Référentiel Certification Electronique

Annexe 1

Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de Certificats Electroniques

Adaptée à la loi sur la Transactions Electroniques et son décret d'application (décret 2018-062)

Version 1

Mise à jour : Décembre 2019

SOMMAIRE

I.Objet et contenu du document

Le présent document « Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques » est basé sur le Référentiel Général de Sécurité Français. Il fait partie des Annexes constitutives du Référentiel des exigences applicables aux Prestataires de Services de Certification Electronique (« PSCE »).

Il fixe les règles de sécurité applicables aux différents « composants » nécessaires à la mise en œuvre des fonctions de sécurité basées sur l'emploi des Certificats Electroniques.

Ces fonctions de sécurité sont les suivantes :

- Signature Electronique ;
- Authentification de personne ;
- double usage Signature Electronique et Authentification ;
- Confidentialité ;
- Cachet ;
- Authentification de serveur

Ces composants sont les suivants :

- les bi-clés et Certificats Electroniques délivrés par des Prestataires de Service de Certification Electronique pour les usages listés ci-dessus ;
- le dispositif de protection des éléments secrets ;
- les applications qui assurent l'interface avec les Utilisateurs (ou les machines), les dispositifs de protection et les éléments secrets.

Les règles spécifiques à une fonction de sécurité donnée seront précédées du nom de la fonction de sécurité entre « [] » (exemple [Signature Electronique]). De la même manière, les règles applicables aux Certificats Electroniques délivrés à des personnes seront précédées par [Personne] et celles applicables aux Services applicatifs par [Service applicatif].

II. Présentation des fonctions de sécurité

II.1. Fonction de sécurité « Signature Electronique »

La Signature Electronique est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés.

La Signature Electronique peut être requise et mise en œuvre lorsque l'Utilisateur est en relation avec une application d'échange dématérialisé depuis son ordinateur personnel ou depuis une borne d'accès.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de Signature, déployée sur une machine (PC, borne publique, serveur...) peut réaliser les premières itérations de calcul d'un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- elle transmet les informations nécessaires à la réalisation de la Signature (informations à signer complètes ou partielles, condensat partiel le cas échéant) au dispositif de création de Signature (exemples : carte à puce, clé USB) également connecté à la machine ;
- le dispositif de création de Signature réalise les itérations restantes (a minima la dernière itération) du calcul du condensat, à l'aide d'une fonction de hachage, à partir des informations transmises par l'application de création de Signature ;
- le dispositif de Signature réalise un calcul cryptographique de Signature du condensat en utilisant la clé privée de Signature de l'Utilisateur, activée le cas échéant par un code d'activation (code PIN par exemple) ;
- ce condensat signé, dit Signature Electronique, est retourné à l'application ;
- la vérification de la Signature s'effectue à l'aide d'un module de vérification de Signature et du Certificat Electronique délivré par PSCE qui lie l'identité de l'Utilisateur avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la Signature Electronique et comparé au condensat obtenu par hachage des informations à signer.

II.2. Fonction de sécurité « Confidentialité»

La Confidentialité est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre Utilisateurs. Elle permet de garantir que seuls les ayants droits ont accès aux informations lors des échanges dématérialisés.

Les types de relations couverts par la fonction de sécurité « Confidentialité » sont notamment les suivants :

- chiffrement de données Electroniques par un Utilisateur à destination d'un autre Utilisateur ;
- chiffrement e données Electronique par un Service à destination d'un Utilisateur.

Le chiffrement permet d'assurer que les données échangées ne seront accessibles, lors de l'échange ou de leur stockage, que par le ou les destinataires de ces données.

Un tel chiffrement peut être requis et mis en œuvre lorsque, par exemple, l'Utilisateur est en relation avec une application d'échange dématérialisé et que les informations échangées

nécessitent d'être protégées en Confidentialité en raison de leur sensibilité.

Le principe de fonctionnement typique d'interaction des composants entre eux pour mettre en œuvre la fonction de sécurité « Confidentialité » est le suivant:

- le chiffrement des données échangées entre un émetteur et un destinataire est effectué *in fine* à l'aide d'une clé symétrique dite « clé de session » ;
- elle est elle-même échangée de façon confidentielle entre l'émetteur et le destinataire, en ayant recours soit à un mécanisme cryptographique asymétrique soit à un mécanisme de type Diffie-Hellman. Le module de chiffrement de l'utilisateur utilise la clé publique du destinataire pour réaliser un calcul cryptographique. Cette clé publique est trouvée dans le Certificat Electronique du destinataire délivré par un PSCE. Le résultat est transmis au destinataire ;
- le destinataire déchiffre ce résultat à l'aide de sa clé privée confinée dans un dispositif de stockage par l'intermédiaire d'un module de déchiffrement.

Il est également possible de ne pas recourir à une clé de session symétrique pour effectuer le chiffrement de données : les données peuvent être chiffrées directement avec la clé publique du destinataire et déchiffrées par lui à l'aide de sa clé privée.

II.3. Fonction de sécurité « Authentification »

L'Authentification est l'une des fonctions de sécurité permettant à un système numérique de s'assurer de l'identité d'une personne ou d'une machine. Elle apporte la confiance dans les échanges dématérialisés entre Utilisateurs.

Le type de relations couvert par le Service d'Authentification est la reconnaissance de l'habilitation d'un Utilisateur vis-à-vis d'un Service.

Cette fonction de sécurité permet à un Utilisateur de s'authentifier dans le cadre de services distants . Ce document ne traite que de l'Authentification basée sur des mécanismes cryptographiques asymétriques.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de Cachet, déployée sur une ou plusieurs machines calcule un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- elle transmet ce condensat au dispositif de création de Cachet ;
- le dispositif de création de Cachet réalise un calcul cryptographique de Signature du condensat en utilisant la clé privée de Signature du Service de création de Cachet, activée le cas échéant par un code d'activation (code PIN par exemple) par le responsable du Certificat de Cachet ;
- ce condensat signé, dit Cachet, est retourné à l'application.

La vérification du Cachet s'effectue à l'aide d'un module de vérification de Cachet et du Certificat Electronique délivré par un PSCE qui lie l'identité du Service de création de Cachet avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la Signature Electronique et comparé au condensat obtenu par hachage des informations à signer.

II.4. Fonction de sécurité « Cachet »

Le Cachet, apposé par un Service de création de Cachet, est l'une des fonctions de sécurité apportant

de la confiance dans les échanges dématérialisés entre Utilisateurs. Le terme « Cachet » est utilisé par un Service applicatif, se différenciant ainsi de la « Signature Electronique » qui est un terme réservé à une personne physique.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application de création de Cachet, déployée sur une machine (PC, borne publique, serveur...) peut réaliser les premières itérations de calcul d'un condensat, à l'aide d'une fonction de hachage, à partir des informations à signer ;
- Elle transmet les informations nécessaires à la réalisation du Cachet (informations à signer complètes ou partielles, condensat partiel le cas échéant) au dispositif de création de Cachet (exemples : carte à puce, clé USB) également connecté à la machine ;
- le dispositif de création de Cachet réalise les itérations restantes (a minima la dernière itération) du calcul du condensat, à l'aide d'une fonction de hachage, à partir des informations transmises par l'application de création de Cachet ; ce condensat signé, dit Cachet, est retourné à l'application ;
- la vérification du Cachet s'effectue à l'aide d'un module de vérification de Cachet et du Certificat Electronique délivré par un PSCE qui lie l'identité du Service de création de Cachet avec sa clé publique : un calcul cryptographique est effectué à l'aide de la clé publique sur la Signature Electronique et comparé au condensat obtenu par hachage des informations à signer.

II.5. Fonction de sécurité « Authentification serveur »

L'Authentification d'un serveur est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre Utilisateurs.

Les types de relations couverts par le Service d'Authentification serveur sont notamment les suivants :

- établissement d'une session sécurisée entre un serveur et un Utilisateur,
- établissement d'une session sécurisée entre deux serveurs.

Cette fonction de sécurité permet à un serveur de s'authentifier et d'établir des sessions sécurisées dans le cadre des types de relations mentionnés ci-dessus.

Le principe de fonctionnement et d'interaction des composants entre eux est le suivant :

- l'application d'Authentification transmet une requête d'Authentification (un « challenge ») au dispositif d'Authentification dans lequel la clé privée d'Authentification du serveur est confinée et protégée notamment en Confidentialité ;
- le dispositif d'Authentification réalise un calcul cryptographique de Signature du « challenge » en utilisant la clé privée, une fois celle-ci activée par le responsable du serveur, le cas échéant à l'aide d'un code d'activation (code PIN par exemple) ;
- ce challenge signé est retourné à l'application ;
- la vérification de l'Authentification s'effectue à l'aide d'un module de vérification et du Certificat Electronique délivré par PSCE qui lie l'identité du serveur avec sa clé publique : un calcul cryptographique « inverse » est effectué à l'aide de la clé publique sur le challenge signé et comparé au challenge initial.

III.Exigences relatives à la mise en œuvre des fonctions de sécurité

Ce paragraphe regroupe toutes les exigences de sécurité, d'interopérabilité ainsi que les bonnes pratiques pour les composants participant aux fonctions de sécurité.

III.1. Les Certificats délivrés par les PSCE

Les exigences que doit respecter un PSCE, délivrant des Certificats Electroniques sont définies dans les Politiques de Certification type (PC Type) « Personne » et « Service applicatif » (Annexes 2 et 3 du Référentiel Certification Electronique). Ces deux PC Types distinguent les exigences spécifiques à chacune des fonctions de sécurité ainsi que trois niveaux de sécurité aux exigences croissantes *, ** et ***.

En l'occurrence, la PC Type « Personne » traite des fonctions de sécurité « Signature Electronique », « Authentification » et « Confidentialité ». La PC Type « Service applicatif » traite des fonctions de sécurité « Cachet » et « Authentification serveur ». Ces deux PC Types distinguent également les règles spécifiques au porteur pour lesquels le Certificat Electronique est délivré.

Il est autorisé d'utiliser au sein d'un système d'information un Certificat Electronique de niveau de sécurité supérieur à celui de la fonction de sécurité demandée sous réserve que le niveau du dispositif de protection de la clé privée et le niveau du Certificat soient cohérents. Par exemple, un Certificat Electronique conforme aux exigences du niveau (***) pourra être employé dans des télé-Services de niveaux inférieurs, sous réserve de son interopérabilité.

Ces PC Type s'appuient sur des règles et recommandations relatives à des profils des Certificats, aux listes de Certificats révoqués et au protocole OCSP ainsi qu'aux exigences sur les algorithmes cryptographiques mis en œuvre (Annexe 4 du Référentiel Certification Electronique).

III.2. Les dispositifs de protection des éléments secrets

Le dispositif de protection des éléments secrets des utilisateurs ou des serveurs est un logiciel ou un matériel (carte à puce par exemple) qui stocke la clé privée dédiée à une fonction de sécurité donnée, les éléments permettant de la déverrouiller (code PIN par exemple), qui permet sa mise en œuvre et, le cas échéant, leur génération.

III.2.1. Dispositifs de protection des éléments secrets d'une personne physique

Quel que soit le niveau visé, le dispositif de protection des éléments secrets de la personne doit répondre aux exigences de sécurité suivantes :

- si la bi-clé est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération ;
- garantir la Confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

- disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ou de destruction des clés privées qui ne sont plus utilisées ;
- permettre de garantir la Confidentialité, l'authenticité et l'intégrité de la clé symétrique lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

Les exigences de sécurité sont décrites dans l'Annexe 2 du Référentiel Certification Electronique.

III.2.2. Dispositifs de protection des éléments secrets d'un Service applicatif

III.2.2.1. Exigences de sécurité

Le dispositif de protection des éléments secrets du Service applicatif doit répondre aux exigences de sécurité suivantes :

- si la bi-clé est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi- clé générée ;
- assurer la correspondance entre la clé privée et la clé publique.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- détecter les défauts lors des phases d'initialisation, et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ;
- garantir la Confidentialité et l'intégrité de la clé privée ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Les exigences sont décrites dans l'Annexe 3 du Référentiel de Certification Electronique.

Cachet
Assurer pour le serveur légitime uniquement la fonction de génération des Cachets Electroniques et protéger la clé privée contre toute utilisation par des tiers.

Authentification Serveur
- Assurer pour le serveur légitime uniquement, d'une part, la fonction d'Authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers; - Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données.

III.2.2.2. Exigences en termes d'évaluation et d'audit

Les composantes de l'Infrastructure de Gestion des Clés qui mettent en œuvre la clé privée doit faire l'objet d'un audit de sécurité.

Cet audit doit comprendre :

- un audit de l'architecture réseau (liaison entre les différentes zones et entités, filtrage),
- un audit de configuration (équipements réseau et de sécurité, serveurs d'infrastructure)
- un audit organisationnel.

Au-delà des strictes composantes de l'IGC, l'environnement dans lequel est déployée la clé privée peut faire l'objet d'un audit de sécurité.

III.3. Les Applications

III.3.1. Exigences de sécurité

Les opérations cryptographiques de chiffrement sont mises en œuvre dans un module de chiffrement qui va procéder au chiffrement. Quel que soit le niveau, un module de chiffrement doit répondre aux exigences de sécurité suivantes :

- garantir la robustesse cryptographique de la clé symétrique de message ou de fichier qui est générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés qui ne sont plus utilisées ;
- garantir la Confidentialité et l'intégrité de la clé symétrique de fichier ou de message et des données à chiffrer ;
- assurer l'accès à la clé symétrique de message ou de fichier exclusivement par les utilisateurs autorisés et protéger cette clé contre toute utilisation par des tiers].

Les opérations cryptographiques de déchiffrement sont mises en œuvre dans un module de déchiffrement qui va procéder au déchiffrement. Quel que soit le niveau, un module de déchiffrement doit répondre aux exigences de sécurité suivantes :

- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés qui ne sont plus utilisées ;
- garantir la Confidentialité et l'intégrité de la clé symétrique de fichier ou de message et des données à chiffrer ;
- assurer l'accès à la clé symétrique de message ou de fichier exclusivement par les utilisateurs autorisés et protéger cette clé contre toute utilisation par des tiers.

III.3.2. Bonnes pratiques

Avant de se fier à un Certificat Electronique, il faut notamment vérifier que celui-ci :

- contient une indication d'usage conforme à ce qui est attendu ;
- est valide et n'est pas révoqué ;
- a une chaîne de Certification qui est correcte à tous les niveaux ;
- correspond au niveau de sécurité cohérent avec l'usage pour lequel il est destiné.

Il est recommandé pour ce faire d'élaborer une politique de vérification des Certificats Electroniques.

III.4. Environnement d'utilisation

Les fonctions de sécurité « Signature », « Authentification » et « Confidentialité » sont notamment

mises en œuvre sur une borne publique ou un ordinateur dans un cadre privé ou professionnel pour un usage par une personne physique.

Les fonctions de sécurité « Cachet » et « Authentification Serveur » sont notamment mises en œuvre sur un ou plusieurs serveurs hébergeant un Service applicatif, pour un usage relevant d'une personne morale et sous le contrôle d'une personne physique.

Il est recommandé de prendre en compte les mesures de sécurité suivantes :

- protection contre les virus, avec mises à jour régulière ;
- contrôle et limitation des échanges entre la machine hôte et d'autres machines dans un réseau ouvert ;
- restriction, lorsque cela est possible, de l'accès aux fonctions d'administration de la machine aux seuls administrateurs de celles-ci (différenciation compte utilisateur/administrateur) ;
- installation et mise à jour de logiciels et de composants sur la machine sous le contrôle de l'administrateur ;
- refus par le système d'exploitation de l'ordinateur ou de la borne d'exécuter des applications téléchargées ne provenant pas de sources sûres ;
- mise à jour des composants logiciels et systèmes lors de la mise à disposition de mises à jour de sécurité de ceux-ci.

Dans le cas de l'utilisation d'une carte à puce comme dispositif de protection des éléments secrets, il est recommandé d'utiliser un lecteur de carte à puce avec PIN/PAD intégré qualifié permettant de saisir le code de déverrouillage et de le vérifier sans que celui-ci ne transite via l'ordinateur ou la borne d'accès publique, ou le serveur utilisés.

Les opérations de chiffrement et de déchiffrement doivent permettre, à tout moment, de garantir la Confidentialité des données à chiffrer / déchiffrer. Il est donc recommandé de procéder aux opérations de chiffrement et de déchiffrement de telle façon que les informations à protéger ne soient jamais présentes en clair sur une machine reliée au réseau sur lequel transitent les données chiffrées à protéger.