

KONINKRIJK BELGIË

ROYAUME DE BELGIQUE

FEDERALE OVERHEIDSDIENST
JUSTITIE

SERVICE PUBLIC JUSTICE

Voorontwerp van 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

Projet d'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.

Filip, Koning der Belgen,

Philippe, Roi des Belges,

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

A tous, présents et à venir, Salut.

Overwegende de wet van 5 augustus 1992 op het politieambt, artikel 40 gewijzigd bij de wet van 25 mei 2018;

Considérant la Loi du 5 août 1992 sur la fonction de police, l'article 40 modifié par la Loi du 25 mai 2018;

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;

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;

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;

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;

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

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

Gelet op het advies van de inspecteur-generaal van Financiën, gegeven op 19 april 2019;

Vu l'avis de l'inspecteur général des finances, donné le 19 avril 2019;

Gelet op de akkoordbevinding van de Vu l'accord du ministre du Budget, Minister van Begroting, d.d. XX Xx donné le XX Xx 2019;
2019;

Gelet op het advies (...) van de Raad Vu l'avis (.....) du Conseil d'Etat, van State, gegeven op XX Xx 2019, donné le XX Xx 2019, en application de met toepassing van artikel 84, § 1, l'article 84, §1, alinéa 1^{er}, 2°, des lois eerste lid, 2°, van de gecoördineerde coordonnées sur le Conseil d'Etat; wetten op de Raad van State;

Op de voordracht van de Minister van Sur la proposition du ministre de la Justitie, Justice;

Hebben Wij besloten en besluiten Nous avons arrêté et arrêtons :
Wij:

Art. 1. § 1. De veiligheidsmaatregelen en de technische normen inzake de productie van het geavanceerd elektronisch zegel bedoeld in artikel 40, § 3, van de wet van 5 augustus 1992 op het politieambt zijn gebaseerd op:
Art. 1. § 1^{er}. Les mesures de sécurité et les normes techniques relatives à la production du cachet électronique avancé visé à l'article 40, § 3 de la Loi du 5 août 1992 sur la fonction de police sont basées sur

1° 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 en in het bijzonder artikel 36 ervan;

2° de regels of richtlijnen uitgevaardigd door de bevoegde internationale instanties die de voorschriften van Verordening (EU) nr. 910/2014 bedoeld in punt a) inzake de handtekening met behulp van het geavanceerd elektronisch zegel operationaliseren.

1° 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 et en particulier son article 36 ;

2° les règles ou directives édictées par les instances internationales compétentes et qui opérationnalisent les prescrits du Règlement (UE) n ° 910/2014 visé au point a) en matière de signature à l'aide du cachet électronique avancé.

§ 2. De federale politie beschikt over een lijst van die maatregelen en technische normen die worden toegepast op het proces van de handtekening met behulp van het geavanceerd elektronisch zegel.
§ 2. La police fédérale dispose d'une liste de ces mesures et normes techniques appliquées au processus de signature par cachet électronique avancé.

In geval van onderaanneming zijn die maatregelen en normen contractueel toepasselijk op de onderaannemer.

§ 3. Het Controleorgaan op de politionele informatie bedoeld in artikel 71 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens controleert of die maatregelen en normen adequaat zijn en correct ten uitvoer worden gelegd.

En cas de sous-traitance, ces mesures et normes sont contractuellement applicables au sous-traitant.

§ 3. L'Organe de contrôle de l'information policière visé à l'article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel vérifie si ces mesures et normes sont adéquates et correctement mises en œuvre.

Art. 2. De politie-informaticasystemen die het geavanceerd elektronisch zegel produceren, beantwoorden aan de veiligheidsmaatregelen en aan de technische normen die de mogelijkheid bieden

- 1° de gebruikers ervan te identificeren en hun functies en hun mandaten te controleren en te beheren;
- 2° voorafgaand aan de ondertekening met behulp van het geavanceerd elektronisch zegel de ondertekenaar met behulp van een systeem van sterke authenticatie te authenticeren;
- 3° de datum en het precieze tijdstip van gebruik van het geavanceerd elektronisch zegel vast te stellen;
- 4° logbestanden 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 bij te houden.

Art. 2. Les systèmes informatiques policiers qui produisent le cachet électronique avancé répondent aux mesures de sécurité et aux normes techniques permettant

- 1° d'en identifier les utilisateurs et d'en vérifier et gérer leurs fonctions et leurs mandats;
- 2° préalablement à la signature par cachet électronique avancé, d'authentifier à l'aide d'un système d'authentification forte, le signataire;
- 3° d'établir la date et le moment précis d'utilisation du cachet électronique avancé;
- 4° d'établir des fichiers de 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.

Art. 3. De identificatie van de federale of lokale politie in het kader van het proces van ondertekening met behulp van het geavanceerd elektronisch zegel gebeurt met behulp van een certificaat voor een geavanceerd elektronisch zegel uitgegeven door een verlener van vertrouwensdiensten in de zin van artikel 3.19 van Verordening (EU) nr. 910/2014.

Art. 3. L'identification de la police fédérale ou de la police locale dans le cadre du processus de signature à l'aide du cachet électronique avancé se fait à l'aide d'un certificat de cachet électronique avancé émis par un prestataire de service de confiance au sens de l'article 3.19 du Règlement (UE) n° 910/2014.

Art. 4. De maatregelen en normen bedoeld in de artikelen 1 en 2 worden door de federale politie bewaard in een volgens de regels van de kunst beveiligde omgeving.

Art. 4. Les mesures et normes visées aux articles 1 et 2 sont conservées par la police fédérale dans un environnement sécurisé selon les règles de l'art.

Art. 5. § 1. Het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening van de processen-verbaal worden gevisualiseerd in een gematerialiseerde omgeving en bevatten de volgende vermeldingen:

Art. 5. § 1^{er}. Le cachet électronique avancé et la signature électronique qualifiée des procès-verbaux sont visualisés dans un environnement matérialisé et comportent les mentions suivantes :

- 1° "elektronisch ondertekend", in de taal waarin het proces-verbaal is opgesteld;
- 2° de naam en voornaam van de verbalisant;

1° « signé électroniquement », dans la langue de rédaction du procès-verbal;

2° les nom et prénom du verbalisateur;

§ 2. Het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening van de processen-verbaal worden gevisualiseerd in een gedematerialiseerde omgeving en bevatten ten minste de volgende vermeldingen:

§ 2. Le cachet électronique avancé et la signature électronique qualifiée des procès-verbaux sont visualisés dans un environnement dématérialisé et comportent au minimum les mentions suivantes :

- 1° de naam en voornaam van de ondertekenaar;
- 2° de vermeldingen met betrekking tot de geldigheid van het certificaat voor een geavanceerd elektronisch zegel of van een gekwalificeerde elektronische handtekening;

1° les nom et prénom du signataire;

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

3° de vermeldingen met betrekking tot de integriteit van het digitaal ondertekende proces-verbaal. 3° les mentions relatives à l'intégrité du procès-verbal signé numériquement.

§ 3. In de hypothese bedoeld in artikel 40, § 3, 1°, van de wet van 5 augustus 1992 op het politieambt bevatten het geavanceerd elektronisch zegel en de gekwalificeerde elektronische handtekening van de processen-verbaal, in afwijking van § 1, 2°, en § 2, 1°, een aan de ondertekenaar toegekend uniek nummer dat zijn reële identiteit beschermt. § 3. Dans l'hypothèse visée à l'article 40, § 3, 1° de la loi du 5 août 1992 sur la fonction de police, en dérogation aux § 1er, 2° et § 2, 1°, le cachet électronique avancé et la signature électronique qualifiée des procès-verbaux comportent un numéro unique attribué au signataire et qui protège son identité réelle.

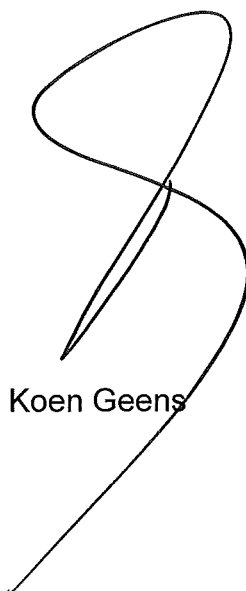
§ 4. De vermeldingen bedoeld in de §§ 1 tot 3 worden gecreëerd op het tijdstip van het gebruik van het geavanceerd elektronisch zegel of van de gekwalificeerde elektronische handtekening. § 4. Les mentions visées aux §§ 1er à 3 sont créées au moment de l'utilisation du cachet électronique avancé ou de la signature électronique qualifiée.

Van Koningswege:

Par le Roi :

De Minister van Justitie

Le ministre de la Justice



Koen Geens

Voorontwerp van koninklijk besluit betreffende 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.

Projet d'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.

VERSLAG AAN DE KONING

RAPPORT AU ROI

Sire,

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.

Le projet d'arrêté 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. 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 acceptatie ervan, niet alleen door de partners van de strafrechtelijke keten en veiligheidsketen, maar ook

1. Introduction générale

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.

door 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, waaronder 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.

Ook al dient het belang van dit vertrouwen voor ondertekening met behulp van een elektronisch zegel meteen al te worden benadrukt, het zou uiteraard niet ambtshalve kunnen impliceren dat dit pakket veiligheidsmaatregelen en technische normen in detail openbaar wordt gemaakt op gevaar af juist de veiligheid van desbetreffende systemen in gevaar te brengen en derhalve, paradoxaal genoeg, de oorspronkelijk nagestreefde veiligheid te schaden.

Uit dit oogpunt wordt in artikel 1 vermeld dat het aan de federale politie is, die een programma voor ondertekening door middel van een geavanceerd elektronisch zegel heeft ingesteld of dit proces uitbesteedt, om altijd te kunnen aantonen ('accountability'-principe) dat zij de functionele en technische nationale en Europese eisen verbonden aan het gebruik van het geavanceerde elektronische zegel in acht neemt.

Bovendien moet vastgesteld worden dat deze technische normen verband houden met de continue ontwikkeling van de technologie en dus per definitie veranderlijk zijn (zie in dit opzicht bijvoorbeeld de werkzaamheden van het technisch comité ESI (Electronic Signatures and Infrastructures) van het ETSI). Overigens heeft tot op heden noch de Europese wetgever, noch de Belgische wetgever een norm ingevoerd waarin de verschillende technische eisen allemaal overgenomen zijn.

Er zou echter niet uitsluitend verwezen moeten worden naar een geheel van processen en procedures geleid door de federale politie. Om die reden wordt in artikel 2 in algemene bewoordingen aangegeven wat de minimale technische eisen zijn die worden gesteld aan de informaticasystemen van de politie die het geavanceerde elektronische zegel produceren. Dientengevolge vormen deze de gemeenschappelijke basis voor het produceren en gebruiken van het geavanceerde elektronische zegel in

Ce cadre d'utilisation du cachet électronique avancé concerne 3 catégories de procès-verbaux, à savoir :

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

2°) celles comprenant les procès-verbaux impliquant la signature d'un lot important de procès-verbaux dont ceux 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 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, soit les procès-verbaux simplifiés.

Si l'importance de cette confiance pour la signature à l'aide d'un cachet électronique avancé doit d'emblée être soulignée, elle ne saurait bien entendu pas d'office impliquer de dévoiler dans leurs détails l'ensemble de ces mesures de sécurité et normes techniques sous peine précisément de compromettre la sécurité desdits systèmes et donc paradoxalement de nuire à la sécurité originellement recherchée.

C'est dans cette optique que l'article 1er énonce qu'il revient à la police fédérale qui a mis au point un logiciel de signature par cachet avancé ou qui sous-traite ce processus de pouvoir démontrer en tout temps (principe d'« accountability ») qu'elle respecte les exigences nationales et européennes fonctionnelles et techniques liées au recours au cachet électronique avancé.

En outre, force est de constater que ces normes techniques sont liées à l'évolution constante de la technologie et sont donc par essence mouvantes (voir par exemple à cet égard les travaux du comité technique ESI (Electronic Signatures and Infrastructures) de l'ETSI). Ni le législateur européen, ni le législateur belge n'a d'ailleurs à ce jour adopté une norme reprenant l'ensemble de ces différentes exigences techniques.

Il ne pourrait néanmoins pas être question d'uniquement référer à un ensemble de processus et de procédures géré par la police fédérale. C'est pourquoi l'article 2 indique en termes génériques les exigences techniques minimales relatives aux systèmes informatiques policiers qui produisent le cachet électronique avancé. Celles-ci constituent dès lors le socle commun entourant la production et l'utilisation du cachet électronique avancé dans le cadre de la signature des procès-verbaux précisée

het kader van het ondertekenen van processen-verbaal zoals weergegeven in artikel 40, § 2, 1° t/m 3° van de wet op het politieambt.

Ten slotte is het aan het Controleorgaan op de politionele informatie om na te gaan of de maatregelen en normen op het gebied van het geavanceerde elektronische zegel adequaat zijn en naar behoren zijn toegepast. Aangezien het Controleorgaan momenteel al beschikt over bevoegdheden om vooraf en achteraf controles uit te voeren betreffende het beheer van politiegegevens, waaronder processen-verbaal, is het logisch dat het ook de controle met betrekking tot de gebruikmaking van het geavanceerde elektronische zegel voor processen-verbaal door de geïntegreerde politie met betrekking tot het elektronisch ondertekenen van processen-verbaal toevertrouwd krijgt, zoals overigens geoorloofd is krachtens artikel 71, § 1, 3° van de wet van 30 juli 2018 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens. In navolging van het bepaalde met betrekking tot auditeerbaarheid vooraf en achteraf van vertrouwensdiensten die gekwalificeerde diensten aanbieden in de zin van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna eIDAS-verordening), zal de federale politie zich in het kader van dit proces ook laten controleren door het Controleorgaan op de politionele informatie. Gezien het technische karakter van de materie en zoals overigens al bepaald is in artikel 245, § 3 van de wet van 30 juli 2018, zal het Controleorgaan, indien het dit passend en nuttig acht, vereiste deskundigen op dit gebied om zich heen kunnen verzamelen om de genoemde controles uit te voeren.

(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

à l'article 40, § 2, 1° à 3° de la loi sur la fonction de police.

Enfin, il appartient à l'Organe de contrôle de l'information policière de vérifier, si les mesures et normes en matière de cachet électronique avancé sont adéquates et correctement mises en œuvre. Etant donné que l'Organe de contrôle a déjà actuellement les compétences pour mener des audits a priori et a posteriori en matière de gestion des données policières en ce compris pour les procès-verbaux, il est logique que le contrôle relatif au cachetage électronique avancé des procès-verbaux par la police intégrée en matière de signature des procès-verbaux lui soit aussi confié, comme le permet d'ailleurs l'article 71, §1er, 3° de la loi du 30 juillet 2018 relative à la protection des personnes à l'égard des traitements de données à caractère personnel.

A l'instar de ce qui est prévu en termes d'auditabilité a priori et a posteriori des services de confiance qui offrent des services qualifiés au sens du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ci-après le Règlement européen eIDAS), la police fédérale se fera aussi auditer dans le cadre de ce processus par l'Organe de contrôle de l'information policière. Vu la technicité de la matière, et comme c'est par ailleurs déjà prévu à l'article 245§3 de la loi du 30 juillet 2018, l'Organe de contrôle pourra s'entourer, s'il l'estime opportun et utile, des experts requis en la matière pour réaliser lesdits audits.

(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, certains logiciels permettent de matérialiser la signature électronique « sur écran ».

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

digitaal gebruik.

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 de artikelen

Artikel 1

Zoals ik in de inleiding heb aangegeven, brengt het gebruik van het geavanceerde zegel door de federale politie het bijhouden van gegevens met zich mee waarbij de concrete maatregelen en technische normen worden overgenomen die van toepassing zijn op de procedure voor ondertekening door middel van het elektronische zegel.

Het bijhouden van deze gegevens gebeurt in samenwerking door de Algemene directie van het middelenbeheer en de informatie, die belast is met het voorbereiden van de technische normen en de regels voor het beheer van de informatie- en communicatiesystemen van de geïntegreerde politie (artikel 6, 3° b van het koninklijk besluit van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie) en het Commissariaat-generaal van de federale politie, dat belast is met het vaststellen van normen en een standaardbenadering op het gebied van informatieveiligheid (artikel 2, e) van datzelfde KB). De technische normen zijn enerzijds gebaseerd op de algemene veiligheidsstandaarden voor de systemen van de geïntegreerde politie en anderzijds op de specifieke standaarden voor toepassing op het gebied van het geavanceerde elektronische zegel, waaronder uiteraard de standaarden die volgen uit de Europese eIDAS-verordening, in het bijzonder artikel 36 daarvan.

Ofschoon het, zoals reeds genoemd, gerechtvaardigd noch passend is om deze lijst uitvoerig te beschrijven, spreekt het vanzelf dat deze moet dienen om de vier noodzakelijke elementen te realiseren zoals bedoeld in

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, 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 des articles

Article 1er

Comme nous l'avons indiqué dans l'introduction, le recours au cachet avancé par la police fédérale implique la tenue d'une documentation reprenant les mesures et norme techniques concrètes appliquées à son processus de signature par cachet électronique.

Cette documentation sera effectuée de concert entre la direction générale de la gestion des ressources et de l'information, qui est chargée de la préparation des normes techniques et des règles de gestion des systèmes d'information et de communication de la police intégrée (article 6, 3° b de l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale) et le Commissariat général de la police fédérale qui est chargé de la détermination de normes et d'une approche standardisée en matière de sécurité de l'information (article 2, e) du même AR).

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.

Si comme nous l'avons déjà mentionné, il n'est ni justifié ni opportun de détailler cette liste, il va de soi qu'elle devra servir à opérationnaliser les 4 éléments indispensables visés à l'article 36 du Règlement

artikel 36 van de Europese eIDAS-verordening, die betrekking hebben op het geavanceerde elektronische zegel; zodat het aan de volgende eisen voldoet:

1°) het maakt het mogelijk de aanmaker van het zegel te identificeren;

Deze identificatie zal, zoals genoemd, gebeuren met hulp van een leverancier van vertrouwensdiensten van buiten de politie, zodat de identiteit van de ondertekenaar met zekerheid kan worden vastgesteld.

2°) het is op unieke wijze aan de aanmaker van het zegel verbonden;

Het zal bijvoorbeeld gaan om verbinding van het certificaat aan een unieke private sleutel voor de ondertekenaar.

3°) het komt tot stand 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 het aanmaken van elektronische zegels;

Voor de federale politie is het belangrijk om ofwel zelf in een door haar beheerde omgeving rechtstreeks het geavanceerde elektronische zegel aan te maken, ofwel, zoals overweging 52 van de Europese eIDAS-verordening toestaat, indien zij het aanmaken van de handtekening door middel van een elektronisch zegel uitbesteedt, de verleners van diensten voor elektronische handtekeningen op afstand door middel van een geavanceerd elektronisch zegel te verplichten om "specifieke veiligheidsprocedures toe te passen wat betreft beheer en administratie, en gebruik te maken van betrouwbare systemen en producten, met inbegrip van beveiligde elektronische communicatiekanalen, om te waarborgen dat de omgeving waarin de elektronische handtekening wordt aangemaakt betrouwbaar is en dat uitsluitend de ondertekenaar controle heeft over het gebruik ervan".

4°) het is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Voor de politie is het dus zaak om technische maatregelen in te voeren om te zorgen voor een logisch verband tussen het proces-verbaal en de handtekening door middel van een geavanceerd elektronisch zegel, zodat elke wijziging achteraf van de gegevens kan worden opgespoord.

Artikel 2

Artikel 2 bevat de vier specifieke technische eisen voor de informaticasystemen van de politie die het geavanceerde elektronische zegel produceren.

européen eIDAS et relatifs au cachet électronique avancé, à savoir le fait que le cachet avancé doit

1°) permettre d'identifier le créateur du cachet

Cette identification sera, comme nous l'avons mentionné, effectuée en recourant à un prestataire de service de confiance externe à la police de sorte que l'identité du signataire puisse être retrouvée de manière certaine.

2°) être lié au créateur du cachet de manière univoque ;

Il s'agira par exemple d'associer le certificat à une clé privée unique pour le signataire.

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 pour créer un cachet électronique ;

Il s'agit pour la police fédérale soit de créer elle-même dans un environnement qu'elle gère directement le cachet électronique avancé, soit comme le considérant 52 du Règlement européen eIDAS le permet, si elle soustraite la création de la signature par cachet électronique, contraindre les prestataires offrant des services de signature électronique par cachet avancé à distance à « appliquer des procédures de sécurité spécifiques en matière de gestion et d'administration et utiliser des systèmes et des produits fiables, notamment des canaux de communication électroniques sécurisés, afin de garantir que l'environnement de création de signatures électroniques est fiable et qu'il est utilisé sous le contrôle exclusif du signataire ».

4°) et être lié aux données auxquelles il est associé de telle sorte qu'une possibilité de modification indétectable de données soit exclue.

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.

Article 2

L'article 2 reprend les 4 exigences techniques spécifiques relatives aux systèmes informatiques policiers qui produisent le cachet électronique avancé.

Op de eerste plaats moeten deze systemen de diverse gebruikers identificeren.

Deze identificatie vooraf is een kernelement van het proces als zij wordt gekoppeld aan het controleren van de functies en machtigingen van degene die zich identificeert. Op die manier hebben immers uitsluitend de medewerkers die een specifieke functie bekleeden en gemachtigd zijn, toegang tot de informaticasystemen.

Anders geformuleerd is het dus zaak dat deze systemen - de medewerker die een elektronisch zegel wil gebruiken, identificeren en

- een zodanig essentiële factor zijn dat uitsluitend daartoe geautoriseerde personen gebruik kunnen maken van de applicatiemodule met betrekking tot de geavanceerde elektronische handtekening. Dit impliceert met name dat de systemen van de politie onderscheid kunnen maken tussen verschillende soorten profielen: bijvoorbeeld een gebruiker die een technische machtiging heeft om zich te bemoeien met de zegelmodule, of een gebruiker die als verbalisant een reeks processen-verbaal wil ondertekenen.

Ten tweede moet de verbalisant, als hij zich eenmaal geïdentificeerd heeft en zijn machtiging is gecontroleerd, zich ook nog authenticeren alvorens de reeks processen-verbaal (artikel 40, § 2, 2° en 3° van de wet op het politieambt) of een individueel proces-verbaal (artikel 40, § 2, 1°) te verzegelen met behulp van bijvoorbeeld zijn identiteitskaart en zijn PIN-code of enig ander betrouwbaar authenticatiemiddel. Deze betrouwbare authenticatie kan één maal worden gebruikt voor een reeks processen-verbaal. Bovendien wordt zij overgenomen in de logboeken. Door deze betrouwbare authenticatiehandeling formaliseert de verbalisant zijn individuele, zelfstandige bereidheid om voor eigen naam en rekening de constatering te doen zoals vermeld in de processen-verbaal.

Wat het technische proces betreft, zal de reeks processen-verbaal meteen worden verzegeld zodra de verbalisant zich heeft geauthenticeerd met behulp van zijn identiteitskaart.

Deze betrouwbare authenticatie bevestigt verder nog eens dat de verbalisant die een proces-verbaal heeft verzegeld, dit later niet zal kunnen ontkennen.

Ten derde moet het politiesysteem dat gebruikmaakt van het geavanceerde elektronische zegel, de datum, het tijdstip en de gebruiker van het elektronische zegel vaststellen en gedurende maximaal 30 jaar bewaren. Met andere woorden: het systeem moet het tijdstip vastleggen van een gebeurtenis (verzegeling) die via elektronische weg plaatsvindt.

Ten slotte vormt de gebruikmaking van een elektronisch zegel voor het ondertekenen van de processen-verbaal een specifieke verwerking die invloed zal hebben op de

Premièremment, ces systèmes doivent identifier leurs différents utilisateurs.

Cette identification en amont est un élément clef 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 sont dans 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 et

- que ces systèmes soient paramétrés de telles sorte que seuls, ceux qui 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, verbalisateur, qui souhaite signer une série de procès-verbaux.

Deuxièmement, dès lors que le verbalisateur s'est identifié et que son mandat a été vérifié, il doit en outre s'authentifier avant de cacheter un lot de procès-verbaux (article 40, § 2, 2° et 3° LFP) ou un procès-verbal individuel (article 40, § 2, 1°) à l'aide par exemple de sa carte d'identité et de son code PIN ou de tout autre moyen d'authentification forte. Cette authentification forte peut être utilisée une seule fois pour un lot de procès-verbaux. Elle sera en outre reprise dans les journaux. Par cet acte d'authentification forte, le verbalisateur formalise sa volonté individuelle et libre de prendre à son nom personnel et à son compte les constatations qui sont faites dans les procès-verbaux.

Au niveau du processus technique, dès lors que le verbalisateur s'est authentifié à l'aide de sa carte d'identité, le lot de procès-verbaux sera immédiatement après cacheté.

Cette authentification forte renforce par ailleurs le fait que le verbalisateur qui a cacheté un procès-verbal ne pourra pas ultérieurement le nier.

Troisièmement, le système policier qui utilise le cachet électronique avancé doit établir et garder pendant au maximum 30 ans la date, le moment, et l'utilisateur du cachet électronique. En d'autres termes, ce système doit fixer dans le temps, un événement (cachetage) qui intervient par voie électronique.

Enfin, le recours à un cachet électronique pour signer les procès-verbaux constitue un traitement spécifique qui aura un impact dans le reste de la chaîne pénale. Dès

rest van de strafrechtelijke keten. Derhalve worden de regels die ervoor zorgen dat alle verrichte handelingen traceerbaar zijn, gewaarborgd door gebruikmaking van verwerkingslogboeken (LOGS) die het mogelijk moeten maken om voor alle verwerkingen met betrekking tot de verzegeling van processen-verbaal vast te stellen wie welke verwerking heeft uitgevoerd, op welk moment en waarom.

Deze traceerbaarheid is natuurlijk een doorslaggevend element op het gebied van 'accountability'.

Artikel 3

Het met zekerheid vaststellen van de identiteit van de ondertekenaar van een proces-verbaal met behulp van een geavanceerd elektronische zegel vormt uiteraard tevens een veiligheidsmaatregel.

Derhalve moet het "numerieke paspoort" waarmee de politie zich zal gaan identificeren bij de ondertekening door middel van een geavanceerd elektronisch zegel, vooraf buiten de politie worden onderworpen aan een controle door een vertrouwde derde (leverancier van vertrouwensdiensten). Het doel is uiteraard om een factor toe te voegen aan de relatie tussen zender en ontvanger van het proces-verbaal door tussenkomst van een vertrouwde derde die door het verschaffen van een certificaat de bevoegdheid van de zender officieel bevestigt.

Indien voor het ondertekenen van processen-verbaal gebruik wordt gemaakt van de technologie van het geavanceerde elektronische zegel, dan is dit in wezen omdat zij het mogelijk maakt om in één keer een grote hoeveelheid processen-verbaal te ondertekenen, hetgeen blijkt geeft van efficiëntie in bepaalde politieprocedures, zoals procedures voor direct verschuldigde belasting. Het blijft daarom niet minder waar dat, naast de identificatie van de rechtspersoon, de identificatie van de individuele verbalisant, die de eindverantwoordelijkheid voor de handeling neemt, even belangrijk is.

In die zin maakt het gebruikte systeem niet alleen het traceren van de ondertekenende rechtspersoon mogelijk, maar ook van de verbalisant die gebruik wenst te maken van het zegel.

Om dezelfde redenen wordt zijn naam zowel in een gedematerialiseerde omgeving (computerscherm) als een niet-gedematerialiseerde omgeving (afgedrukt PV) of weergegeven.

Artikel 4

Aangezien deze lijst van technische maatregelen gevoelige elementen bevat die met name betrekking hebben op het aanmaken en gebruiken van programma's die te maken hebben met het geavanceerde elektronische

lors, les règles permettant d'assurer la traçabilité de tous les actes posés sont assurées via le recours à des journaux de traitements (de LOGS) devant permettre d'établir pour tous les traitements liés au cachetage des procès-verbaux, qui a réalisé quel traitement, à quel moment et pourquoi.

Cette traçabilité est bien entendu un élément déterminant en termes d'«accountability».

Article 3

L'identification certaine du signataire d'un procès-verbal à l'aide d'un cachet électronique avancé constitue bien entendu aussi une mesure de sécurité.

Dès lors, le « passeport numérique » à l'aide duquel la police va s'identifier dans la signature par cachet électronique avancé doit faire l'objet d'une vérification préalable et externe à la police par un tiers de confiance (un prestataire de service de confiance). Le but est bien entendu d'apporter une triangulation dans la relation émetteur de procès-verbal, récepteur par le truchement d'un tiers de confiance qui, par la fourniture d'un certificat, atteste formellement de la qualité de l'émetteur.

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.

Il n'en reste pas moins vrai qu'outre l'identification de la personne morale, l'identification du verbalisateur individuel, qui endosse la responsabilité finale de l'acte est aussi importante.

C'est dans ce sens que le système utilisé permet non seulement de tracer la personne morale signataire mais aussi le verbalisateur qui souhaite recourir au cachet.

C'est pour les mêmes raisons que son nom apparaît aussi dans un environnement dématérialisé (écran de PC) ou matérialisé (PV imprimé).

Article 4

Vu que cette liste de mesures techniques comporte des éléments sensibles relatifs notamment à la création et l'utilisation de logiciels liés au cachet électronique avancé, au stockage des certificats et des mots de passe, il est

zegel, het opslaan van certificaten en wachtwoorden, dient de lijst te worden beveiligd, met name ter beperking van het risico op vervalsing of oneigenlijk gebruik.

Artikel 5

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 tastbare omgeving, voor zover de automatisering niet 'end to end' wordt toegepast en er papieren verwerking van dossiers blijft plaatsvinden.

In een tastbare 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 verbalisant te vermelden.

Het zichtbaar maken van een digitale handtekening (gekwaliceerde 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 voor- en achternaam van de ondertekenaar weergeven, informatie verstrekken over de geldigheid van het handtekeningcertificaat (geavanceerd elektronisch zegel of gekwalificeerde elektronische handtekening) en garanties bieden betreffende de integriteit van het document (na ondertekening kan het document niet meer worden gewijzigd).

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. Uiteraard kunnen andere identiteitsbeschermende maatregelen worden toegepast om de anonimiteit van de

nécessaire de la protéger notamment pour limiter tout risque de falsification ou d'usage inapproprié.

Article 5

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 associée 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 verbalisateur.

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 nom et prénom du signataire, de donner les informations relatives à la validité du certificat de signature (cachet électronique avancé ou signature électronique qualifiée) et de donner des garanties quant à l'intégrité du document (le document, une fois signé, ne peut plus être modifié).

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 aux procès-verbaux visés à l'article 41, § 2, de la loi sur la fonction de police, ainsi que ceux visés aux articles 112quater et 112quinquies 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 112quater du Code d'instruction criminelle.

D'autres mesures de protection de l'identité peuvent bien entendu être appliquées pour protéger l'anonymat du

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
ondertekening van processen-verbaal van toepassing

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.

Wij hebben de eer te zijn,

de zeer eerbiedige
en zeer getrouwe dienaars,

De Minister van Justitie,

Nous avons l'honneur d'être,

les très respectueux
et très fidèle serviteur,

Le Ministre de la Justice,

Koen GEENS