Cible de sécurité CSPN

ClearBUS – Application cliente pour la communication sécurisée

Version 1.12 Le 25/11/2011

Identifiant : **CBUS-CS-1.12-20111125**

contact@clearbus.fr
tel : +33(0)485.029.634

Table des matières

Suivi des modifications

Identification		
Client	**Projet**	**Fournisseur**
	Transport sécurisé de documents numériques	ClearBUS

Validité du document			
Actions	**Date**	**Version**	**Nom**
Rédaction initiale	29/11/2010	V 0.1	Karim Slamani
Changement de la cible de sécurité	3/12/2010	V0.2	Jean Marc Lefebvre
Commentaires sur les modifications apportées à la nouvelle cible.	8/12/2010	V 0.3	Karim Slamani
Correctifs par rapport au nouveau périmètre de certification	10/12/2010	V0.4	Karim Slamani
Version finale pour soumission à l'ANSSI	17/12/2010	V1.0	Jean-Marc Lefebvre
Prise en compte des remarques de la première évaluation ANSSI	18/11/2011	V1.1	Jean-Marc Lefebvre
Corrections après relecture de la V1.1	23/11/2011	V1.11	Jean-Marc Lefebvre
Précision sur l'environnement	25/11/2011	V1.12	Jean-Marc Lefebvre

1. Identification de la cible

Catégorie	Identification
Organisation éditrice	ClearBUS
Lien vers l'organisation	http://www.clearbus.fr/
Nom commercial du service	ClearBUS
Numéro de version évaluée	1.1
Catégorie de produit	Communication Sécurisée

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN.

Le produit évalué est l'ensemble des sources de la librairie qui permet l'envoi de documents numériques électroniquement signés vers une application tierce qui aura pour but de tracer les opérations réalisées et de les conserver de manière sécurisée, c'est-à-dire en garantissant leur confidentialité et leur intégrité.

Ce document décrit le produit évalué, précise les hypothèses sur l'environnement du produit, les menaces qui portent sur le produit ainsi que les fonctions de sécurité du produit.

2. Argumentaire

1. Description générale.

La société ClearBUS est un éditeur de logiciel qui propose un service innovant de « service postal dématérialisé ».

Pour se faire, ClearBUS propose une solution composée :

- D'une interface Web pour la partie « gestion utilisateur/abonné » (BSS).
- D'un logiciel que l'on qualifiera de client lourd pour la partie « dépôt et réception du courrier » de type « Communication sécurisée » (CLIC). Ce logiciel utilise une bibliothèque informatique « ClearBUS Secure » qui gère la communication sécurisée, l'authentification et l'intégrité des échanges

- D'un logiciel spécifique (partie serveur) hébergé par ClearBUS pour la gestion du courrier intégrant des fonctions de type « Stockage sécurisée », routage, horodatage et authentification d'abonnés (OSS).

Cette évaluation portera sur l'ensemble des sources de la bibliothèque du client lourd qui gère les fonctions de sécurité dont :

- le nom commercial est : ClearBUS Secure
- la version évaluée est: V1.1

Les principales fonctionnalités de la cible seront découpées ainsi :

- Application d'identification/authentification.
- Application de signature numérique
- Sécurité de la liaison client-serveur.
- Sureté des transferts de bout en bout.

Les fonctionnalités ci-dessous sont hors-périmètre car elles concernent la partie serveur de la solution ClearBUS:

- Vérification de l'autorité de certification et de la liste de révocation.
- Horodatage des évènements.
- Enregistrement des abonnés.

2. Description de l'environnement prévu d'utilisation du service

Un internaute désire envoyer un courrier simple ou recommandé, via la solution ClearBUS.

Il commence tout d'abord par une inscription sur l'interface de gestion des utilisateurs accessible par le Web que propose ClearBUS : www.clearbus.fr.

Ensuite, le nouvel abonné, en possession d'un certificat électronique personnel X.509v3 préalablement délivré par une autorité de confiance, génère une enveloppe numérique dont il détermine librement le contenu qui est composé de n'importe quel type de fichier informatique, avec typiquement :

- Un document principal (le courrier)
- Une liste d'annexes (les pièces jointes)

Il indique sur cette enveloppe le destinataire de son courrier et son adresse, sous un format libre, choisit le niveau de service (simple, suivi, prioritaire, recommandé, recommandé avec accusé de réception…) peut rajouter des métadonnées et enfin envoie cette enveloppe.

Le document est signé à l'aide de son certificat d'identité numérique. Cela génère une preuve d'origine conservée dans l'enveloppe.

L'enveloppe et son contenu sont acheminés par une liaison sécurisée sur les serveurs ClearBUS pour y être horodaté (preuve de dépôt), pour vérifier la validité du certificat (autorité et révocation) et pour être stocké temporairement. Le courrier et les pièces jointes ne seront extraits que lorsque l'enveloppe devra être délivré au destinataire ou supprimé (délai de retrait dépassé). L'enveloppe est conservée sans son contenu pendant une durée de un an à titre de preuve.

Si le destinataire n'est pas abonné ClearBUS, une boite aux lettres temporaire sera créée pour son enveloppe sur les serveurs ClearBUS. ClearBUS le notifiera par un moyen adapté de la réception d'un courrier numérique et l'invitera à se rendre sur le site pour télécharger l'application « CLIC » qui inclut la bibliothèque ClearBUS Secure.

Cette bibliothèque contient toutes les fonctions utilisées pour la sécurité du service ClearBUS.

Le destinataire pourra retirer son enveloppe grâce à l'application « CLIC ». S'il n'est pas abonné ou utilisateur référencé, il lui sera demandé de donner le numéro du pli, de confirmer son identité et son adresse avant délivrance du courrier.

Dans le cas d'un courrier recommandé, que le destinataire soit référencé ou non, son identité sera vérifiée à l'aide d'un certificat d'identité numérique personnel X.509v3 délivré par une autorité de confiance. La vérification a lieu au niveau des serveurs de stockage ClearBUS (soit, la partie serveur OSS) avec une identité associée au nom et prénom du destinataire.

Lors de la remise du courrier au destinataire, le serveur rajoutera sur l'enveloppe numérique un cachet avec la date de retrait grâce à son système d'horodatage.

Après remise de l'enveloppe à son destinataire, le contenu est supprimé du serveur, seule une copie de l'enveloppe vide est conservée à titre de preuve.

Les utilisateurs du service peuvent être distingués en trois profils différents :

Les utilisateurs abonnés

Profil attribué par le logiciel CLIC qui permet la génération et la réception de message. Le logiciel s'authentifie à l'aide d'un certificat X.509v3 auprès des serveurs de stockage ClearBUS (soit, la partie serveur OSS). L'utilisateur s'identifie auprès du serveur par le couple login/mot de passe.

Les utilisateurs référencés

Profil attribué par le logiciel CLIC qui permet seulement la réception de message. Le logiciel s'authentifie à l'aide d'un certificat X.509v3 auprès des serveurs de stockage ClearBUS (soit, la partie serveur OSS). L'utilisateur s'identifie auprès du serveur par le couple login/mot de passe.

Les invités.

Profil attribué par le logiciel CLIC qui permet la lecture d'un message unique à l'aide de son numéro d'enveloppe. Le logiciel s'authentifie à l'aide d'un certificat X.509v3 auprès des serveurs de stockage

ClearBUS (soit, la partie serveur OSS). Dans le cas d'un courrier simple pour un invité, des informations permettant une authentification légère du destinataire sont demandées.

3. Description des utilisateurs typiques concernés et de leur rôle dans l'utilisation du service.

Les utilisateurs typiques concernés sont les abonnés, les référencés et les invités. Du point de vue de la TOE ils ont tous le même mode d'utilisation du service.

La TOE et les utilisateurs du service peuvent être représentés par le schéma suivant :

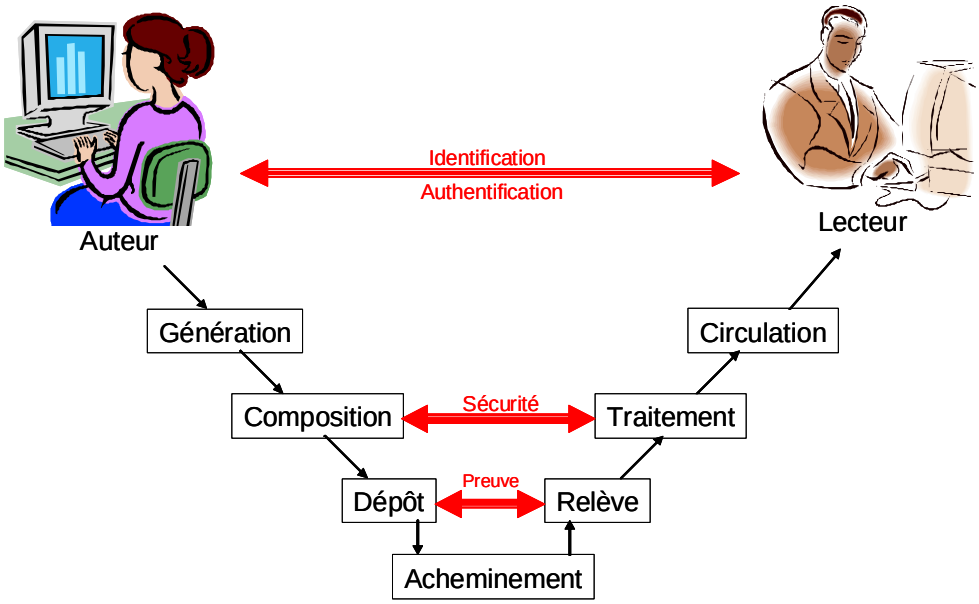


Schéma représentant l'architecture du service postal numérique

4. Description des dépendances par rapport à des matériels, des logiciels et/ou des librairies du système qui ne sont pas fourni avec le service.

Il n'y a aucune dépendance connue pour la librairie ClearBUS Secure.

5. Description des hypothèses sur l'environnement

1. PKI Fiable

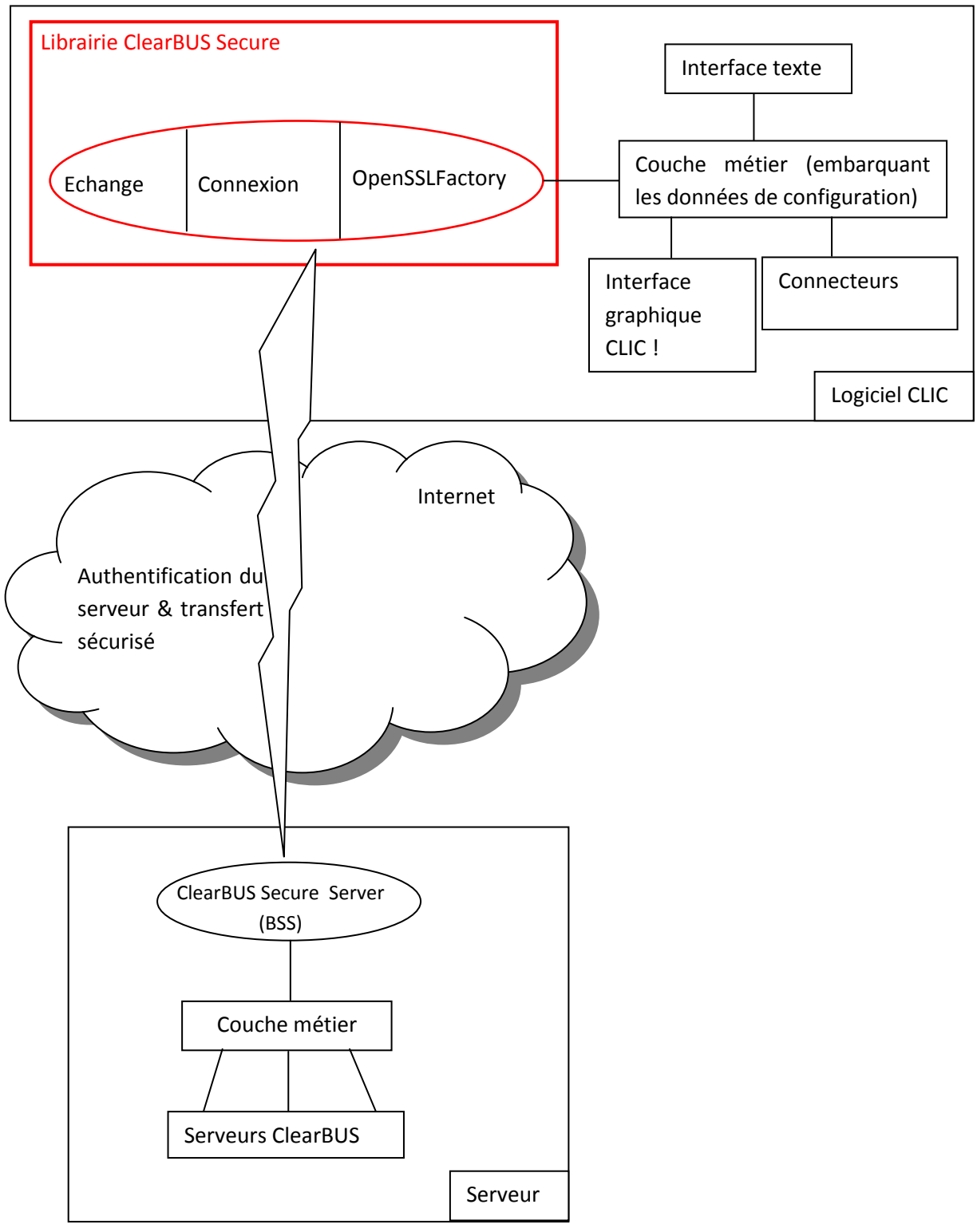
Il est considéré pour l'évaluation que la ou les PKI utilisées pour générer et gérer le cycle de vie des certificats utilisés par le service sont fiables. C'est-à-dire qu'elles ne permettent pas de divulguer ou de rendre possible la divulgation des clés privées qu'elle gère mais également que leurs CRL sont publiques et disponibles.

2. Environnement sain

Il est considéré que le poste de l'utilisateur est sain notamment grâce à un anti-virus à jour. La machine hôte qui est supposée saine et tenue à jour par rapport aux correctifs de sécurité publics. L'administrateur du poste est également considéré comme un acteur de confiance.

6. Définition du périmètre de l'évaluation.

La cible d'évaluation est constituée des sources de la librairie ClearBUS Secure et ses données de configuration, qui contribuent à fournir les services d'application de signature et de communication sécurisée.



Représentation du logiciel CLIC et la librairie ClearBUS Secure embarquée.

3. Description de l'environnement technique de fonctionnement

La librairie ClearBUS Secure étant dépendante de la couche métier, il est donc important de décrire son environnement.

Systèmes d'exploitation compatibles

La librairie ClearBUS-Secure utilise les librairies portables Qt et OpenSSL.

ClearBUS-Secure est donc compatible avec les systèmes d'exploitation pour lesquels un adaptateur (wrapper) de ces librairies est disponible, du moment que la compilation est possible sans modification des sources de ClearBUS-Secure. Ces systèmes d'exploitation devront être mis à jour avec les correctifs de sécurité effectifs.

4. Description des biens sensibles que le produit doit protéger

1. Données utilisateur protégées par la TOE

1. Les messages émis ou reçus.

L'objectif même de la solution ClearBUS est de délivrer un message d'un émetteur vers un destinataire. Le contenu du message, soit le document principal ainsi que les pièces jointes sont à protéger en confidentialité et en intégrité par l'application ClearBUS.

Les messages reçus sont stockés dans le répertoire de session de l'utilisateur système courant. Ils ne sont pas chiffrés.

2. Données confidentielles de l'utilisateur

Les données privées de l'utilisateur doivent également être protégées. Il s'agit notamment de la clé privée du certificat de l'utilisateur ainsi que la passphrase qui permet de la déchiffrer. Ces données sont à protéger en intégrité et en confidentialité par l'application ClearBUS. Le certificat de l'utilisateur même est à protéger en intégrité ainsi que sa clé publique.

Ces données utilisateurs comprennent également l'identifiant et le mot de passe utilisateur qui permettent l'identification et l'accès aux services ClearBUS. Ces donnés sont aussi à protéger en confidentialité et intégrité.

L'identifiant et le mot de passe de l'utilisateur peuvent être stockés dans le répertoire de session utilisateur, une case à cocher permet cela. Ces identifiants ne sont pas chiffrés.

5. Description des menaces

1. Agents menaçants

Les différents agents menaçants pour la TOE sont les utilisateurs illicites du service. Il s'agira :

- De personnes malveillantes ayant un accès physique ou logique sur le poste utilisateur mais sans les droits d'administrateur sur le poste.
- D'autres utilisateurs du service.
- D'attaquants externes sur le réseau.

Par hypothèse, les agents d'exploitation qui disposent d'un accès logique aux machines hébergeant les services que propose ClearBUS seront identifiés comme étant de confiance. Les menaces associées seront traitées dans un second CSPN portant sur la partie serveur (OSS).

2. Menaces

1. Lecture illicite des messages durant leur transmission et en lecture sur le poste utilisateur.

Un attaquant réussit à lire des messages qui ne lui sont pas destinés.

2. Altération des messages durant leur transmission.

Un attaquant altère le message et son enveloppe (modification) lorsque que ces derniers transitent via les réseaux à destination des serveurs de stockage de ClearBUS.

3. Suppression des messages.

Un utilisateur malveillant réussit à empêcher la transmission correcte des informations aux serveurs de ClearBUS.

4. Altération des données de l'utilisateur

Un attaquant réussit à modifier les données d'un utilisateur autorisé. Cela comprend son certificat, la clé publique et la clé privée de son certificat mais également son identifiant et mot de passe pour l'accès aux services de ClearBUS.

5. Accès aux données confidentielles de l'utilisateur

Un attaquant accède aux données confidentielles d'un utilisateur autorisé. Il s'agit de sa clé privée, de la passphrase du certificat ainsi que son identifiant et mot de passe pour l'accès aux services de ClearBUS.

6. Déni de service

Un utilisateur malveillant altère le logiciel CLIC et ses données de configuration afin d'empêcher le bon fonctionnement de la librairie ClearBUS Secure.

6. Description des fonctions de sécurité de la librairie.

1. Authentification du serveur

Il s'agit de l'authentification entre la librairie ClearBUS Secure via le client CLIC et la plateforme de distribution de courrier. CLIC vérifie l'authenticité du serveur par certificat X509v3 via un tunnel SSL garantissant ainsi aussi la confidentialité et l'intégrité des données transmises au serveur.

2. Protection lors de la transmission de données.

Toutes les communications entre le client et les serveurs de stockage de ClearBUS sont protégées en confidentialité et en intégrité via le protocole SSLv3/TLS1.0 . Les données émises du client CLIC vers la plateforme de distribution de courrier sont ainsi acheminées de façon sécurisée.

3. Signature électronique

Le message généré par l'utilisateur est signé avec son certificat personnel. La clé de son certificat lui est demandée au moment de la signature de façon à s'assurer de l'identité de l'auteur (non-répudiation) ainsi que de l'intégrité du message.

7. Argumentaires des fonctions de sécurité.

Menaces / Fonction de sécurité	Authentifi-cation Serveur	Authentifi-cation utilisateur	Chiffrement des données pendant la transmission	Signature électroni-que des messages	Reçu de dépôt (Via le WS)
Lecture illicite des messages par un autre utilisateur du service		X			
Altération illicite des messages par un autre utilisateur du service		X			
Envoi illicite des messages par un autre utilisateur du service		X			
Suppression illicite des messages par un autre utilisateur du service		X			
Lecture des données confidentielles d'un autre utilisateur du service		X			
Lecture illicite des messages par un internaute malveillant		X	X	X	
Altération des messages par un internaute malveillant		X	X	X	
Suppression des messages par un internaute malveillant lors de la transmission					X
Suppression des messages par un internaute malveillant		X			
Lecture des données confidentielles par un internaute malveillant		X			
Envoi illicite des messages par un internaute malveillant		X			

Menaces / Fonction de sécurité	Authentifi-cation Serveur	Authentifi-cation utilisateur	Chiffrement des données pendant la transmission	Signature électroni-que des messages	Reçu de dépôt (Via le WS)
Lecture illicite des messages par un utilisateur malveillant du poste		X			
Altération des messages par un utilisateur malveillant du poste		X			
Suppression des messages par un utilisateur malveillant du poste		X			
Déni de service provoqué par un utilisateur malveillant du poste (altération de la configuration du logiciel CLIC ou du logiciel en lui-même)	-	-	-	-	-
Lecture des données confidentielles par un utilisateur malveillant du poste		X			
Envoi illicite de messages par un utilisateur malveillant du poste		X			

8. Sigles

Sigle	Désignation
CSPN	Certification de Sécurité Premier Niveau
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
PKI	Public Key Infrastructure
SSH	Secure Shell
SSL	Secure Sockets Layer

Glossaire

Certificat électronique

Un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.

Certificat électronique qualifié

Un certificat électronique répondant aux exigences définies à l'article 6 du Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique.

Courrier :

C'est le fichier informatique principal de l'enveloppe.

Document :

Désigne l'ensemble constitué du courrier ainsi que des pièces jointes et des métadonnées optionnelles qui sont véhiculé par le système de courrier numérique à l'intérieur d'une enveloppe.

Données de création de signature électronique

Les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique.

Données de vérification de signature électronique

Les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique.

Enveloppe :

C'est l'objet qui transite dans le système créée par l'émetteur et reçue par le destinataire. L'enveloppe contient le document, les preuves, les désignations de l'émetteur et du destinataire, et les différents états qui ont permis son routage.

Signataire

Toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique.

Signature électronique

Donnée sous forme électronique, jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification pour ces données électroniques.

Signature électronique sécurisée

Une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;
- être créé par des moyens que le signataire puisse garder sous son contrôle exclusif.
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

Signature électronique présumée fiable

Une signature mettant en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et reposant sur l'utilisation d'un certificat électronique qualifié.

On parle aussi de signature électronique qualifiée.

Signature numérique

Résultat de l'opération cryptographique de signature sur des données à signer et utilisant une clé privée de signature.

Système de création de signature

Le système complet qui permet la création d'une signature électronique et qui inclut l'application de création de signature et le dispositif de création de signature.