JUSTEL - Législation consolidée

<http://www.ejustice.just.fgov.be/eli/arrete/2021/07/18/2021032042/justel>

Dossier numéro : 2021-07-18/08

Titre

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

Source : INTERIEUR

Publication : Moniteur belge du 13-08-2021 page : 84228

Entrée en vigueur : 23-08-2021

Table des matières

[CHAPITRE Ier.](#) - DEFINITIONS

Art. 1

[CHAPITRE II.](#) - MESURES DE SECURITE ET NORMES TECHNIQUES MINIMALES DES SYSTEMES POLICIERS QUI PRODUISENT LE CACHET ELECTRONIQUE AVANCE

Art. 2-11

[CHAPITRE III.](#) - Mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée

Art. 12-13

[ANNEXE.](#)

Art. N

Texte

[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 ;

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.

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.