du numéro de Registre national dans les certificats de signature électronique et pourquoi une telle solution aurait le cas échéant été écartée. L'Autorité a interrogé le Demandeur une première fois à ce sujet et celui-ci a répondu ce qui suit :

> « *Afin de répondre à cette préoccupation, il est prévu de* ***délivrer à l'avenir des certificats professionnels*** *aux personnes travaillant pour les autorités fédérales et exerçant une fonction particulière. Dans ce cas,* ***l'identité réelle de la personne derrière le certificat n'apparaîtra pas dans le certificat, mais bien le rôle de cette personne****. Par exemple, une amende sera valablement signée de manière électronique par un agent, mais le citoyen ne voit pas dans le certificat le nom et le numéro de registre national de l'agent qui a signé. En revanche, il est nécessaire que l'autorité d'enregistrement (la police dans ce cas) connaisse toujours la véritable identité de l'agent et sache qui a apposé une signature. Le cas échéant l'autorité d'enregistrement va devoir dévoiler cette information dans certaines situations. L'autorité d'enregistrement devra retirer le certificat professionnel lorsque l'agent ne remplit plus cette fonction (en cas de démission, de départ à la retraite, de suspension, etc.)* » (mis en gras par l'Autorité).
>
> L'Autorité **a réinterrogé le Demandeur à ce propos** dès lors que son interrogation est bien plus large. Il a répondu ce qui suit :
>
> « *Veuillez trouver ci-dessous nos éléments de réponse relatifs à l'utilisation du numéro de Registre national dans les certificats, (en lien avec ce qui a été exposé dans le cadre du dossier portant la référence* ***DOS-2021-06312***[43]*) :*
>
> ***L'option*** *consistant à remplacer le numéro de Registre national par un identifiant alternatif (par exemple un numéro de série unique)* ***avait été examinée****.*
> ***Dans le contexte des administrations belges, le numéro de Registre national constitue l'identifiant administratif unique*** *permettant d'établir de manière certaine le lien avec une personne physique,* ***notamment dans les relations avec les autorités publiques ainsi qu'avec certains organismes privés soumis à des obligations légales d'identification et tenus d'utiliser le numéro de Registre national****.*

[43] [Ce dossier a donné lieu à la Beslissing ten gronde 65/2025 du 3 avril 2025 de la Chambre contentieuse de l'Autorité, disponible sur https://gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-65-2025.pdf, dernièrement consulté le 16/02/2026. Il s'agit d'une décision de classement sans suite dans laquelle la Chambre contentieuse ne se prononce pas directement sur la problématique posée dans le présent avis (« *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* »)].

*Le recours à un **identifiant alternatif** impliquerait la mise en place d'un **service de correspondance permettant d'établir le lien** entre cet identifiant et le numéro de Registre national. Un tel mécanisme serait **indispensable pour les autorités publiques et les organismes légalement tenus d'identifier** formellement une personne.*

*Par ailleurs, un document signé électroniquement produisant des **effets juridiques à l'égard de tiers**, le destinataire doit pouvoir **identifier de manière certaine et non ambiguë** la personne signataire. **Dans l'ordre juridique belge, cette identification certaine repose sur l'identifiant administratif unique** qu'est le numéro de Registre national.*

*Le remplacement du numéro de Registre national ne supprimerait donc pas son traitement, mais en **déplacerait l'usage vers une infrastructure supplémentaire de correspondance,** introduisant une **complexité technique additionnelle et un point central supplémentaire de traitement de données**, avec une **dépendance structurelle** vis-à-vis de ce service intermédiaire.*

*Dans ces conditions, cette option **n'apporte pas de plus-value réelle au regard des principes du RGPD,** notamment en matière de minimisation et de sécurité des données, tout en générant des **désavantages opérationnels et organisationnels significatifs**. Elle n'a dès lors pas été retenue* » (mis en gras et souligné par l'Autorité).

50. L'Autorité prend acte de la réponse communiquée par le Demandeur qui toutefois, **ne lui paraît pas en l'état, totalement décisive** et ce, pour les raisons suivantes :

- Il convient de **distinguer la signature électronique qualifiée de l'identification/authentification des personnes concernées** en tant que telles et ce en particulier, lorsque cette identification/authentification est fondée sur une obligation légale. Le Projet lui-même est articulé sur la base de cette distinction[44], dès lors qu'aux fins d'identification et d'authentification, le certificat d'authentification présent sur la puce de la carte d'identité électronique belge peut toujours être utilisé, et le sera par l'utilisateur, pour créer son compte afin d'utiliser le service prévu par le Projet[45]. Autrement dit, ne pas recourir au numéro de Registre national dans le certificat qualifié de *signature* électronique, n'empêche pas par ailleurs des possibilités d'identification comprenant le numéro de Registre national dans les cas, comme indiqué par le demandeur, de relations avec une **autorité publique** ou avec une **entité privée** à laquelle incombe une **obligation légale spécifique d'identification** de ses « clients »[46]. Cela est

[44] Voir les considérants nos 4-8.

[45] Remarque : l'Autorité ne se prononce pas ici sur la question de la communication du numéro de Registre national aux entités privées qui requièrent une identification en l'absence d'obligation légale spécifique à ce sujet. Le présent Avis ne porte pas sur la question de l'identification/authentification en tant que telle.

[46] Il convient de noter que dans certains de ces cas, des entités privées ont même le droit de consulter le Registre national (dans le cadre de la lutte contre le blanchiment d'argent, voir l'Avis n° 14/2025 du 27 février 2025 *concernant une proposition de loi relative au partage de données provenant de sources authentiques avec les prestataires de services d'identification*

possible via le certificat d'*authentification*. En matière d'identification, il ne serait donc pas nécessaire de mettre en place un éventuel « *service de correspondance* » ;

- Le Demandeur indique que « *un document signé électroniquement produisant des effets juridiques à l'égard de tiers, le destinataire doit pouvoir identifier de manière certaine et non ambiguë la personne signataire. Dans l'ordre juridique belge, cette identification certaine repose sur l'identifiant administratif unique qu'est le numéro de Registre national* ». Avant tout, il existe de très **nombreuses situations dans lesquelles un acte ayant des effets juridiques à l'égard des tiers peut avoir lieu sans que soit traité le numéro de Registre national** des personnes concernées et sans d'ailleurs qu'il doive (puisse) l'être[47] (de nombreuses transactions du commerce électronique/de l'économie numérique l'illustrent). L'identification d'une personne est, en particulier dans les relations entre personnes privées[48], une notion relative qui doit être appréciée à l'aune de la finalité du traitement de données concerné. D'ailleurs, l'Annexe I du Règlement EIDAS indique que le certificat qualifié de signature électronique indique (c) « *au moins le nom du signataire ou un pseudonyme ; si un pseudonyme est utilisé, cela est clairement indiqué* ». Mais plus fondamentalement, **par définition, en exécution du Règlement EIDAS, une signature électronique qualifiée implique que l'identité de la personne concernée a été vérifiée par le prestataire de services de confiance qualifié via l'une des méthodes visées à l'article 24, 1*bis*, du Règlement EIDAS**. Autrement dit, il n'est *a priori* pas nécessaire dans une telle situation, que la partie à laquelle est communiqué le document signé doive connaître le numéro de Registre national de la personne concernée, puisque le recours à la signature électronique qualifié implique déjà que la personne concernée a été identifiée avec un niveau de confiance élevé ;

- Le Demandeur précise encore que « *Le remplacement du numéro de Registre national ne supprimerait donc pas son traitement, mais en déplacerait l'usage vers une infrastructure supplémentaire de correspondance, introduisant une complexité technique additionnelle et un point central supplémentaire de traitement de données, avec une dépendance structurelle vis-à-vis de ce service intermédiaire* ». Or premièrement, le Projet met justement en place un nouveau service et *de facto*, une nouvelle infrastructure, service dans le cadre duquel d'ailleurs, vont être créés et gérés **des comptes d'utilisateur** qui se voient attribuer un identifiant (au sein d'un Registre des comptes d'utilisateurs). Et le Demandeur indique lui-même deuxièmement, qu'est envisagée la possibilité de création de **certificats**

électronique agréés (DOC56 0330/001) et un amendement y lié (DOC56 0330/002) (CO-A-2025-003), considérant n° 50). C'est dire si cette situation se distingue du simple recours à la signature électronique même qualifiée.

[47] Sur la nécessité de s'identifier voir l'Avis n° 69/2025 du 26 août 2025 concernant la « Nationale Cybersecurity Strategie 3.0, 2026-2030 » (CO-A-2025-108), considérants nos 16-19 ;

[48] Les relations avec une autorité publique n'imposent pas non plus toujours une identification fondée sur le numéro de Registre national (par exemple, un citoyen peut simplement poser une question d'ordre général à une autorité publique).

professionnels[49] au profit de personnes travaillant pour les autorités fédérales et exerçant une fonction particulière (un certificat de signature spécifique dédié aux relations avec le secteur public ne pourrait-il pas également être créé ?) (**remarque** : l'Autorité rappelle au passage qu'il est possible pour les organisations, dans le cadre du Règlement EIDAS, de recourir à des **cachets électroniques qualifiés**). Troisièmement, comme cela a été rappelé, en tout état de cause, un **certificat d'authentification** demeure disponible par ailleurs. En conclusion, **l'Autorité manque d'informations concrètes convaincantes pour conclure que la complexité supplémentaire** que nécessiterait la délivrance de certificats qualifiés de signature électronique sans le numéro de Registre national **est en pratique insurmontable ou impossible à envisager en termes de coût au regard de l'avantage comparatif** qu'impliqueraient sur le plan de la protection des données des certificats qualifiés de signature électronique sans numéro de Registre national ;

- Enfin, et c'est là un sujet qui dépasse la portée du présent Avis, **autre chose serait de considérer que le numéro de Registre national, initialement un outil du secteur public, constitue en fait et désormais une donnée à caractère personnel dont les conditions de traitement par les entités privées doivent être globalement assouplies dans le contexte de l'économie numérique**[50]. Une telle réforme dans l'appréhension du traitement du numéro de Registre national par les entités privées nécessiterait d'être étudiée en tant que telle notamment dans le cadre d'une analyse d'impact relative à la protection des données. L'Autorité se borne à rappeler à ce sujet qu'un numéro d'identification national constitue une donnée à caractère personnel particulière qui, selon l'article 87 du RGPD, « *n'est utilisé que sous réserve des garanties appropriées pour les droits et libertés de la personne concernée adoptées en vertu* » du RGPD. Le droit belge a spécialement encadré l'utilisation du numéro de Registre national. Le maintien d'une solution technique dans le cadre de laquelle le numéro de Registre national est une donnée incluse dans le certificat qualifié de signature électronique implique une circulation et un traitement significatif des numéros de Registre national de la population belge, cela d'autant plus qu'il sera toujours plus fréquemment recouru à la signature électronique dans la société contemporaine. **Sauf changement de paradigme, il existe donc bien une plus-value réelle, sur le plan de la protection des**

[49] L'Autorité ne se prononce pas dans le présent Avis à propos de cette piste et des informations communiquées par le Demandeur à ce sujet.

[50] En poussant la logique plus loin, dans un sens inverse, l'utilisation du numéro de Registre national *seul* afin d'identifier la personne concernée, pourrait minimiser l'échange de données à caractère personnel à propos de la personne concernée dès lors qu'il est certain que dans le monde, une seule personne est identifiée par un numéro de Registre national belge. Mais il s'agit d'un scénario qui n'est pas envisagé et qui d'ailleurs, n'est pas prévu (permis) dans le cadre normatif du Règlement EIDAS (voir l'article 12, 3., d), du Règlement EIDAS et l'annexe du Règlement d'exécution (UE) n° 2015/1501 de la Commission du 8 septembre 2015 *sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*).

données, à prévoir des certificats qualifiés de signature électronique sans numéro de Registre national.

51. En synthèse, l'Autorité est d'avis que **les arguments avancés par le Demandeur pour ne pas prévoir la création de certificats qualifiés de signature électronique sans le numéro de Registre national ne sont pas complètement convaincants**. Le choix posé en la matière **doit dans tous les cas être l'objet d'une analyse d'impact relative à la protection des données approfondie**. Le Demandeur indique toutefois dans son formulaire de demande d'avis qu'une telle analyse n'a pas été réalisée. Il est important d'y procéder. (Remarque : l'Autorité est consciente que **l'identification** dans les relations privées pose un questionnement similaire qui toutefois, n'est pas abordé dans le présent Avis).

II.4.3. Journalisation - logging

52. Concernant le ***logging* – la journalisation**, qui est également une obligation découlant de la mise en œuvre du RGPD lui-même, s'agissant du traitement de données à caractère personnel, l'Autorité a invité le demandeur à lui préciser quelles dispositions du **contexte normatif EIDAS** (actes d'exécution de la Commission, normes applicables) prévoient une journalisation spécifique (aux fins de la prestation des services de confiance), afin de pouvoir identifier les catégories de données qui seront traitées dans ce contexte. Par exemple, lorsqu'une personne concernée utilise le service de création de signature électronique ou « appose » une signature sur un document via le service mis à disposition en vertu du Projet, quelles traces sont conservées concernant cette action (l'intitulé et les propriétés du document signés sont-elles par exemple également enregistrées ?). Le demandeur a répondu ce qui suit : « *Concernant l'usage du service de signature électronique,* ***l'action d'activation de la clé privée pour apposer une signature est loggée, il n'y a aucune trace du document qui est signé*** » (mis en gras par l'Autorité). **L'Autorité en prend acte**.

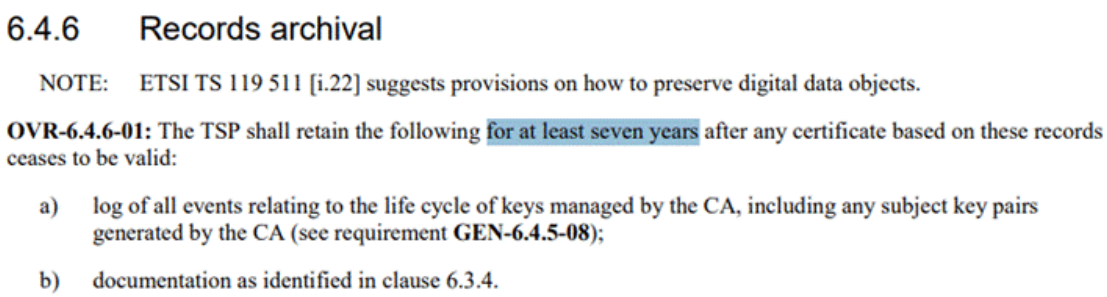
53. Interrogé par ailleurs concernant la durée de conservation des données de journalisation, le Demandeur a également précisé ce qui suit :

> « *Il y a une journalisation et audit* ***concernant les comptes d'utilisateur par le SPF BOSA*** *qui* ***conserve pendant 10 ans les données suivantes*** *:*
> - *Nom;*
> - *Prénom;*
> - *CanSign (true or false);*
> - *Date de la création du compte;*
> - *Date de la modification du compte;*
> - *Raison de terminaison du compte;*

- *Signature des conditions d'utilisation;*
- *Action d'activation de la clé privée pour apposer une signature (sans le document).*

*Au niveau des **logs qui concernent les certificats**, la base de données ne contient rien de plus que les données reprises dans le certificat ainsi que les événements liés au cycle de vie du certificat : réception de la demande de certificat, création et gestion du certificat. Les données du certificat sont conservées par le sous-traitant du SPF BOSA et du SPF IBZ, ZETES SA, pendant **7 ans conformément aux exigences du règlement eIDAS**.*

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.

Les logs de consultation du Registre National sont réglés par l'article 17 de la loi du 8 août 1983 organisant un registre national des personnes physiques » (mis en gras par l'Autorité).

54. L'Autorité prend acte de cette réponse. Cette réponse est néanmoins potentiellement partielle : qu'en est-il de la journalisation relative au service **d'apposition** de signatures électroniques, à supposer que l'objectif du Projet soit bien de réglementer également ce service[51] ? Compte-tenu de l'importance de la journalisation dans le cadre du Projet et de la fourniture des services de confiance qualifiés concernés, l'Autorité est d'avis que **le Demandeur pourrait envisager de prévoir** dans le Projet ou plutôt dans un arrêté d'exécution de celui-ci **la journalisation qui doit être mise en œuvre** (données et durée de conservation de celles-ci), **dans la mesure où celle-ci ne serait pas déjà définie dans le contexte normatif** (y compris les normes techniques rendues applicables) **du Règlement EIDAS lui-même**. Il appartient au demandeur de vérifier et justifier si est nécessaire ou pas un cadre normatif complémentaire aux fins de l'encadrement des traitements de données de journalisation nécessaires à la mise en œuvre du Projet.

[51] Voir le considérant n° 21.

II.5. Durée de conservation des données

55. L'article 3, § 5, du Projet dispose que les données du Registre des comptes utilisateurs[52] sont conservées « *pendant 30 ans après désactivation* » du compte. L'exposé des motifs indique que « *Ce délai a été fixé en prenant en considération le délai maximal de prescription possible en droit belge* ». L'Autorité a invité le Demandeur à lui indiquer de quel délai de prescription il était question (fondement légal). Celui-ci a précisé ce qui suit :

> « *Nous avons retenu ce délai de 30 ans car c'est le délai prévu pour les données enregistrées dans le registre national des personnes physiques.*
> *Afin d'éviter qu'une même information enregistrée dans des banques de données différentes ne soit pas effacée dans une et maintenue malgré tout dans une autre, il nous a semblé nécessaire d'aligner les durées de conservation des informations, dès lors que ce délai correspond au délai maximal de prescription (certes, principalement en matière pénale) applicable en droit national* ».

56. La durée de conservation des données **doit être déterminée par le Projet <u>à l'aune de la finalité poursuivie par celui-ci</u>**. Le fait que de mêmes données puissent être conservées pour des durées différentes dans des systèmes différents poursuivant des finalités distinctes est logique au regard du RGPD et des articles 8 CEDH et 22 de la Constitution. Le Registre des comptes utilisateurs prévu par le Projet ne poursuit pas la même finalité que le Registre national des personnes physiques. Chaque finalité de traitement nécessite une évaluation de la durée de traitement nécessaire des données. En outre, l'Autorité ne perçoit pas directement le lien logique entre la durée de conservation des données du Registres des comptes des utilisateurs et le délai de prescription maximal existant en droit belge (d'ailleurs, bien que l'Autorité ne mène pas cette analyse, on peut s'interroger sur la plus-value concrète de ses données qui seules, se limitent en fait à lier une personne à un compte utilisateur et à son numéro).

57. **Il revient au Demandeur de motiver dans l'exposé des motifs du Projet la durée de conservation qu'il fixe dans son Projet et le cas échéant, d'adapter celle-ci si elle n'est pas conforme aux principes juste rappelés.**

58. Plus fondamentalement, peu de données sont visées à l'article 3, § 5, du Projet et il est clair que d'autres catégories de données à caractère personnel seront traitées par le SPF Intérieur et le SPF Stratégie et Appui telles que par exemple les données de journalisation concernant la création et la gestion des certificats ou concernant la gestion des comptes et l'utilisation du service de signature

[52] Voir le considérant n° 37.

électronique, et encore, les données de vérification des conditions à remplir en relation avec les comptes utilisateurs. L'Autorité a interrogé le demandeur à ce sujet et celui-ci a communiqué les éléments de réponse cités au considérant n° 53 au sujet desquels l'Autorité s'est positionnée dans le considérant n° 54. *In fine*, en l'état du Projet, il incombera aux responsables du traitement de fixer la durée de conservation des données de journalisation conformément notamment aux normes techniques applicables en vertu du Règlement EIDAS.

II.6. Divers

59. L'article 3, § 1er du Projet indique que pour créer un compte utilisateur, le citoyen doit marquer son accord quant aux **conditions d'utilisation** qui sont disponibles via le site de la Direction générale Identité et Affaires citoyennes du Service public fédéral Intérieur et du Service public fédéral Stratégie et Appui. L'Autorité observe que cette étape de la création du compte utilisateur peut aussi utilement être utilisée pour informer correctement l'utilisateur au sujet des traitements de données à caractère personnel mis en œuvre par le SPF Intérieur et par le SPF Stratégie et Appui en exécution du Projet, conformément aux articles 12 et 13 du RGPD. Il sera également important à cette étape, d'informer clairement la personne concernée quant aux services offerts et à la possibilité de recourir séparément à chacun de ceux-ci[53].

PAR CES MOTIFS,
L'Autorité est d'avis que,

1. Sur la base de l'hypothèse réalisée en fonction des réponses communiquées par le Demandeur, le dispositif mis en place est apte à accomplir l'objectif poursuivi (création de signature électronique qualifiée à distance) (**considérants nos 4-8**) ;

2. La portée du Projet (« *refonte complète de notre service de signature existant* », offre de « *la fonctionnalité de signature via le portefeuille belge pour l'identité numérique* » et fort probable disparition de la possibilité pour le citoyen de signer électroniquement de manière qualifiée au moyen d'un certificat de signature électronique présent sur sa carte d'identité électronique) devrait être mieux mise en évidence à titre introductif, dans l'exposé des motifs du Projet.

Il est recommandé d'envisager la possibilité de maintenir une solution de signature électronique qualifiée du type de celle qui existe actuellement (signature via un certificat de signature électronique qualifié sur la puce de la carte d'identité électronique), étant entendu

[53] Voir les considérants nos 21-22.

qu'il appartient au Demandeur de vérifier si cela est ou pas possible dans le cadre normatif et technique du Règlement EIDAS tel que réformé par le Règlement EIDAS2. Le choix posé en la matière doit être l'objet d'une analyse d'impact relative à la protection des données (**considérants nos 9-12**) ;

3. Le Projet doit identifier clairement, en s'alignant sur les concepts définis dans le Règlement EIDAS, les services auxquels il s'applique, et articuler son dispositif (conditions d'accès au service ; journalisation ; responsables du traitement) en fonction des services concernés. Si l'intention du Demandeur est d'encadrer par son Projet un service d'apposition de signature (une application web), il convient de définir ce service, et ensuite, d'en encadrer le fonctionnement et la fourniture à la manière dont sont encadrés les autres services de confiance concernés. Sous réserve de ce qui suit, l'analyse n'est pas poursuivie sur ce point. Le Projet doit être clair quant à l'offre des services concernés aux citoyens : quels services peuvent être utilisés séparément ou quels services doivent être utilisés de manière intégrée (**considérants nos 17-24**) ;

4. Le Projet doit être précisé afin d'identifier clairement quelles entités sont responsables (conjointes ou pas) de quels traitements de données à caractère personnel dans le cadre de l'identification et de l'authentification des utilisateurs ainsi que de la fourniture des différents services de confiance (ou service simplement) prévus par le Projet. S'agissant des responsabilités conjointes au regard du traitement prévues par le Projet, à titre de garantie complémentaire en matière de transparence, le Demandeur devrait vérifier si le Projet ne pourrait pas prévoir la publication de la convention qui sera conclue (**considérants nos 25-36**) ;

5. Sur le plan des principes, si une norme technique est rendue obligatoire en vertu du droit européen, il appartient au législateur, lorsque cela est possible, d'adapter le droit belge de manière telle que cette norme puisse être mise en œuvre conformément au principe de minimisation des données consacré dans le RGPD (**considérant n° 40**) ;

6. L'utilisation des services prévus par le Projet par la personne concernée nécessite la vérification de son identité telle que visée à l'article 24, 1*bis*., du Règlement EIDAS (**considérants nos 42-43**) ;

7. Sans préjudice du point suivant, l'article 4, § 5, du Projet doit être adapté (**considérants nos 44-47**) ;

8. Les arguments avancés pour ne pas prévoir la création de certificats qualifiés de signature électronique sans le numéro de Registre national ne sont pas complètement convaincants. Le maintien d'une solution technique dans le cadre de laquelle le numéro de Registre national est une donnée incluse dans le certificat qualifié de signature électronique implique une circulation et un traitement significatif des numéros de Registre national de la population belge, cela d'autant plus qu'il sera toujours plus fréquemment recouru à la signature électronique dans la société contemporaine. Le choix posé en la matière doit dans tous les cas être l'objet d'une analyse d'impact relative à la protection des données (**considérants nos 44-51**) ;

9. Le Demandeur pourrait envisager de prévoir dans le Projet ou plutôt dans un arrêté d'exécution de celui-ci la journalisation qui doit être mise en œuvre (données et durée de conservation de celles-ci), dans la mesure où celle-ci ne serait pas déjà définie dans le contexte normatif (y compris les normes techniques rendues applicables) du Règlement EIDAS. Il appartient au demandeur de vérifier et justifier si est nécessaire ou pas un cadre normatif complémentaire aux fins de l'encadrement des traitements de données de journalisation nécessaires à la mise en œuvre du Projet (**considérants nos 52-54 et 59**) ;

10. Il revient au Demandeur de motiver dans l'exposé des motifs du Projet la durée de conservation qu'il fixe dans son Projet et le cas échéant, d'adapter celle-ci si elle n'est pas conforme aux principes rappelés dans le présent Avis (**considérants nos 55-57**).

Pour le Service d'Autorisation et d'Avis,
(sé) Alexandra Jaspar, Directrice