SERVICE PUBLIC FEDERAL INTERIEUR

[C − 2021/32042]

18 JUILLET 2021. — Arrêté royal relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée

RAPPORT AU ROI

Sire,

Le projet d'arrêté royal que nous avons l'honneur de soumettre à la signature de Votre Majesté est relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée.

1. CONSIDERATIONS GENERALES

Sire, l'article 40, § 3 de la loi sur la fonction de police donne au Roi deux missions en matière de signature électronique des procès-verbaux par la police intégrée.

(1) Il doit premièrement fixer «les mesures de sécurité et les normes techniques minimales auxquelles doivent répondre les systèmes informatiques policiers qui produisent le cachet électronique avancé».

L'établissement de ces mesures de sécurité et normes techniques minimales relatives au cachet électronique avancé dans le cadre de la signature des procès-verbaux a pour but de renforcer la confiance dans l'utilisation qui en est faite par la police intégrée sur la base de l'article 40, § 2, 1° à 3° de la loi sur la fonction de police et dès lors son acceptation forte, non seulement par les partenaires de la chaîne pénale et de sécurité mais aussi par les citoyens.

Ce cadre d'utilisation du cachet électronique avancé concerne trois catégories de procès-verbaux, à savoir :

1°) celle où le verbalisateur n'est légalement pas tenu de s'identifier nominativement dans le procès-verbal ;

2°) celle comprenant les procès-verbaux qui doivent être signés en grand volume relatifs aux constatations effectuées dans le cadre des articles 62 et 65, § 1er, de la loi du 16 mars 1968 relative à la police de la circulation routière ;

3°) les catégories de procès-verbaux déterminées par le Collège des procureurs généraux relatifs à des infractions déterminées qui, en fonction de la nature des faits et des circonstances de l'affaire, ne font pas ou pas encore l'objet de poursuites de la part du ministère public.

Si la technologie du cachet électronique avancé est utilisée pour signer les procès-verbaux, c'est essentiellement parce qu'elle permet de signer en une seule fois une quantité importante de procès-verbaux, ce qui est gage d'efficacité dans certains processus policiers, tels ceux relatifs aux perceptions immédiates, tout en maintenant un haut degré de sécurité.

L'importance de la confiance qui doit être accordée à la signature à l'aide d'un cachet électronique avancé a été d'emblée soulignée ; cependant, celle-ci ne saurait bien entendu pas d'office impliquer de dévoiler dans les moindres détails, l'ensemble de ces mesures de sécurité et normes techniques sous-jacentes à sa production, sous peine précisément de compromettre la sécurité desdits systèmes et donc paradoxalement de nuire à la sécurité originellement recherchée.

Néanmoins, comme sollicité par le Conseil d'Etat dans son avis 66.584/2 du 14 octobre 2019 et par l'Organe de contrôle de l'information policière dans son avis DA190008 du 11 avril 2019, le projet a été complété en vue de donner plus de précisions quant aux mesures de sécurité et aux normes techniques minimales auxquelles doivent répondre les systèmes informatiques policiers qui produisent le cachet électronique avancé.

C'est dans cette optique que les articles 2 à 11 et l'annexe au présent :

- énoncent les dispositions relatives aux éléments de sécurité standards des systèmes informatiques utilisés lors de la production du cachet électronique avancé ;

- décrivent la fonction de hash utilisée ;

- déterminent le processus d'utilisation des certificats et des clés de chiffrement, les modalités de stockage des certificats, le mécanisme d'horodatage, l'identification et l'authentification des membres du personnel ;

- rendent obligatoires les journalisations et un contrôle humain lors de l'apposition du cachet ;

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN

[C − 2021/32042]

18 JULI 2021. — Koninklijk besluit betreffende de veiligheidsmaatregelen en de minimale technische normen voor de informaticasystemen van de politie die het geavanceerde elektronisch zegel produceren, en de vermeldingen die in het geavanceerde elektronisch zegel en de gekwalificeerde elektronische handtekening voorkomen

VERSLAG AAN DE KONING

Sire,

Het ontwerp van koninklijk besluit dat ik de eer heb aan Uwe Majesteit ter ondertekening voor te leggen, heeft betrekking op de veiligheidsmaatregelen en de minimale technische normen voor de informaticasystemen van de politie die het geavanceerde elektronische zegel produceren, en de vermeldingen die in het geavanceerde elektronische zegel en de gekwalificeerde elektronische handtekening voorkomen.

1. ALGEMENE INLEIDING

Sire, artikel 40, § 3 van de wet op het politieambt geeft de Koning twee taken met betrekking tot het elektronisch ondertekenen van processen-verbaal door de geïntegreerde politie.

(1) Hij moet ten eerste "de veiligheidsmaatregelen en de minimale technische normen waaraan de informaticasystemen van de politie die het geavanceerde elektronische zegel produceren, moeten voldoen" vaststellen.

Het invoeren van deze veiligheidsmaatregelen en minimale technische normen met betrekking tot het geavanceerde elektronische zegel in het kader van het ondertekenen van processen-verbaal dient om het vertrouwen te vergroten in de toepassing ervan door de geïntegreerde politie op basis van artikel 40, § 2, 1° t/m 3° van de wet op het politieambt en dientengevolge sterke aanvaarding ervan, niet alleen door de partners van de strafrechtelijke keten en veiligheidsketen, maar ook door de burgers.

Dit toepassingskader van het geavanceerde elektronische zegel betreft drie categorieën processen-verbaal, te weten :

1°) gevallen waarin de verbalisant wettelijk niet gehouden is zich bij naam te identificeren in het proces-verbaal;

2°) gevallen waarin de processen-verbaal met zich meebrengen dat er een grote hoeveelheid processen-verbaal moet worden ondertekend, die met betrekking tot de vaststellingen verricht in het kader van artikel 62 en 65, § 1, van de wet van 16 maart 1968 betreffende de politie over het wegverkeer;

3°) de categorieën processen-verbaal met betrekking tot bepaalde strafbare feiten die, afhankelijk van de aard van de feiten en omstandigheden van de zaak, niet of nog niet worden vervolgd door het openbaar ministerie, oftewel de vereenvoudigde processen-verbaal.

De belangrijkste reden voor het gebruik van de technologie van het geavanceerde elektronische zegel om processen-verbaal te ondertekenen, is dat daarmee een groot aantal processen-verbaal in één keer kan worden ondertekend, hetgeen efficiënt is in bepaalde politieprocessen, zoals die in verband met onmiddellijke inningen, terwijl een hoog veiligheidsniveau wordt gehandhaafd.

Van meet af aan is gewezen op het belang van het vertrouwen dat moet worden gesteld in de handtekening met een geavanceerd elektronisch zegel, dit vertrouwen kan echter niet automatisch inhouden dat al deze veiligheidsmaatregelen en technische normen die aan de totstandkoming ervan ten grondslag liggen tot in de kleinste details openbaar mogen worden gemaakt, precies om de veiligheid van deze systemen en dus paradoxaal genoeg de oorspronkelijk beoogde veiligheid niet in gevaar te brengen.

Niettemin is het ontwerp, zoals gevraagd door de Raad van State in zijn advies 66.584/2 van 14 oktober 2019 en door het Controleorgaan op de politionele informatie in zijn advies DA190008 van 11 april 2019, aangevuld om meer preciseringen te geven over de veiligheidsmaatregelen en de minimale technische normen waaraan de informaticasystemen van de politie die het geavanceerd elektronisch zegel produceren, moeten voldoen.

Het is vanuit dit oogpunt dat artikelen 2 tot 11 en de bijlage hierbij :

- de bepalingen vastestellen met betrekking tot de standaardveiligheidselementen van de gebruikte informaticasystemen die worden gebruikt voor de productie van het geavanceerde elektronische zegel;

- de gebruikte hashfunctie beschrijven;

- het gebruiksproces van de certificaten en de encryptiesleutels, de bewaarmodaliteiten van de certificaten, het tijdstempelmechanisme, de identificatie en de authenticatie van de personeelsleden bepalen;

- logbestanden en een menselijke controle bij het aanbrengen van het zegel verplicht maken;

- prévoient un audit régulier des mesures et du système de management de la sécurité de l'information et

- déterminent les exigences en cas de sous-traitance qui devront être mises en place pour mettre en œuvre le service de signature de la police ou en anglais le Police Signing Service (ci-après « PSS ») qui permet de produire le cachet électronique avancé.

Ces mesures de sécurité et normes techniques sont établies conformément au 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.

L'implémentation de ces normes techniques est liée à l'évolution constante de la technologie et est donc par essence mouvante (voir par exemple à cet égard les travaux du comité technique ESI (Electronic Signatures and Infrastructures) de l'ETSI (*European Telecommunications Standards Institute*)).

Cette évolution constante va aussi être reflétée dans les audits de ces normes et mesures de sécurité qui seront réalisés tous les 5 ans.

Les normes techniques et mesures de sécurité présentes dans le projet d'arrêté royal constituent néanmoins le socle commun entourant la production et l'utilisation du cachet électronique avancé dans le cadre de la signature des procès-verbaux précisée à l'article 40, § 2, 1° à 3° de la loi sur la fonction de police.

Par ailleurs, pour répondre à une des remarques du Conseil d'Etat, ces normes techniques se basent, d'une part, sur les standards généraux de sécurité des systèmes de la police intégrée et, d'autre part, sur les standards spécifiques d'application en matière de cachet électronique avancé dont, bien entendu, ceux découlant du Règlement européen eIDAS, et en particulier son article 36, à savoir le fait que le cachet avancé doit :

1°) permettre d'identifier le créateur du cachet, ce qui est notamment précisé à l'article 4 ;

2°) être lié au créateur du cachet de manière univoque : cette condition est rencontrée par le fait que la clé privée fait l'objet de mesures de sécurité idoines et ne peut donc pas être contrefaite par un tiers ;

3°) avoir été créé à l'aide de données de création du cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle : il s'agit pour la police de créer, dans un environnement qu'elle gère, directement le cachet électronique avancé, d'appliquer des procédures de sécurité spécifiques en matière de gestion et d'administration et d'utiliser des systèmes et des produits de confiance afin de garantir que l'environnement de création de signatures électroniques est fiable et qu'il est utilisé sous son contrôle exclusif. C'est dans cette optique que les clés privées font l'objet de mesures de sécurité idoines et que les certificats de signature sont gérés sur la base de l'article 5 par la police, conformément sur la base de procédures auditables ;

4°) et être lié aux données auxquelles il est associé de telle sorte qu'une possibilité de modification indétectable de données soit exclue : l'article 3 précise à cet effet le mécanisme de hachage qui est utilisé.

Il s'agit donc pour la police d'adopter des mesures techniques pour assurer un lien logique entre le procès-verbal et la signature par cachet électronique avancé de sorte que toute modification ultérieure puisse être détectée.

(2) L'article 40, § 3 de la loi sur la fonction de police demande ensuite au Roi de déterminer les mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée.

Si la signature électronique se différencie de la signature écrite notamment par le fait qu'elle n'est pas visuelle mais correspond en réalité à un nombre ou une suite de chiffres, il doit être possible de visualiser lors du traitement électronique qu'une signature électronique a été utilisée.

Il va de soi que cette matérialisation doit aussi être apportée « sur papier », même si la signature électronique est par essence appelée à exister et à rester dans un monde digital.

- voorzien in een regelmatige audit van de maatregelen en van het managementsysteem voor informatiebeveiliging en

- de noodzakelijke vereisten in geval van verwerking door de verwerker bepalen om de handtekeningendienst van de politie, of in het Engels de Police Signing Service (hierna 'PSS'), die het mogelijk maakt het geavanceerd elektronisch zegel te produceren, op te zetten.

Deze veiligheidsmaatregelen en technische normen worden opgesteld overeenkomstig Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

De implementering van deze technische normen houdt verband met de voortdurende technologische ontwikkelingen en is dus per definitie evolutief (zie in dit verband bijvoorbeeld de werkzaamheden van het technisch comité ESI (*Electronic Signatures and Infrastructures) van ETSI (European Telecommunications Standards Institute*)).

Deze voortdurende ontwikkelingen zullen zich ook weerspiegelen in de audits van deze normen en veiligheidsmaatregelen die om de 5 jaar zullen plaatsvinden.

De technische normen en veiligheidsmaatregelen vervat in het ontwerp van het koninklijk besluit vormen niettemin de gemeenschappelijke grondslag voor de productie en het gebruik van het geavanceerd elektronisch zegel in het kader van de ondertekening van processenverbaal, zoals vermeld in artikel 40, § 2, 1° tot 3° van de wet op het politieambt.

Om te antwoorden op een van de opmerkingen van de Raad van State, zijn deze technische normen enerzijds gebaseerd op de algemene veiligheidsstandaarden voor de systemen van de geïntegreerde politie en anderzijds op de geldende specifieke standaarden voor het geavanceerd elektronisch zegel, waaronder natuurlijk deze die voortvloeien uit de Europese eIDAS-verordening, in het bijzonder artikel 36 van deze verordening, namelijk dat het geavanceerd zegel :

1°) het mogelijk moet maken de aanmaker van het zegel te identificeren, wat met name in artikel 4 wordt vermeld;

2°) op unieke wijze aan de aanmaker van het zegel verbonden moet zijn : aan deze voorwaarde wordt voldaan omdat de private sleutel het voorwerp uitmaakt van passende veiligheidsmaatregelen en dus niet door een derde kan worden nagemaakt;

3°) tot stand moet komen met gebruikmaking van gegevens voor het aanmaken van elektronische zegels die de aanmaker van het zegel met een hoog vertrouwensniveau onder zijn controle kan gebruiken voor de politie betekent dit in een door haar beheerde omgeving rechtstreeks het geavanceerd elektronisch zegel aanmaken, specifieke veiligheidsprocedures toepassen wat betreft beheer en administratie en gebruikmaken van vertrouwde systemen en producten om te waarborgen dat de omgeving waarin de elektronische handtekening wordt aangemaakt betrouwbaar is en dat uitsluitend zij controle heeft over het gebruik ervan. Daarom maken de private sleutels het voorwerp uit van passende veiligheidsmaatregelen en worden de handtekeningcertificaten op basis van artikel 5 door de politie, op basis van een auditeerbare procedure, beheerd;

4°) op zodanige wijze aan de gegevens waarop het betrekking heeft verbonden zijn dat de mogelelijkheid tot onmerkbare wijziging van gegevens kan worden uitgesloten : artikel 3 vermeldt daartoe het gebruikte hashingmechanisme.

De politie moet dus technische maatregelen nemen om voor een logisch verband tussen het proces-verbaal en de ondertekening, door middel van een geavanceerd elektronisch zegel, te zorgen zodat elke wijziging achteraf kan worden opgespoord.

(2) Artikel 40, § 3 van de wet op het politieambt verlangt vervolgens dat de Koning vaststelt welke vermeldingen voorkomen in het geavanceerde elektronische zegel en de gekwalificeerde elektronische handtekening.

Ook al verschilt de elektronische handtekening met name van de schriftelijke handtekening doordat zij niet visueel is, maar in feite overeenkomt met een getal of een reeks cijfers, toch kan met sommige programma's de elektronische handtekening concreet 'op het scherm' worden weergegeven.

Het spreekt vanzelf dat deze concretisering ook 'op papier' kan worden verschaft, ook al is en blijft de elektronische handtekening per definitie bestemd voor digitaal gebruik.

Enfin, Sire, s'il est compréhensible que la mise en œuvre de la signature électronique puisse susciter des craintes vu son caractère relativement neuf, notamment au sein de certains services publics, il est néanmoins important de rappeler dans cette introduction générale qu'elle offre des avantages importants en termes de sécurité (intégrité du document, authentification du signataire, infalsifiabilité et non répudiation par le signataire), de praticabilité (signer un lot de procès-verbaux en une seule fois, il y a autant d'originaux que de documents signés électroniquement) et d'interopérabilité, qui ne sont simplement pas possibles avec une signature manuelle, même si cette dernière est, uniquement pour des raisons historiques, considérée comme une référence.

2. COMMENTAIRE DU CHAPITRE PREMIER

L'article **premier** introduit les définitions nécessaires. Concernant le « règlement eIDAS », la « signature électronique qualifiée » et le « cachet électronique avancé », il est renvoyé au 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.

Le « service de signature de la police » est défini comme le service informatique policier qui produit le cachet électronique avancé, ainsi que les mentions qui figurent dans le cachet électronique avancé. Ce service intègre différents composants technologiques, des processus et des procédures de travail spécifiques et repose sur d'autres services IT transversaux aux systèmes policiers.

La notion « d'authentification forte » est également définie. L'authentification forte mise en place comprend des éléments appartenant aux deux catégories suivantes :

-"connaissance" (quelque chose que seul l'utilisateur connaît),

- "possession" (quelque chose que seul l'utilisateur possède),

lesquels sont indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité de l'autre, de manière à protéger la confidentialité des données d'authentification.

Enfin, il est également précisé que le procès-verbal vise tant le corps du procès-verbal que, le cas échéant, ses annexes.

Pour répondre à une remarque du Conseil d'Etat, la partie utilisatrice est celle qui va recevoir le procès-verbal (le verbalisé, son avocat, le juge,...) et le signataire est le membre du personnel qui appose le cachet électronique ou la signature qualifiée. Si le cachet avancé est créé par une personne morale, c'est *in fine* bien entendu un membre du personnel et donc une personne physique qui va l'utiliser pour signer un procès-verbal. Néanmoins, comme recommandé par le Conseil d'Etat, le présent projet n'utilise pas le terme signataire lorsqu'il est question de cachet électronique.

3. COMMENTAIRE DU CHAPITRE II

L'article 2 précise les mesures de sécurité applicables aux systèmes informatiques qui seront utilisés. Ces mesures établissent un socle de base pour l'ensemble de l'infrastructure technique.

L'article 3 décrit le système technologique de « hash » (fonction de hachage cryptographique) qui est utilisé en vue de prouver l'intégrité du fichier informatique qui est signé. En créant un « condensé » (un hash) unique au moyen d'un algorithme informatique, il peut à tout moment être démontré que le document signé n'est ni modifié ni altéré. Le chiffrement SHA256, exigé comme minimum sur la base des connaissances actuelles, calcule une empreinte numérique de 256 bits soit 32 octets, dont l'écriture hexadécimale comprend 64 caractères.

L'article 4 décrit le mécanisme utilisé en vue de procéder à la vérification de l'identité du créateur du cachet. Le mécanisme de cryptographie asymétrique utilisé est un domaine de la cryptographie où il existe une distinction entre des données publiques et privées. Dans le cas présent, une clé privée est utilisée pour signer et la clé publique disponible sur un site internet permet de vérifier que le document a bien été signé par une entité autorisée.

Un des éléments essentiels de la sécurité du processus de chiffrement est de garantir la sécurité des clés utilisées. Dans le cadre du PSS, la protection des clés privées est bien entendu aussi un élément essentiel de l'ensemble des mesures de sécurité. Il est dès lors prévu que le délégué à la protection des données désigné auprès du Commissariat général donne un avis quant au stockage et à la gestion des certificats de signature électronique.

L'article 5 fixe les conditions de sécurisation des certificats de signature électronique et des clés privées. Ce volet « sécurisation » devra aussi faire partie de l'audit prévu à l'article 11.

Ten slotte, Sire, is het logisch dat de toepassing van de betrekkelijk nieuwe elektronische handtekening mogelijk enige zorg zal wekken, met name binnen bepaalde overheidsdiensten. Desalniettemin is het belangrijk om er in deze algemene inleiding aan te herinneren dat zij grote voordelen biedt op het gebied van veiligheid (integriteit van het document, legalisatie van de handtekening, niet-vervalsbaarheid, geen verwerping door de ondertekenaar), bruikbaarheid (een grote hoeveelheid processen-verbaal in één keer ondertekenen, er zijn evenveel originelen als elektronisch ondertekende documenten) en interoperabiliteit, die eenvoudigweg niet mogelijk zijn met een handmatige handtekening, ook al wordt deze laatste, uitsluitend om historische redenen, beschouwd als het uitgangspunt.

2. COMMENTAAR BIJ HET EERSTE HOOFDSTUK

Artikel **1** bevat de nodige definities. Voor de 'eIDAS-verordening', de 'gekwalificeerde elektronische handtekening' en het 'geavanceerd elektronisch zegel' wordt verwezen naar Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

De 'handtekeningendienst van de politie' wordt gedefinieerd als de politionele informaticadienst die het geavanceerd elektronisch zegel vervaardigt, alsmede de vermeldingen die in het geavanceerd elektronisch zegel voorkomen. Deze dienst omvat verschillende technologische componenten, specifieke werkprocessen en -procedures en steunt op andere transversale IT-diensten binnen de politiesystemen.

Het begrip 'sterke authenticatie' wordt eveneens gedefinieerd. De geïmplementeerde sterke authenticatie omvat elementen die tot en twee volgende categorieën behoren :

-'kennis' (iets dat alleen de gebruiker weet) en

- 'bezit' (iets dat alleen de gebruiker bezit),

die losstaan van elkaar in die zin dat de compromittering van het ene de betrouwbaarheid van het andere niet in het gedrang brengt, en ze is zo ontworpen dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd.

Ten slotte wordt ook gespecificeerd dat het proces-verbaal zowel de hoofdtekst als in voorkomend geval de bijlagen bevat.

Om te antwoorden op een opmerking van de Raad van State, de bestemmeling is degene die het proces-verbaal zal ontvangen (de geverbaliseerde, zijn advocaat, de rechter, ...) en de ondertekenaar is het personeelslid dat het elektronisch zegel of de gekwalificeerde handtekening aanbrengt. Indien het geavanceerde zegel door een rechtspersoon is gecreëerd, is het natuurlijk uiteindelijk een personeelslid en dus een natuurlijke persoon die het zal gebruiken om een proces-verbaal te ondertekenen. Niettemin wordt in dit ontwerp, zoals door de Raad van State is aanbevolen, de term ondertekenaar niet gebruikt wanneer wordt verwezen naar de elektronische stempel.

3. COMMENTAAR BIJ HOOFDSTUK II

Artikel 2 vermeldt de veiligheidsmaatregelen die op de gebruikte informaticasystemen van toepassing zijn. Deze maatregelen vormen de basis van de hele technische infrastructuur.

Artikel 3 beschrijft het technologische 'hashsysteem' (cryptografische hashingfunctie) dat wordt gebruikt om de integriteit van het ondertekende informaticabestand aan te tonen. Door één enkele 'gecomprimeerde versie' (een hash) aan te maken door middel van een computeralgoritme, kan op elk moment worden aangetoond dat het ondertekende document niet gewijzigd of aangepast is. De SHA256-versleuteling, die minimaal vereist is op basis van de huidige kennis, berekent een digitale vingerafdruk van 256 bits of 32 bytes, waarvan de hexadecimale notatie uit 64 tekens bestaat.

Artikel 4 beschrijft het mechanisme dat wordt gebruikt om de identiteit van de aanmaker van het zegel te verifiëren. Het gebruikte asymmetrische cryptografiemechanisme is een domein van de cryptografie waarin er een onderscheid bestaat tussen publieke en privégegevens. In dit geval wordt een private sleutel gebruikt om te ondertekenen en maakt de online beschikbare publieke sleutel het mogelijk te verifiëren of het document wel degelijk door een gemachtigde entiteit is ondertekend.

Een van de essentiële elementen voor de veiligheid van het versleutelproces is het waarborgen van de veiligheid van de gebruikte sleutels. In het kader van de PSS is de bescherming van de private sleutels uiteraard ook een essentieel onderdeel van het geheel van veiligheidsmaatregelen. Daarom is bepaald dat de bij het Commissariaat-generaal aangewezen functionaris voor gegevensbescherming advies verstrekt over het bewaren en beheren van certificaten voor elektronische handtekening.

Artikel 5 bepaalt de beveiligingsvoorwaarden van de certificaten voor elektronische handtekening en de private sleutels. Dit luik 'beveiliging' moet ook deel uitmaken van de geplande audit krachtens artikel 11.

Le processus de signature électronique vise entre autres à pouvoir fixer et démontrer que les certificats de signature sont valables et que les procès-verbaux signés l'ont été à un moment précis. Le mécanisme utilisé pour ce faire et mentionné à **l'article 6** est l'horodatage (en anglais timestamping) qui consiste à associer une date et une heure à un événement, la signature dans le cas présent.

L'article 7 décrit les exigences d'identification et d'authentification des membres des services de police avant d'accéder au PSS.

Cette identification en amont est un élément clé du processus lorsqu'elle est couplée à la vérification des fonctions et mandats de la personne qui s'identifie. En effet, de la sorte, seuls les membres du personnel qui occupent une fonction spécifique et qui sont autorisés, sauront accéder à ces systèmes informatiques.

Autrement formulé, il s'agira dès lors que ces systèmes :

- identifient le membre du personnel qui souhaite utiliser un cachet électronique ;

- soient paramétrés de telle sorte que seuls ceux qui y sont autorisés puissent utiliser le module applicatif relatif au cachet électronique avancé.

Ceci implique notamment que les systèmes policiers puissent réaliser une distinction entre différents types de profils : par exemple un utilisateur qui a un mandat technique pour intervenir sur le module de cachet, d'un utilisateur, fonctionnaire de police ou membre du personnel du cadre administratif et logistique habilité qui souhaite apposer un cachet électronique avancé sur des procès-verbaux.

Cette identification est décrite dans les articles 4, 7 et 9 de l'arrêté royal.

En outre, dès lors que le membre du personnel s'est identifié et que ses droits ont été vérifiés, il doit aussi s'authentifier avant de pouvoir engendrer un cachet électronique sur des procès-verbaux (au moyen d'un système d'authentification forte (cfr. article 7)). Cette authentification forte peut être utilisée une seule fois pour un lot de procès-verbaux. Elle sera en outre reprise dans les journaux (voir articles 8 et 9). Par cet acte d'authentification forte, le verbalisateur formalise sa volonté individuelle et libre de prendre à son nom propre et à son compte les constatations qui sont faites dans les procès-verbaux.

Cette authentification forte et les journalisations y associées renforcent par ailleurs le fait que le signataire qui a engendré le cachet sur un procès-verbal ne pourra pas ultérieurement le nier.

Le recours à un cachet électronique pour signer les procès-verbaux constitue un traitement spécifique qui aura un impact sur le reste de la chaîne pénale. Dès lors, le respect des règles permettant d'assurer la traçabilité de tous les actes posés est assuré via le recours à des journaux de traitements (Loggings) devant permettre d'établir pour tous les traitements liés au cachetage des procès-verbaux, qui a réalisé quel traitement, à quel moment et pourquoi (cfr. **articles 8 et 9**).

Cette traçabilité est bien entendu un élément déterminant en termes d'« accountability ». La signature électronique des procès-verbaux est un traitement qui relève du titre II de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. L'obligation de journalisation prévue à l'article 56 s'applique dès lors. L'article 8 fixe le délai de conservation de ces loggings à 5 ans après la destruction du procès-verbal en se basant sur les délais fixés dans la loi sur la fonction de police.

L'article 9 apporte une garantie supplémentaire quant à l'utilisation du PSS : un cachet électronique avancé ne peut être apposé que suite à une décision volontaire de la personne habilitée à l'apposer.

En exécution de **l'article 10**, les mesures de sécurité en vue de s'assurer que le PSS réponde aux objectifs de sécurité que sont la confidentialité, la disponibilité, l'intégrité et la non-répudiation doivent être auditables. Les dispositions reprises en annexe à l'arrêté royal serviront de modèle à cet audit. Elles sont directement inspirées des normes ISO/IEC 27001 :2013 Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences, ISO/IEC 27002 :2013 Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information et ISO/IEC 27005 :2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information.

Het proces van elektronische handtekening is er onder meer op gericht te kunnen vaststellen en aantonen dat de handtekeningencertificaten geldig zijn en dat de ondertekende processen-verbaal op een bepaald tijdstip zijn ondertekend. Het mechanisme dat hiervoor wordt gebruikt en dat in **artikel 6** wordt vermeld, is de tijdstempel (in het Engels timestamping), waarbij een datum en een tijdstip gekoppeld worden aan een gebeurtenis, in dit geval de handtekening.

Artikel 7 beschrijft de identificatie- en authenticatievereisten waaraan de leden van de politiediensten moeten voldoen om toegang te hebben tot de PSS.

Deze identificatie vooraf is een sleutelelement van het proces, wanneer zij gepaard gaat met een verificatie van de functies en mandaten van de persoon die zich identificeert. Op die manier zullen alleen de personeelsleden die een specifieke functie hebben en daartoe gemachtigd zijn, toegang hebben tot deze informaticasystemen.

Met andere woorden, het komt erop aan dat deze systemen :

- het personeelslid identificeren dat een elektronisch zegel wenst te gebruiken en;

- zo ingesteld worden dat enkel gemachtigde personen de toepassingsmodule met betrekking tot het geavanceerde elektronische zegel kunnen gebruiken.

Dit houdt met name in dat de politiesystemen een onderscheid kunnen maken tussen verschillende soorten profielen : bijvoorbeeld een gebruiker die een technisch mandaat heeft om aan de zegelmodule te werken, een gebruiker die politieambtenaar is of een bevoegd personeelslid van het administratief en logistiek kader die een geavanceerd elektronisch zegel wil aanbrengen op processen-verbaal.

Deze identificatie wordt beschreven in de artikelen 4, 7 en 9 van het koninklijk besluit.

Zodra het personeelslid zich heeft geïdentificeerd en zijn rechten zijn geverifieerd, moet hij zich bovendien authentifiëren voordat hij een elektronisch zegel op processen-verbaal kan aanbrengen (door middel van een sterk authenticatiesysteem (cf. artikel 7)). Deze sterke authenticatie kan slechts één keer voor een reeks processen-verbaal worden gebruikt. Ze zal bovendien vermeld worden in de logbestanden (zie artikelen 8 en 9). Door middel van deze sterke authenticatie formaliseert de verbalisant zijn individuele en vrije wil om de vaststellingen in de processen-verbaal in eigen naam en voor eigen rekening te doen.

Deze sterke authenticatie en de daaraan gekoppelde logbestanden versterken bovendien het feit dat de ondertekenaar die het zegel op een proces-verbaal heeft aangebracht, dit achteraf niet kan ontkennen.

Het gebruik van een elektronisch zegel om processen-verbaal te ondertekenen, vormt een specifieke verwerking die een impact zal hebben voor de rest van de strafrechtelijke keten. Bijgevolg wordt de naleving van de regels die de traceerbaarheid garanderen van alle verrichte handelingen gegarandeerd door het gebruik van verwerkingslogboeken (Loggings) die het mogelijk moeten maken om voor alle verwerkingen in verband met de verzegeling van processen-verbaal vast te stellen wie welke verwerking heeft verricht, op welk tijdstip en waarom (cf. **artikelen 8 en 9**).

Deze traceerbaarheid is natuurlijk een bepalend element in termen van 'accountability'. De elektronische ondertekening van processen-verbaal is een verwerking die valt onder titel II van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. De verplichting tot logbestanden bepaald in artikel 56 is bijgevolg van toepassing. Artikel 8 stelt de bewaartermijn van deze logbestanden vast op 5 jaar na de vernietiging van het proces-verbaal, op basis van de termijnen die bepaald zijn in de wet op het politieambt.

Artikel 9 biedt een extra garantie voor het gebruik van de PSS : een geavanceerd elektronisch zegel mag enkel aangebracht worden na een bewuste beslissing van de persoon die bevoegd is om het aan te brengen.

In uitvoering van **artikel 10** moeten de veiligheidsmaatregelen die ervoor moeten zorgen dat de PSS voldoet aan de veiligheidsdoelstellingen van vertrouwelijkheid, beschikbaarheid, integriteit en onweerlegbaarheid controleerbaar zijn. De bepalingen in de bijlage bij het koninklijk besluit dienen als model. Ze zijn rechtstreeks gebaseerd op de normen ISO/IEC 27001 :2013 Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Vereisten, ISO/IEC 27002 :2013 Informatietechnologie - Beveiligingstechnieken - Praktijkcode voor het management van informatiebeveiliging en ISO/IEC 27005 :2018 Informatietechnologie - Beveiligingstechnieken - Risicomanagement voor informatiebeveiliging.

Les mécanismes de signature électronique résultant de systèmes technologiques parfois complexes, il est important de pouvoir démontrer que les mesures de sécurité et les normes techniques sont bien implémentées. Pour ce faire, le PSS et les processus et procédures nécessaires à son fonctionnement seront audités par un service compétant désigné pour ce faire, dépendant directement du Commissaire général de la police fédérale.

Le premier audit sera réalisé un an après la publication de l'arrêté royal et renouvelé tous les 5 ans. L'audit prendra en compte l'ensemble des paramètres du système de management de la sécurité de l'information repris dans l'annexe 1. Ces paramètres ont été fixés en se basant sur la norme ISO/IEC 27001 :2013 Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences.

Par ailleurs, comme responsable du traitement de police judiciaire (article 44/4 de la loi sur la fonction de police les procès-verbaux relèvent en effet exclusivement de la police judiciaire), le ministre de la Justice pourra bénéficier des avis et conseils du délégué à la protection des données (DPO) désigné pour ce traitement. Il s'agit du DPO désigné auprès du Commissariat général qui est par ailleurs également compétent pour les traitements policiers dont les ministres sont également responsables. Il sera associé aux évaluations et aux choix des mesures de sécurité mises en place (voir entre autre l'article 5). Le DPO aura bien évidemment accès aux locaux, aux informations techniques et autres procédures utilisées pour rendre ses différents avis en la matière.

Conformément à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, le rapport d'audit sera transmis à l'Organe de contrôle de l'information policière qui pourra également lui-même évaluer ces mesures et normes techniques.

Le recours à la sous-traitance est autorisé. Si tel est le cas, l'ensemble des mesures de sécurité et normes techniques seront également applicables tout comme l'obligation de se soumettre à un audit (article 11).

4. COMMENTAIRE DU CHAPITRE III

Article 12

Fondamentalement, une signature électronique est totalement différente d'une signature traditionnelle et manuscrite. Dans le « panneau des signatures », elle apparaît sous la forme d'une série de nombres et de lettres associées à un fichier et à la personne à l'origine de la signature.

L'ajout d'un élément visuel n'est donc en soi un élément nécessaire ni au niveau juridique ni au niveau technique mais c'est un des facteurs qui permet de renforcer la confiance et l'acceptabilité vis-à-vis de la signature électronique.

Cet élément restera assurément utile dans un environnement matérialisé tant que l'informatisation ne sera pas généralisée 'end to end' et qu'il subsistera des traitements papier de dossiers.

Au niveau d'un environnement matérialisé (un PV imprimé) et donc d'un monde papier, il s'agira donc de préciser que le PV est signé électroniquement, ainsi que de mettre les nom et prénom du ou des signataires lorsque le procès-verbal est signé via une signature électronique qualifiée et les coordonnées de la personne morale lorsque le procès-verbal est signé par cachet électronique avancé. Dans cette dernière hypothèse, le(s) nom(s) des verbalisateurs sont de toute façon d'office repris dans le corps du procès-verbal.

La visualisation d'une signature digitale (signature électronique qualifiée et cachet électronique avancé) sur **un écran** est bien entendu tributaire des logiciels de lecture.

Ces différents logiciels ont cependant au moins en commun d'afficher les informations du signataire (le nom et prénom de la personne physique en cas de signature qualifiée et les données de la personne morale en cas de signature avec le cachet - dans cette dernière hypothèse, le(s) nom(s) des verbalisateurs sont de toute façon d'office repris dans le corps du procès-verbal), de donner les informations relatives à la validité du certificat de signature (cachet électronique avancé ou signature électronique qualifiée) et de mentionner la date de la signature électronique du procès-verbal.

Aangezien de mechanismen voor elektronische handtekeningen soms complexe technologische systemen zijn, is het van belang te kunnen aantonen dat de veiligheidsmaatregelen en technische normen goed worden toegepast. Daartoe zullen de PSS en de voor de werking ervan noodzakelijke processen en procedures worden geauditeerd door een daartoe aangewezen bevoegde dienst die rechtstreeks afhangt van de commissaris-generaal van de Federale Politie.

De eerste audit zal één jaar na de publicatie van het koninklijk besluit worden uitgevoerd en om de vijf jaar worden herhaald. Bij de audit zal rekening worden gehouden met alle in bijlage 1 genoemde parameters van het managementsysteem voor informatiebeveiliging. Deze parameters zijn vastgesteld op basis van de norm ISO/IEC 27001 :2013 Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Vereisten.

Voorts zal de minister van Justitie als verwerkingsverantwoordelijke van verwerkingen van gerechtelijke politie (article 44/4 van de wet op het politieambt- de processen-verbaal vallen in feite uitsluitend onder de bevoegheid van de gerechtelijke politie) advies en raad kunnen krijgen van de functionaris voor gegevensbescherming (DPO) die voor deze verwerking is aangewezen. Het gaat om de bij het Commissariaatgeneraal aangewezen DPO die bovendien ook bevoegd is voor de politionele verwerkingen waarvoor de ministers ook verantwoordelijk zijn. Hij zal worden betrokken bij de evaluaties en de keuzes van de uitgevoerde veiligheidsmaatregelen (zie o.a. artikel 5). De DPO zal uiteraard ter plaatse lokale toegang hebben tot de technische informatie en andere procedures die worden gebruikt om deze adviezen op dit gebied uit te brengen.

In overeenstemming met de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens zal het auditverslag worden toegezonden aan het Controleorgaan op de politionele informatie, dat zelf ook die maatregelen en technische normen kan evalueren.

Het is toegestaan om beroep te doen op een verwerker. In dat geval zijn alle veiligheidsmaatregelen en technische normen eveneens van toepassing, evenals de verplichting zich aan een audit te onderwerpen (artikel 11).

4. COMMENTAAR BIJ HOOFDSTUK III

Artikel 12

Een elektronische handtekening is in wezen iets heel anders dan een traditionele, met de hand geplaatste handtekening. In het 'handtekeningenvenster' wordt zij weergegeven als een reeks cijfers en letters die gelinkt is aan een bestand en de persoon van wie de handtekening afkomstig is.

Het toevoegen van een visueel element is op zichzelf juridisch of technisch gezien dus niet een noodzakelijk element, maar het is wel een van de factoren die het vertrouwen in en de aanvaardbaarheid van de elektronische handtekening helpen vergroten.

Dit element zal beslist nuttig blijven in een gematerialiseerde omgeving, voor zover de automatisering niet 'end to end' wordt toegepast en er papieren verwerking van dossiers blijft plaatsvinden.

In een **gematerialiseerde omgeving** (gedrukt PV) en dus op papier zal het dus belangrijk zijn om duidelijk aan te geven dat het PV elektronisch ondertekend is, en de voor- en achternaam van de ondertekenaar(s) te vermelden voor de gekwalificeerde handtekening en de contactgegevens van de rechtspersoon die ondertekent in geval van ondertekening door middel van een geavanceerd elektronisch zegel. In het laatste geval wordt/worden de naam/namen van de verbalisant(en) automatisch in de hoofdtekst van het proces-verbaal opgenomen.

Het zichtbaar maken van een digitale handtekening (gekwalificeerde elektronische handtekening en geavanceerd elektronisch zegel) **op een scherm** is uiteraard afhankelijk van leesprogramma's.

De diverse programma's hebben echter ten minste gemeen dat zij de informatie m.b.t. de ondertekenaar (de naam en voornaam van de fysieke persoon in geval van de gekwalificeerde handtekening en de gegevens van de rechtspersoon in geval van de ondertekening met het zegel - in het laatste geval wordt/worden de naam/namen van de verbalisant(en) automatisch in de hoofdtekst van het poces-verbaal opgenomen.) weergeven, informatie verstrekken over de geldigheid van het handtekeningcertificaat (geavanceerd elektronisch zegel of gekwalificeerde elektronische handtekening) en dat zij de datum vermelden van de elektronische ondertekening van de processenverbaal.

Dans les hypothèses où la sécurité ou l'intégrité des membres du personnel sont en jeu et où le législateur a déjà décidé que l'identification du verbalisateur n'était dès lors pas requise (par exemple pour les procès-verbaux visés à l'article 41, § 2, de la loi sur la fonction de police, ainsi que ceux visés aux articles 112*quater* et 112*quinquies* du Code d'instruction criminelle), la mention de ses nom et prénom sera remplacée par un numéro unique attribué au signataire. Il s'agit soit du numéro visé à l'article 41, § 2 de la loi sur la fonction de police ou celui visé à l'article 112*quater* du Code d'instruction criminelle. Bien entendu, cela ne s'applique pas à la signature qualifiée.

Le cas échéant, d'autres mesures de protection de l'identité peuvent bien entendu être appliquées pour protéger l'anonymat du verbalisateur, comme par exemple la signature du procès-verbal par le chef de service lorsque ces mesures sont préconisées par l'autorité judiciaire.

Dans ce cas, l'exception prévue par l'article 40, § 3, 1° ne joue pas et les règles génériques en matière de signature des procès-verbaux sont d'application.

J'ai l'honneur d'être,

Sire,
de Votre Majesté,
le très respectueux
et très fidèle serviteur,

Le Ministre de la Justice,
V. VAN QUICKENBORNE

La Ministre de l'Intérieur
A. VERLINDEN

---

18 JUILLET 2021. — Arrêté royal relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la Loi du 5 août 1992 sur la fonction de police, l'article 40, § 3, alinéa 4, modifié par la Loi du 25 mai 2018 ;

Vu l'avis n° DA 190008 de l'Organe de contrôle de l'information policière rendu le 11 avril 2019 ;

Vu les avis des Inspecteurs généraux des Finances, donnés les 19 et le 20 avril 2019 ;

Vu l'accord du ministre du Budget, donné le 21 juin 2019 ;

Vu l'avis 66.584/2 du Conseil d'Etat, donné le 14 octobre 2019, en application de l'article 84, §1, alinéa 1er, 2°, des lois coordonnées sur le Conseil d'Etat ;

Considérant 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 ;

Considérant la Loi du 21 juillet 2016 mettant en œuvre et complétant 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, portant insertion du titre 2 dans le livre XII "Droit de l'économie électronique" du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique ;

Sur la proposition des ministres de la Justice et de l'Intérieur,

Nous avons arrêté et arrêtons :

CHAPITRE Ier. - *DEFINITIONS*

Article 1er. Pour l'exécution du présent arrêté, on entend par :

1° « Règlement eIDAS » : 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 ;

In het geval dat de veiligheid of de integriteit van medewerkers in het geding zijn en de wetgever al beslist heeft dat identificatie van de verbalisant derhalve niet vereist was (bijvoorbeeld in processen-verbaal zoals bedoeld in artikel 41, § 2 van de wet op het politieambt en zoals bedoeld in artikel 112*quater* en 112*quinquies*), zal de vermelding van de voor- en achternaam worden vervangen door een uniek nummer dat aan de ondertekenaar toegewezen is. Het betreft ofwel het nummer zoals bedoeld in artikel 41, § 2 van de wet op het politieambt of het nummer zoals bedoeld in artikel 112*quater* van het wetboek van strafvordering. Dit geldt uiteraard niet wanneer er getekend wordt met de gekwalificeerde handtekening.

Uiteraard kunnen in voorkomend geval andere identiteitsbeschermende maatregelen worden toegepast om de anonimiteit van de verbalisant te beschermen, zoals bijvoorbeeld ondertekening van het proces-verbaal door het hoofd van dienst als deze maatregelen aanbevolen worden door de gerechtelijke autoriteit.

In dat geval speelt de uitzondering in artikel 40, § 3, 1° niet en zijn de algemene regels met betrekking tot de ondertekening van processen-verbaal van toepassing

Ik heb de eer te zijn,

Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaar,

De Minister van Justitie,
V. VAN QUICKENBORNE

De Minister van Binnenlandse Zaken,
A. VERLINDEN

---

18 JULI 2021. — Koninklijk besluit inzake de veiligheidsmaatregelen en de minimale technische normen voor politie-informaticasystemen die het geavanceerd elektronisch zegel produceren en inzake de vermeldingen die voorkomen in het geavanceerd elektronisch zegel en in de gekwalificeerde elektronische handtekening

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Overwegende de Wet van 5 augustus 1992 op het politieambt, artikel 40 § 3, alinea 4, gewijzigd bij de Wet van 25 mei 2018;

Gelet op advies nr. DA 190008 van het Controleorgaan op de politionele informatie, gegeven op 11 april 2019;

Gelet op de adviezen van de Inspecteurs-generaal van de Financiën, gegeven op 19 en 20 april 2019;

Gelet op het akkoord van de Minister van Begroting, gegeven op 21 juni 2019;

Gelet op het advies 66.584/2 van de Raad van State, gegeven op 14 oktober 2019, met toepassing van artikel 84, § 1, eerste lid, 2°, van de gecoördineerde wetten op de Raad van State;

Overwegende Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG;

Overwegende de Wet van 21 juli 2016 tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, houdende invoeging van titel 2 in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan titel 2 van boek XII en van de rechtshandhavingsbepalingen eigen aan titel 2 van boek XII, in de boeken I, XV en XVII van het Wetboek van economisch recht;

Op de voordracht van de Ministers van Justitie en Binnenlandse Zaken,

Hebben Wij besloten en besluiten Wij :

HOOFDSTUK I. - *DEFINITIES*

Artikel 1. Voor de toepassing van dit besluit gelden de volgende definities :

1° « eIDAS-verordening » : de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG;

2° « signature électronique qualifiée » : la signature visée à l'article 3.12 du Règlement eIDAS ;

3° « cachet électronique avancé » : le cachet visé à l'article 3.26 du Règlement eIDAS ;

4° « service de signature de la police » (Police Signing Service) : le service informatique de la police qui produit le cachet électronique avancé, ainsi que les mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée ;

5° « coordonnées de la personne morale »: pour la police locale et la police fédérale, leur numéro d'entreprise respectif auprès de la Banque Carrefour des Entreprises ;

6° « authentification forte » : une authentification des membres du personnel des services de police dont l'identité est préalablement vérifiée dans le registre national des personnes physiques et dont les fonctions sont précisées et tenues à jour dans un registre interne aux services de police, et reposant sur l'utilisation de deux éléments : un élément "connaissance" (quelque chose que seul le membre du personnel connaît) et un élément "possession" (quelque chose que seul le membre du personnel possède) ;

7° « procès-verbal » : le corps du procès-verbal et, le cas échéant, ses annexes ;

8° « données relatives à l'identification du créateur du cachet avancé » : Geïntegreerde Politie - Police Intégrée - Integrierte Polizei, BE, OrganizationIdentifier : PSDBE-NTRBE-0869909460, Mail : dri.services@police.belgium.eu, Téléphone : +32 2 554 40 00 ;

9° clé privée et clé publique : les clés utilisées dans la cryptographie asymétrique qui servent à chiffrer et déchiffrer les données.

CHAPITRE II. – *MESURES DE SECURITE ET NORMES TECHNIQUES MINIMALES DES SYSTEMES POLICIERS QUI PRODUISENT LE CACHET ELECTRONIQUE AVANCE*

Art. 2. Le service de signature de la police est intégré dans un environnement informatique comprenant :

a) un antimalware et un antivirus à jour ;

b) un système de détection et de blocage des intrusions ou des accès non autorisés ;

c) une procédure de mise à jour des logiciels ;

d) une gestion des incidents, y compris leur communication ;

e) des procédures de back-up et de continuité des activités.

Art. 3. Afin d'assurer l'intégrité des données, le service de signature de la police utilise une fonction de condensation des procès-verbaux.

La fonction de condensation permet d'assurer que le procès-verbal est associé à un seul condensé.

L'algorithme de condensation sécurisé doit être au moins un « Secure Hash Algorithm 256 ».

L'algorithme est calculé sur la base du contenu du procès-verbal signé électroniquement ayant fait l'objet de la condensation de sorte que sur la base d'une condensation déterminée, il n'y ait qu'un seul code de condensation qui corresponde à un contenu déterminé.

Si le contenu d'un procès-verbal signé électroniquement par cachet avancé est modifié, le code de condensation est différent.

Le code de condensation original permet également de déterminer si le procès-verbal signé électroniquement a été modifié.

Art. 4. Le service de signature de la police utilise un mécanisme de chiffrement du condensé du procès-verbal basé sur l'emploi d'une clé privée et d'un certificat électronique.

La vérification de l'identité du créateur du cachet est réalisée en ouvrant un procès-verbal signé par cachet avancé à l'aide du programme qui visualise le procès-verbal et qui utilise la clé publique associée à la clé privée pour déchiffrer les informations de signature électronique.

La validité du procès-verbal et de la signature peut être vérifiée au moyen d'un certificat de clé publique mis à disposition en ligne par la police intégrée, de sorte que ce certificat puisse être importé sur un appareil afin qu'il soit identifié comme un certificat de confiance lorsqu'il est utilisé pour une vérification ultérieure de l'identité.

2° « gekwalificeerde elektronische handtekening » : de handtekening zoals bedoeld in artikel 3.12 van de eIDAS-verordening;

3° « geavanceerd elektronisch zegel » : het zegel zoals bedoeld in artikel 3.26 van de eIDAS-verordening;

4° « handtekeningendienst van de politie » (Police Signing Service) : de informaticadienst van de politie die het geavanceerd elektronisch zegel vervaardigt, alsmede de vermeldingen die in het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening voorkomen;

5° « gegevens van de rechtspersoon » : voor de lokale politie en de federale politie, hun ondernemingsnummer bij de Kruispuntbank van Ondernemingen;

6° « sterke authenticatie » : een authenticatie van de personeelsleden van de politiediensten waarvan de identiteit vooraf is geverifieerd in het rijksregister van natuurlijke personen en waarvan de functies zijn omschreven en worden bijgehouden in een intern register van de politiediensten en dat gebaseerd is op het gebruik van twee elementen : een "kennis"-element (iets dat alleen het personeelslid weet) en een "bezit"-element (iets dat alleen het personeelslid bezit);

7° « proces-verbaal » : de hoofdtekst van het proces-verbaal en, in voorkomend geval, de bijlagen;

8° « gegevens met betrekking tot de identificatie van de maker van het geavanceerd zegel » : Geïntegreerde Politie - Police Intégrée - Integrierte Polizei, BE, OrganizationIdentifier : PSDBE-NTRBE-0869909460, Mail : dri.services@police.belgium.eu, Telefoon : +32 2 554 40 00;

9° private sleutel en publieke sleutel : de sleutels die worden gebruikt bij asymmetrische cryptografie en die dienen om gegevens te versleutelen en te ontsleutelen.

HOOFDSTUK II. – *VEILIGHEIDSMAATREGELEN EN MINIMALE TECHNISCHE NORMEN VOOR POLITIE-INFORMATICASYSTEMEN DIE HET GEAVANCEERD ELEKTRONISCH ZEGEL PRODUCEREN*

Art. 2. De handtekeningendienst van de politie is ingebed in een omgeving die het volgende bevat :

a) een up-to-date antimalware en antivirus;

b) een systeem voor het opsporen en tegenhouden van binnendringing of ongeoorloofde toegangen;

c) een procedure voor het bijwerken van de software;

d) een beheer van de incidenten, met inbegrip van de mededeling;

e) procedures voor back-up en bedrijfscontinuïteit.

Art. 3. Teneinde de integriteit van de gegevens te waarborgen, maakt de handtekeningendienst van de politie gebruik van een functie voor het comprimeren van processen-verbaal.

De comprimeringsfunctie zorgt ervoor dat het proces-verbaal wordt verbonden aan één enkele gecomprimeerde versie.

Het algoritme van beveiligde comprimering moet ten minste een "Secure Hash Algorithm 256" zijn.

Het algoritme wordt berekend op basis van de inhoud van het elektronisch ondertekende proces-verbaal dat is gecomprimeerd, zodat er, op basis van een gegeven comprimering, slechts één comprimeringscode is die overeenkomt met een gegeven inhoud.

Indien de inhoud van een elektronisch ondertekend proces-verbaal met geavanceerd zegel wordt gewijzigd, is de comprimeringscode anders.

De oorspronkelijke comprimeringscode laat ook toe om te bepalen of het elektronisch ondertekend proces-verbaal is gewijzigd.

Art. 4. De handtekeningendienst van de politie gebruikt een mechanisme om de comprimering van het proces-verbaal te versleutelen gebaseerd op het gebruik van een privésleutel en een elektronisch certificaat.

De identiteit van de maker van het zegel wordt geverifieerd door een ondertekend proces-verbaal met een geavanceerd zegel te openen met behulp van het programma dat het proces-verbaal bekijkt en de openbare sleutel gebruikt die aan de privésleutel is gekoppeld om de gegevens van de elektronische handtekening te ontcijferen.

De geldigheid van het proces-verbaal en de handtekening kan geverifieerd worden aan de hand van een publieke sleutel certificaat dat online ter beschikking gesteld wordt door de geïntegreerde politie, zodat het certificaat kan geïmporteerd worden op een toestel en het geïdentificeerd wordt als een vertrouwd certificaat wanneer het wordt gebruikt voor een daaropvolgende identiteitsverificatie.

Ce certificat de clé publique comprend notamment les données relatives à l'identification du créateur du cachet avancé (« DRI integrated police »), la clé publique ainsi que la durée de validité.

Art. 5. Le stockage et la gestion des certificats de signature électronique valides, expirés ou périmés sont réalisés par la direction de l'information policière et des moyens ICT de la police fédérale, après avis du délégué à la protection des données désigné auprès du Commissariat général.

Les clés privées sont sécurisées de manière adéquate dans l'infrastructure informatique et les bâtiments de la police intégrée, tant durant leur stockage que pendant leur utilisation.

Art. 6. Le service de signature de la police utilise un mécanisme d'horodatage. Ce mécanisme est associé à chaque signature par cachet.

Art. 7. Le service de signature électronique de la police n'est accessible à des fins de signature que pour les membres des services de police s'étant préalablement :

a) identifiés avec un identifiant unique en fonction d'un profil d'accès spécifique et

b) authentifiés à l'aide d'un moyen d'authentification forte.

Art. 8. Les traitements réalisés à l'aide de ce service font l'objet d'une journalisation au sens de l'article 56 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel qui est conservée 5 ans après la destruction du procès-verbal. Cette journalisation permet notamment de réaliser un traçage de toute création, modification ou destruction du procès-verbal, signé par cachet avancé.

Art. 9. Lors de l'utilisation du service de signature de la police dans le cadre de l'article 40, § 3 de la loi sur la fonction de police, le cachet électronique avancé est apposé par le membre du personnel qui utilise le cachet avancé uniquement lors d'un processus humain volontaire et ne peut pas être apposé inopinément.

Cette apposition est reprise dans la journalisation de sorte que le moment d'apposition, la personne qui a demandé cette apposition et les procès-verbaux signés puissent être contrôlés.

Lors de l'utilisation du service de signature de la police dans le cadre de l'article 40, § 6 de la loi sur la fonction de police, le cachet électronique avancé est apposé lors d'un processus automatique maîtrisé et le cachet ne peut pas être apposé inopinément.

Art. 10. Les mesures de sécurité et les normes techniques permettant d'assurer un niveau de confidentialité, de disponibilité, d'intégrité, de fiabilité, d'authenticité et d'irréfutabilité du service de signature électronique de la police sont auditées au minimum tous les 5 ans.

Le rapport d'audit détaille les 15 paramètres repris dans l'annexe 1.

Le Commissariat général de la police fédérale réalise ces audits.

Le premier audit a lieu au plus tard 12 mois après la parution de cet arrêté royal. Le rapport d'audit est transmis à l'Organe de contrôle de l'information policière.

Art. 11. En cas de traitement par un sous-traitant, les mesures de sécurité et normes techniques reprises au chapitre II du présent arrêté sont contractuellement applicables au sous-traitant. Les traitements qui sont réalisés par un sous-traitant font également l'objet de l'audit prévu à l'article 10.

CHAPITRE III. - *Mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée*

Art. 12. §1er. Quand un procès-verbal est signé avec le cachet électronique avancé ou la signature électronique qualifiée, les mentions suivantes sont visualisées dans un environnement matérialisé :

a) « signé électroniquement », dans la langue de rédaction du procès-verbal ;

b) les données d'identification du ou des signataire(s) en cas de signature électronique qualifiée et les coordonnées de la personne morale qui signe en cas de signature par cachet électronique avancé.

Dit publieke sleutel certificaat bevat met name gegevens met betrekking tot de identificatie van de maker van het geavanceerd zegel ("DRI integrated police"), de publieke sleutel en de geldigheidsduur.

Art. 5. Het bewaren en beheren van geldige, verlopen of verouderde certificaten voor elektronische handtekeningen wordt uitgevoerd door de directie van de politionele informatie en de ICT-middelen van de federale politie, na advies van de bij het Commissariaat-generaal aangewezen functionaris voor gegevensbescherming.

De private sleutels worden zowel bij opslag als bij gebruik op een adequate wijze beveiligd in de IT-infrastructuur en in de gebouwen van de geïntegreerde politie.

Art. 6. De handtekeningendienst van de politie maakt gebruik van een tijdstempelmechanisme. Dit mechanisme wordt aan elke handtekening gekoppeld door middel van een stempel.

Art. 7. De handtekeningendienst van de politie is enkel toegankelijk voor ondertekeningsdoeleinden voor de leden van de politiediensten die op voorhand :

a) geïdentificeerd zijn met een unieke identificatiecode op basis van een bepaald toegangsprofiel en

b) zich hebben geauthentificeerd met een sterke authenticatie.

Art. 8. De verwerkingen die met behulp van deze dienst worden uitgevoerd maken het voorwerp uit van een logbestand in de zin van artikel 56 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, dat tot 5 jaar na de vernietiging van het proces-verbaal, wordt bewaard. Dit logbestand maakt het met name mogelijk elke creatie, wijziging of vernietiging te traceren van het proces-verbaal, dat is ondertekend met een geavanceerd zegel.

Art. 9. Bij het gebruik van de handtekeningendienst van de politie in het kader van artikel 40, §3 van de wet op het politieambt, wordt het geavanceerd elektronisch zegel slechts door het personeelslid dat het geavanceerde zegel gebruikt, ingevolge een bewust menselijk proces en mag niet onverwachts worden aangebracht.

Deze aanbrenging wordt in het logbestand hernomen, zodat het tijdstip van deze aanbrenging, de persoon die deze aanbrenging heeft gedaan en de ondertekende processen-verbaal kunnen worden gecontroleerd.

Bij gebruikmaking van de handtekeningendienst van de politie in het kader van artikel 40, § 6 van de wet op het politieambt, wordt het geavanceerd elektronisch zegel in een gecontroleerd automatisch proces aangebracht en kan het zegel niet onverwachts worden aangebracht.

Art. 10. De veiligheidsmaatregelen en de technische normen die het mogelijk maken een niveau van vertrouwelijkheid, beschikbaarheid, integriteit, betrouwbaarheid, authenticiteit en onweerlegbaarheid van de elektronische handtekeningendienst van de politie te waarborgen, worden minstens om de 5 jaar geauditeerd.

In het auditrapport wordt nader ingegaan op de 15 in bijlage 1 genoemde parameters.

Het Commissariaat-generaal van de federale politie voert deze audits uit.

De eerste audit vindt plaats ten laatste 12 maanden na de publicatie van dit koninklijk besluit. Het auditrapport wordt verstuurd naar het Controleorgaan op de politionele informatie.

Art. 11. In geval van verwerking door een verwerker zijn de veiligheidsmaatregelen en technische normen onder hoofdstuk II van dit besluit contractueel van toepassing op de verwerker. De door een verwerker uit te voeren verwerkingen, maken eveneens het voorwerp uit van de audit voorzien in artikel 10.

HOOFDSTUK III. - *Vermeldingen in het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening*

Art. 12. § 1. Wanneer een proces-verbaal, getekend wordt met het geavanceerd elektronisch zegel of de gekwalificeerde elektronische handtekening, worden de volgende vermeldingen in een gematerialiseerde omgeving gevisualiseerd :

a) « elektronisch ondertekend », in de taal waarin het proces-verbaal is opgesteld;

b) de identificatiegegevens van de ondertekenaar(s) in geval van gekwalificeerde elektronische handtekening en de gegevens van de rechtspersoon die ondertekent in geval van ondertekening door middel van een geavanceerd elektronisch zegel.

§ 2. Quand un procès-verbal est signé avec le cachet électronique avancé ou la signature électronique qualifiée, au minimum, les mentions suivantes sont visualisées dans un environnement dématérialisé :

1° les données d'identification du ou des signataire(s) en cas de signature électronique qualifiée et les coordonnées de la personne morale qui signe en cas de signature par cachet électronique avancé ;

2° les mentions relatives à la validité du certificat de cachet électronique avancé ou de signature électronique qualifiée ;

3° la date de la signature électronique du procès-verbal.

§ 3. Les mentions visées aux §§ 1er et 2 sont créées au moment de l'utilisation du cachet électronique avancé ou de la signature électronique qualifiée.

Art. 13. Le Ministre qui a l'Intérieur dans ses attributions et le Ministre qui a la Justice dans ses attributions sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Donné à Bruxelles, le 18 juillet 2021.

PHILIPPE

Par le Roi :

Le Ministre de la Justice
V. VAN QUICKENBORNE

La Ministre de l'Intérieur
A.VERLINDEN

§ 2. Wanneer een proces-verbaal, getekend wordt met het geavanceerd elektronisch zegel of de gekwalificeerde elektronische handtekening, worden minstens de volgende vermeldingen gevisualiseerd in een gedematerialiseerde omgeving :

1° de identificatiegegevens van de ondertekenaar(s) in geval van gekwalificeerde elektronische handtekening en de gegevens van de rechtspersoon die ondertekent in geval van ondertekening door middel van een geavanceerd elektronisch zegel;

2° de vermeldingen met betrekking tot de geldigheid van het certificaat voor een geavanceerd elektronisch zegel of van een gekwalificeerde elektronische handtekening;

3° de datum van de elektronische ondertekening van het procesverbaal.

§ 3. De vermeldingen bedoeld in de § § 1 en 2 worden gecreëerd op het tijdstip van het gebruik van het geavanceerd elektronisch zegel of van de gekwalificeerde elektronische handtekening.

Art. 13. De Minister bevoegd voor Binnenlandse Zaken en de Minister bevoegd voor Justitie zijn, ieder wat zijn bevoegdheden betreft, belast met de uitvoering van dit besluit.

Gegeven te Brussel, op 18 juli 2021.

FILIP

Van Koningswege :

De Minister van Justitie,
V. VAN QUICKENBORNE

De Minister van Binnenlandse Zaken,
A.VERLINDEN

Annexe à l'arrêté royal du 18 juillet 2021 relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée

L'audit des mesures de sécurité et des normes techniques permettant d'assurer un niveau de confidentialité, de disponibilité, d'intégrité, de fiabilité, d'authenticité, d'irréfutabilité du service de signature électronique de la police (Police Signing Service) porte sur les 15 paramètres suivants :

1) La politique de sécurité de l'information et les plans de sécurité concernant le Police Signing Service, c'est-à-dire :

a) la stratégie des services de police ;

b) les réglementations, la législation et les contrats ;

c) l'environnement réel et anticipé des menaces liées à la sécurité de l'information.

2) L'organisation de la sécurité relative au Police Signing Service, c'est-à-dire :

a) l'identification des rôles et responsabilités des différents acteurs concernés par la sécurité de l'information ;

b) les données relatives au délégué à la protection des données compétent pour la mise en oeuvre et le suivi des mesures de sécurité ;

c) l'identification des membres du personnel et les tiers opérant sous la responsabilité de la police ;

d) le contrôle d'accès / la gestion des autorisations ;

e) le retrait des droits ;

f) la confidentialité des données ;

g) l'accès physique aux bâtiments et aux infrastructures ;

h) les systèmes d'accès et la confidentialité des données d'accès ;

i) les mesures permettant de déterminer l'utilisation correcte des outils de travail mis à disposition (tels que les appareils mobiles) ;

j) les mesures qui sont prises pour contrôler les activités (accès, destruction de stockage, accès à distance, journalisation) ;

k) la gestion des certificats et des clés.

Bijlage aan het koninklijk besluit van 18 juli 2021 inzake de veiligheidsmaatregelen en de minimale technische normen voor politie-informaticasystemen die het geavanceerd elektronisch zegel produceren en inzake de vermeldingen die voorkomen in het geavanceerd elektronisch zegel en in de gekwalificeerde elektronische handtekening

De audit van de veiligheidsmaatregelen en de technische normen die het mogelijk maken een niveau van vertrouwelijkheid, beschikbaarheid, integriteit, betrouwbaarheid, authenticiteit en onweerlegbaarheid van de elektronische handtekeningendienst van de politie (Police Signing Service) heeft betrekking op de 15 volgende parameters :

1) Het informatieveiligheidsbeleid en beveiligingsplannen betreffende de Police Signing Service, dit wil zeggen :

a) de strategie van de politiediensten;

b) de regelgeving, wetgeving en contracten;

c) de huidige en de verwachte omgeving van bedreigingen voor de informatieveiligheid.

2) De organisatie van de beveiliging betreffende de Police Signing Service, dit wil zeggen :

a) de identificatie van de rollen en de verantwoordelijkheden van de verschillende actoren betrokken bij informatieveiligheid;

b) gegevens betreffende de functionaris voor gegevensbescherming die bevoegd is voor de uitvoering van en het toezicht op de beveiligingsmaatregelen;

c) de identificatie van personeelsleden en derden die onder de verantwoordelijkheid van de politie optreden;

d) de toegangscontrole / het autorisatiebeheer;

e) de intrekking van rechten;

f) de vertrouwelijkheid van gegevens;

g) de fysieke toegang tot gebouwen en infrastructuur;

h) de toegangssystemen en vertrouwelijkheid van toegangsgegevens;

i) de maatregelen om het juiste gebruik te bepalen van werkinstrumenten die ter beschikking gesteld worden (zoals mobiele apparaten);

j) de maatregelen die genomen worden om de activiteiten te controleren (toegang, vernietiging van opslag, toegang op afstand, logbestanden);

k) het beheer van de certificaten en de sleutels.

3) La sécurité concernant les ressources humaines, c'est-à-dire que :

a) seuls des membres du personnel et, le cas échéant, des sous-traitants qui possèdent l'expertise, la fiabilité, l'expérience et les qualifications nécessaires et qui ont reçu une formation appropriée en ce qui concerne les règles en matière de sécurité seront employés pour mettre en œuvre le Police Signing Service.

b) les modalités visant à l'adhésion de tous les collaborateurs internes et externes aux instructions internes de l'organisation doivent être documentées et connues ;

c) les responsabilités et les obligations relatives à la sécurité de l'information et à la protection des données demeurent après la résiliation ou le changement d'emploi et que ces conditions doivent être clairement communiquées et intégrées dans le processus de gestion des collaborateurs (internes ou externes) ;

d) un contrat de confidentialité est conclu avec toute personne, non soumise au statut des membres de la police intégrée, ayant accès aux systèmes d'information des services de police.

4) La sensibilisation et la formation des membres du personnel et des collaborateurs externes.

Un programme de sensibilisation/formation est mis en place afin :

a) de conscientiser les membres du personnel et les collaborateurs externes à la sécurité de l'information et à la protection de la vie privée (en mettant l'accent sur le Police Signing Service) ;

b) d'expliquer clairement les responsabilités respectives de l'autorité hiérarchique, d'un service spécifique, du collaborateur et des personnes chargées du contrôle de l'application des mesures de sécurité en lien avec le Police Signing Service.

5) La gestion des actifs relatifs au Police Signing Service.

L'inventaire des actifs nécessaires au Police Signing Service, quels que soient leurs types (informations, données, applications, réseaux, processus, systèmes) est réalisé.

Chaque actif sera détaillé et tous les éléments seront repris et tenus à jour afin de bénéficier d'une cartographie correcte de l'architecture des systèmes et de l'information de l'organisation.

Un responsable fonctionnel est identifié pour chaque élément de cet inventaire et sa tâche est précisée dans le plan de sécurité concerné.

6) Le contrôle d'accès relatif au Police Signing Service.

Pour l'accès au Police Signing Service, les services de police définissent les règles d'accès dans des procédures spécifiques.

Un processus qui garantit l'identification et l'authentification forte du membre du personnel lorsque celui-ci souhaite exercer ses tâches est mis en place.

7) La protection des données à caractère personnel.

Les données à caractère personnel contenues dans les procès-verbaux, en ce compris la signature électronique, doivent être protégées de manière appropriée pendant leur utilisation, leur stockage, et leur transmission. Le niveau de protection tient compte de l'analyse de risque avec, selon les besoins, des mesures de pseudonymisation ou de chiffrement des données ou de l'information, ou toute autre mesure permettant de garantir le niveau de protection approprié.

8) La sécurité physique.

Les services de police sécurisent les infrastructures dans lesquelles le Police Signing Service est mis en œuvre. Ils prennent les mesures de protection et de sécurisation afin de gérer l'accès des personnes autorisées aux bâtiments et aux locaux.

Les mesures sont adaptées en fonction de la présence physique de personnes dans les locaux.

Les services de police protègent leurs données et leurs supports de données. Ils prennent des mesures préventives contre la perte, la divulgation non autorisée, la détérioration, le vol, l'accès non autorisé des actifs de l'organisation et contre une éventuelle interruption des activités de l'organisation.

3) De veiligheid inzake het personeelsbeheer, dit wil zeggen dat :

a) alleen personeelsleden en, in voorkomend geval, verwerkers ingezet die beschikken over de nodige deskundigheid, betrouwbaarheid, ervaring en kwalificaties en die een passende opleiding op het gebied van veiligheidsvoorschriften hebben gekregen zullen worden ingezet om de Police Signing Service uit te voeren.

b) modaliteiten die voorzien dat alle personeelsleden en externe medewerkers zich dienen te houden aan de interne instructies van de organisatie moeten gedocumenteerd zijn en bekend zijn;

c) verantwoordelijkheden en verplichtingen voor informatiebeveiliging en gegevensbescherming blijven bestaan na beëindiging of verandering van dienstverband en dat deze voorwaarden duidelijk moeten worden gecommuniceerd en geïntegreerd in het werknemersmanagementproces (intern of extern);

d) een vertrouwelijkheidsovereenkomst wordt met alle personen die toegang hebben tot de informatiesystemen van de politiediensten en die niet onderworpen zijn aan het statuut van de personeelsleden van de geïntegreerde politie afgesloten.

4) De sensibilisering en de opleiding van de personeelsleden en externe medewerkers betreffende de Police Signing Service.

Er wordt een sensibiliserings-/opleidingsprogramma opgezet om :

a) de personeelsleden en de externe medewerkers bewust te maken van de informatieveiligheid en de bescherming van het privéleven (met focus op de Police Signing Service);

b) duidelijk uit te leggen welke de verantwoordelijkheden zijn van de hiërarchische overheid, van een specifieke dienst, van de medewerker en van de personen belast met de controle van de toepassing van de veiligheidsmaatregelen in verband met de Police Signing Service.

5) Het beheer van de activa gelinkt aan de Police Signing Service.

De inventaris wordt opgemaakt van de voor de Police Signing Service noodzakelijke activa, ongeacht de categorie ervan (informatie, gegevens, applicaties, netwerken, processen, systemen).

Alle activa dienen in detail beschreven te worden en alle elementen ervan worden bijgehouden en geactualiseerd om zodoende te beschikken over een correct beeld van de informatie- en systeemarchitectuur van de organisatie.

Een functionele verantwoordelijke wordt geïdentificeerd voor elk element van deze inventaris en in het betrokken beveiligingsplan wordt zijn taak duidelijk omschreven.

6) De toegangscontrole betreffende de Police Signing Service.

Voor de toegang tot de Police Signing Service bepalen de politiediensten de toegangsregels in specifieke procedures.

Er wordt een proces voorzien dat de identificatie en sterke authenticatie van het personeelslid waarborgt wanneer deze zijn of haar taken wenst uit te oefenen.

7) De bescherming van de persoonsgegevens.

De in de processen-verbalen opgenomen persoonsgegevens met inbegrip van de elektronische handtekening moeten tijdens hun gebruik, hun opslag en hun overdracht adequaat worden beschermd. Het beschermingsniveau houdt rekening met de risicoanalyse en, indien nodig, worden pseudonimiserings- of versleutelingsmaatregelen voor de gegevens of informatie of elke andere maatregel die een passend beschermingsniveau waarborgt genomen.

8) De fysieke veiligheid.

De politiediensten beveiligen de infrastructuur waarin de Police Signing Service wordt uitgevoerd. Zij nemen de beschermings- en beveiligingsmaatregelen om de toegangen te beheren van de personen die de gebouwen en lokalen mogen betreden.

De maatregelen worden aangepast in functie van de fysieke aanwezigheid van personen in de lokalen.

De politiediensten beschermen hun gegevens en hun gegevensdragers. Zij nemen preventieve maatregelen tegen verlies, ongeoorloofde verstrekking beschadiging, diefstal, de ongeoorloofde toegang tot de activa van de organisatie en tegen een eventuele onderbreking van de activiteiten van de organisatie.

9) La sécurité opérationnelle.

Les services de police mettent en œuvre des mesures spécifiques pour chaque actif essentiel du Police Signing Service : tout acte suspect ou tout incident est rapporté et investigué. Une trace du suivi de ces incidents est également conservée. Les systèmes et les produits mis en œuvre pour le Police Signing Service sont fiables et protégés contre les modifications. La sécurité technique et la fiabilité des processus sont prises en charge.

10) La sécurité de la communication des informations.

Les services de police prennent des mesures spécifiques pour sécuriser la communication de l'information, afin d'éviter les accès non autorisés aux données et informations.

11) L'acquisition, le développement et la maintenance des systèmes d'information.

Lors de l'achat, du développement et de la maintenance du Police Signing Service, les services de police conçoivent et utilisent des processus et des procédures pour protéger les informations et ce, aussi bien pendant la phase de son développement que lors de son utilisation opérationnelle.

Le Police Signing Service et les processus de traitement de données sont développés et conçus pour protéger par défaut les données et informations.

12) Les relations avec les tiers (fournisseurs, autorités).

Les services de police définissent les relations avec les fournisseurs et les autorités pour mettre en œuvre le Police Signing Service.

Ces relations sont formalisées dans un document qui indique clairement, le cas échéant :

a) qui est (sont) le(s) responsable(s) du traitement ;

b) quelle partie est le sous-traitant ;

c) comment les responsabilités sont réparties ;

d) comment la protection des données est organisée, y compris :

- o la sécurité et le comportement requis ;
- o la gestion des incidents ;
- o le signalement des violations ;
- o le contact avec les autorités.

13) La gestion des incidents liés à la sécurité de l'information.

Les membres du personnel ainsi que les collaborateurs externes et d'autres personnes impliquées dans le Police Signing Service disposent d'une procédure permettant de signaler les activités suspectes.

Il s'agit d'une procédure permettant de rapporter, d'enregistrer et de gérer des violations potentielles ou présumées de données à caractère personnel ou de la sécurité du Police Signing Service afin que les vulnérabilités puissent être traitées rapidement et de manière structurée.

Cette procédure reprendra : les rôles et les responsabilités de tous les acteurs impliqués.

Un registre interne des incidents contenant tous les incidents de sécurité signalés sera tenu à jour.

14) Les aspects de la gestion de la continuité des activités liés à la sécurité de l'information.

Le Police Signing Service fait l'objet d'un plan de protection garantissant la disponibilité des données et de l'information.

Les mesures permettent de prévoir la protection nécessaire de l'information et des données qui sont traitées dans le système contre la perte, la modification ou la destruction non autorisée, soit par accident soit par acte malveillant.

Les services de police veillent à ce que la disponibilité et l'accès à des informations ou à des données soient rétablis en temps utile après un incident physique ou technique.

Les services de police prévoient une solution afin d'assurer la continuité du Police Signing Service. Dans cette solution, les codes de développement des applications seront au maximum conservés.

15) L'évaluation des points 1 à 14 est réalisée au moins en fonction :

a) des changements dans les menaces et des leçons tirées suite à la gestion d'incidents ;

b) des résultats d'analyses de risques, d'enquêtes de contrôle ou d'audits ;

c) de changements de l'organisation ou du contexte juridique, réglementaire ou technologique.

9) De operationele veiligheid.

De politiediensten nemen voor alle essentiële activa van de Police Signing Service afzonderlijk specifieke maatregelen : elke verdachte handeling of elk incident wordt gemeld en onderzocht. Er wordt tevens een spoor bewaard van de opvolging van deze incidenten. De voor de Police Signing Service geïmplementeerde systemen en producten zijn betrouwbaar en beschermd tegen veranderingen. Er wordt gezorgd voor technische veiligheid en procesbetrouwbaarheid.

10) De beveiliging van de mededeling van de informatie.

De politiediensten nemen specifieke maatregelen om de mededeling van informatie te beveiligen, teneinde een ongeoorloofde toegang tot de gegevens en informatie te vermijden.

11) De aankoop, de ontwikkeling en het onderhoud van informatiesystemen.

De politiediensten dienen bij de aankoop, de ontwikkeling en het onderhoud van de Police Signing Service, processen en procedures op te stellen en te gebruiken om de informatie te beschermen, zowel in de ontwikkelingsfase als tijdens het operationeel gebruik ervan.

De Police Signing Service en de processen voor gegevensverwerking worden ontworpen en ontwikkeld om de gegevens en informatie door standaardinstellingen te beschermen.

12) De betrekkingen met derden (leveranciers, autoriteiten).

De politiediensten leggen de relaties met de leveranciers en de overheden vast om de Police Signing Service te realiseren.

Deze relaties worden geformaliseerd in een document, dat in voorkomend geval duidelijk aangeeft :

a) wie de verwerkingsverantwoordelijke(n) is (zijn);

b) welke partij de verwerker is;

c) hoe de verantwoordelijkheden worden verdeeld;

d) hoe de gegevensbescherming georganiseerd is, met inbegrip van :

- o de veiligheid en de vereiste houding;
- o het beheer van incidenten;
- o de melding van inbreuken;
- o het contact met de overheden.

13) Het Incident Management aangaande informatieveiligheid.

Zowel personeelsleden als externe medewerkers en andere betrokken personen betrokken bij de Police Signing Service beschikken over een procedure die het mogelijk maakt om verdachte activiteiten te rapporteren.

Het gaat om een procedure om mogelijke of vermoedelijke inbreuken in verband met persoonsgegevens of in verband met de veiligheid van de Police Signing Service te rapporteren, te registeren en te behandelen zodat kwetsbaarheden voortijdig en gestructureerd kunnen behandeld worden.

Deze procedure bevat de rollen en verantwoordelijkheden van alle betrokken actoren.

Een intern register waarin alle gemelde inbreuken op de beveiliging worden hernomen.

14) De informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer.

De Police Signing Service maakt deel uit van een beveiligingsplan dat de beschikbaarheid van de gegevens en de informatie garandeert.

De maatregelen laten toe te voorzien in de nodige bescherming van de informatie en de gegevens die in het systeem verwerkt worden tegen verlies, ongeoorloofde wijziging of vernietiging, hetzij per ongeluk hetzij door een moedwillige handeling.

De politiediensten zorgen ervoor dat de beschikbaarheid van en toegang tot de informatie en de gegevens na een fysiek of technisch incident tijdig kan hersteld worden.

De politiediensten voorzien een oplossing, teneinde de continuïteit van de Police Signing Service te verzekeren. In deze oplossing worden maximaal de ontwikkelcodes van de toepassingen bijgehouden.

15) De evaluatie van de punten 1 tot en met 14 wordt ten minste uitgevoerd in functie van :

a) veranderingen in bedreigingen en feedback als gevolg van incidentenbehandeling;

b) de resultaten van risicoanalyses, controleonderzoeken of audits;

d) veranderingen van de organisatie of van de juridische, regelgevende en technologische context.

Vu pour être annexé à Notre arrêté du 18 juillet 2021 relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée.

PHILIPPE

Par le Roi :

Le Ministre de la Justice,
V. VAN QUICKENBORNE

La Ministre de l'Intérieur,
A.VERLINDEN

Gezien om te worden gevoegd bij Ons besluit van 18 jumi 2021 inzake de veiligheidsmaatregelen en de minimale technische normen voor politie-informaticasystemen die het geavanceerd elektronisch zegel produceren en inzake de vermeldingen die voorkomen in het geavanceerd elektronisch zegel en in de gekwalificeerde elektronische handtekening.

FILIP

Van Koningswege :

De Minister van Justitie,
V. VAN QUICKENBORNE

De Minister van Binnenlandse Zaken,
A.VERLINDEN

SERVICE PUBLIC FEDERAL FINANCES

[C − 2021/31951]

5 AOUT 2021. — Arrêté du Président du Comité de direction fixant les travaux devant être considérés comme salissants au sens de l'article 5, alinéa 2, de l'arrêté ministériel du 12 avril 1965 relatif à l´octroi de certaines indemnités à divers agents du Service public fédéral Finances

Le Président du Comité de direction,

Vu l'arrêté ministériel du 12 avril 1965 relatif à l'octroi de certaines indemnités à divers agents du Service public fédéral Finances, l'article 5, alinéa 2, remplacé par l'arrêté ministériel du 12 novembre 2017 ;

Vu l'arrêté du Président du comité de direction du 14 juin 2018 fixant les travaux devant être considérés comme salissants au sens de l'article 5, alinéa 2, de l'arrêté ministériel du 12 avril 1965 relatif à l'octroi de certaines indemnités à divers agents du Service public fédéral Finances ;

Vu l'avis de l'Inspecteur des Finances, donné le 24 mai 2019 et 24 mars 2021;

Vu l'accord de la Ministre du Budget, donné le 15 juillet 2019 ;

Vu l'accord de la Secrétaire d'Etat au Budget, donné le 23 avril 2021 ;

Vu le protocole de négociation n°C.D. 337/D/117-118 du Comité de Secteur II – Finances, conclu le 14 juillet 2021,

Arrête :

Article 1er. En application de l'article 5, alinéa 2, de l'arrêté ministériel du 12 avril 1965 relatif à l'octroi de certaines indemnités à divers agents du Service public fédéral Finances, les travaux énumérés ci-après sont considérés comme étant des travaux salissants:

A. à l'Administration générale des douanes et accises :

1° la vérification, le contrôle et le recensement dans les entrepôts fiscaux d'huiles minérales ;

2° les constatations de rendement et recensement dans les usines de benzole ;

3° la surveillance de la remise en service du benzole ;

4° la vérification d'huile créosote ;

5° la vérification du diesel en cas de contrôle des véhicules sur la voie publique ;

6° les contrôles dans les raffineries de pétrole, les usines pétrochimiques, les sociétés d'avitaillement et les sociétés d'entreposage d'huile minérale, réalisés;

7° le traitement des marchandises abandonnées et des marchandises confisquées dans le cadre du chapitre XII d'une succursale ;

8° l'addition de produit d'identification à l'huile minérale ;

9° *a)* sur les navires commerciaux :

a.1. le contrôle de la chambre des machines ;

a.2. le contrôle des citernes à ballast en cas de présence éventuelle d'huiles minérales ;

a.3. le contrôle des installations sanitaires ;

FEDERALE OVERHEIDSDIENST FINANCIEN

[C − 2021/31951]

5 AUGUSTUS 2021. — Besluit van de Voorzitter van het Directiecomité tot vaststelling van de werkzaamheden die als bevuilend moeten worden beschouwd in de zin van artikel 5, tweede lid, van het ministerieel besluit van 12 april 1965 betreffende de toekenning van sommige vergoedingen aan verschillende personeelsleden van de Federale Overheidsdienst Financiën

De Voorzitter van het Directiecomité,

Gelet op het ministerieel besluit van 12 april 1965 betreffende de toekenning van sommige vergoedingen aan verschillende personeelsleden van de Federale Overheidsdienst Financiën, artikel 5, tweede lid, vervangen bij het ministerieel besluit van 12 november 2017;

Gelet op het besluit van de Voorzitter van het Directiecomité van 14 juni 2018 tot vaststelling van de werkzaamheden die als bevuilend moeten worden beschouwd in de zin van artikel 5, tweede lid, van het ministerieel besluit van 12 april 1965 betreffende de toekenning van sommige vergoedingen aan verschillende personeelsleden van de Federale Overheidsdienst Financiën;

Gelet op het advies van de Inspecteur van Financiën, gegeven op 24 mei 2019 en op 24 maart 2021;

Gelet op de akkoordbevinding van de Minister van Begroting, d.d. 15 juli 2019;

Gelet op de akkoordbevinding van de Staatssecretaris voor Begroting, d.d. 23 april 2021;

Gelet op het protocol van onderhandelingen nr. D.I. 337/D/117-118 van het Sectorcomité II – Financiën, gesloten op 14 juli 2021,

Besluit :

Artikel 1. In uitvoering van artikel 5, tweede lid, van het ministerieel besluit van 12 april 1965 betreffende de toekenning van sommige vergoedingen aan verschillende personeelsleden van de Federale Overheidsdienst Financiën, worden de hierna opgesomde werken als bevuilend beschouwd:

A. bij de Algemene Administratie van de Douane en Accijnzen:

1° de verificatie, de controle en de opneming in belastingentrepots voor minerale olie;

2° vaststellingen verrichten inzake opbrengstpercentages en verliezen in benzeentanken;

3° het toezicht op heringebruikname van benzeen;

4° de controle van creosoot;

5° de verificatie van diesel bij controles van voertuigen op de openbare weg;

6° controleactiviteiten uitgeoefend in petroleumraffinaderijen, petrochemische fabrieken, bunkerfirma's en opslagbedrijven van minerale olie;

7° behandeling van verlaten goederen en verbeurdverklaarde goederen in kapittel XII van een hulpkantoor;

8° het toevoegen van herkenningsmiddelen aan minerale olie;

9°*a)* op commerciële vaartuigen:

a.1. de controle van de machinekamer;

a.2. de controle van de ballasttanks op de eventuele aanwezigheid van minerale oliën;

a.3. de controle van de sanitaire installatie;