Sécuriser les échanges numériques

Hassan BEZZAZI, Maître de conférences en informatique à l'Université de Lille 2.
Grégory BEAUVAIS, Docteur en droit public, Ingénieur de recherche à l'Université de Lille 2.
Fabienne MOLURI, Avocate au Barreau de Lille.

Février 2013 - UNJF

Légende

 Référence Bibliographique

 Référence générale

 Jurispridence

 Texte de loi

Table des matières

Avant-propos

I

A. Fiche descriptive

1. Informations générales

Domaine

Maîtriser le cycle de vie d'un document juridique

Titre du module

Sécuriser les échanges numériques

Auteur

- Hassan BEZZAZI, Maître de conférences en informatique à l'Université de Lille 2.
- Grégory BEAUVAIS, Docteur en droit public, Ingénieur de recherche à l'Université de Lille 2.
- Fabienne MOLURI, Avocate au Barreau de Lille.

Code référentiel

D 4-3

Durée

10 heures

2. Prérequis

L'objet de ces notes et de sensibiliser le professionnel du droit au risque informatique dans son métier et de lui fournir quelques techniques pour réduire ce risque. De fait, la plupart de ces techniques, qu'elles appellent à la technologie ou non, sont utiles aussi bien pour l'entreprise que pour le particulier.

3. Objectifs

L'objet de ces notes et de sensibiliser le professionnel du droit au risque

informatique dans son métier et de lui fournir quelques techniques pour réduire ce risque. De fait, la plupart de ces techniques qu'elles appellent à la technologie ou non sont utiles aussi bien pour l'entreprise que pour le particulier.

4. Mots clés

Systèmes d'information, sécurité, échanges numériques, attaques informatiques, man in the middle, usurpation, ingenierie sociale, chiffrement, importabilité, traçabilité, auditabilité, sécurité organisationnelle et juridique, sécurité physique, sécurité de l'exploitation, sécurité logique, sécurité applicative, sécurité des télécommunications.

Savoir

II

A. Les objectifs

Le savoir-faire visé dans cette formation peut se résumer autour des points suivants :

1. Protéger les accès par des mots de passes convenablement choisis et changer les mots de passe par défaut. Verrouiller et protéger les données.
2. Réaliser des sauvegardes systématiques chiffrées. Un fichier peut être accidentellement supprimé ou infecté par un virus. Il est utile de savoir récupérer un fichier, parfois même quand il a été supprimé, et de savoir supprimer définitivement un fichier.
3. Installer un antivirus et le tenir à jour, un pare-feu, un anti-spyware ainsi que les dernières mises à jour du système d'exploitation et des logiciels installés qui peuvent corriger des failles de sécurité.
4. Être conscient des dangers de certains emails et naviguer sur le Web avec prudence en sachant reconnaître les situations où il y a risque d'hameçonnage.
5. Être conscient des métadonnées que les documents peuvent contenir.
6. S'assurer que seules les personnes autorisées ont accès aux données via une authentification des utilisateurs par login et mot de passe ou par certificats. Sécuriser les accès distant à l'aide du protocole SSL ou en mettant en œuvre un réseau virtuel privé VPN. Se familiariser avec l'utilisation des certificats, en particulier lors d'échange de courriels. Être capable de choisir et de mettre en œuvre les solutions cryptographiques adéquates pour sécuriser son environnement de travail.
7. Assurer une protection physique des serveurs et désactiver les ports pour les mémoires amovibles.
8. Protéger les connexions sans fil. La protection est double, elle concerne la

confidentialité des échanges numériques mais aussi l'accès même au réseau par une personne qui cherche un accès gratuit à Internet.

9. Mettre en œuvre une politique de sécurité informatique écrite accompagnée d'audit et sensibiliser le personnel aux attaques relevant de l'ingénierie sociale. Pour être pleinement opposable et référencée en cas de doute la politique de sécurité doit être clairement rédigée dans la charte informatique. Une politique de sécurité doit se faire avec les utilisateurs : ils doivent comprendre cette politique et respecter ses règles.
   Exemple :
   Les recommandations dans le choix des mots de passe et le recours aux téléchargements.
10. Être conscient que l'utilisation d'un certain nombre de mécanismes et d'outils pour la sécurisation des échanges numériques tels que la signature électronique et la pratique de la dématérialisation des procédures sont des réalités accompagnée de nombreux avantages. Être à même de justifier ces réalités par le gain en temps, en productivité et le niveau élevé de sécurité qu'elles assurent quand les risques ont bien été identifiés sur la base d'exemples concrets issus du monde des métiers du droit et de l'administration publique en évoquant notamment le secret professionnel, le secret des correspondances privées et la protection des données à caractère personnel.
    Il va sans dire que pour traiter convenablementles points ci-dessus, certaines connaissances sont utiles sinon nécessaires sur les réseaux, les enjeux de la cryptographie et le crime informatique, plus particulièrement la cybercriminalité. Ceci peut être classé dans les *« savoirs associés »* que tout bon enseignement professionnel doit intégrer à son programme.

Attention

D'une façon générale la sécurité informatique d'une organisation est assurée par des personnes compétentes qui maîtrisent les points ci-dessus et qui s'appuient sur des référentiels et des critères nationaux ou internationaux.

Mis ensemble, ces points reflètent une approche globale à la sécurité informatique. Toutefois certaines structures petites ou moyennes n'ont pas un service informatique interne pour veiller sur la sécurité informatique. Quand bien même ce service existe en externe, les points ci-dessus montrent que le facteur humain est essentiel et sa défaillance en la matière peut faire écrouler toutes les protections aussi solides soient elles.

B. Les menaces sur les systèmes d'information

Un système d'information se définit à l'aide de trois composantes :

- la composante humaine,
- l'infrastructure informatique et
- les données.
- La composante humaine comprend les informaticiens et les utilisateurs
- L'infrastructure informatique comprend le matériel, le logiciel et les réseaux de communication.

Important

Le terme « *système informatique* » souvent rencontré désigne tout système dont le fonctionnement fait appel, d'une façon ou d'une autre, à l'électricité et destiné à élaborer, traiter, stocker, acheminer ou présenter de l'information.

- Les données peuvent être des données relatives aux clients, au personnel, aux dossiers, etc.

Différents types de menaces pèsent sur les systèmes d'information. Dés lors, la sécurité informatique d'un système d'information doit être considérée en se rapportant à chacune de ces composantes :

- sécurité organisationnelle et juridique
- sécurité physique
- sécurité de l'exploitation
- sécurité logique
- sécurité applicative
- sécurité des télécommunications

C. La sécurisation des échanges numériques

Pour appréhender globalement le contenu de ces notes, nous précisons ce que doit couvrir le concept « *sécurité des échanges numériques* ».

Important

Pour nous, il s'agit de sécurité des données numériques transmises via un canal de communication réputé non sûr.

Typiquement, ce canal est le réseau internet filaire ou sans fil mais d'autres canaux existent et doivent être pris en compte. Les réseaux de télécommunication fixe ou mobile servent à l'échange de données numériques (données, voix, images). Mais, il faut le rappeler, un moyen d'échange numérique des plus courants consiste à transporter physiquement les données géographiquement d'un point à un autre à l'aide de supports aussi diverses que l'ordinateur ou le téléphone portable, la clé USB ou même dans certains cas tout simplement le papier. Le papier peut en effet constituer un moyen d'échange de données numériques après que celles-ci soient imprimées, leur recouvrement après transport étant le résultat d'une simple numérisation à l'aide d'un scanner et d'un logiciel de reconnaissance optique de caractères. Ces canaux et les supports qu'ils utilisent ne sont pas sûrs dans le sens où les données qu'ils font circuler ou qu'ils stockent peuvent être interceptées ou extraites par des personnes non autorisées.

Après avoir décrit le canal de communication, venons en maintenant au terme de sécurité des données numériques auquel nous pouvons nous restreindre même si souvent il est question de sécuriser le canal de communication car la sécurisation du canal n'a de sens que pour la sécurisation des données qui le traversent. En fait la sécurité des données est au cœur de tout dispositif de sécurité des échanges numériques puisque la sécurisation des données *« sur place »* est nécessaire à la sécurisation des échanges. Ainsi sécuriser son document sur le portable ou l'accès à sa session par un mot de passe sont des procédures basiques à considérer dans le cadre de la sécurisation des échanges numériques aussi bien pour le particulier que pour le professionnel. La sécurité des données numériques est nécessaire pour prévenir de la malveillance, des accidents ou des erreurs qui peuvent nuire au système d'information.

La malveillance informatique a pour objet :

- l'entrave au bon fonctionnement d'un système informatique ou
- l'utilisation non autorisée des ressources informatiques ou
- l'accès non autorisé à des données ayant pour conséquence une atteinte à la vie privée, au secret des correspondances privées ou au secret professionnel.

Elle regroupe un certain nombre d'attaques qui seront présentées plus loin et peut constituer un crime informatique ou un cybercrime quand l'infraction est commise via le réseau internet. Deux types d'infraction sont distingués dans le guide du traitement judiciaire de la cybercriminalité (cf. Guide du traitement judiciaire de la cybercriminalité) du ministère de la justice :

- les infractions où l'informatique est le moyen de commission d'un crime ou d'un délit telles que celles relatives aux atteintes à la personnalité, les infractions à la loi sur la presse, les infractions contre les biens, l'atteinte à la propriété intellectuelle par exemple.
- les infractions où l'informatique est l'objet même du crime ou du délit et qui ont été prévues dans des textes spécifiques telles que la loi Godfrain ou la loi informatique et libertés.

Pour protéger son système informatique, le professionnel a généralement recours aux services d'une société spécialisée mais la sécurité informatique n'incombe pas aux seuls spécialistes de l'informatique. Et c'est pour cela que des compétences de base dans la sécurité informatique comme l'installation d'un antivirus et les précautions de sauvegarde sont requises dans le référentiel du c2i niveau 1. Dans le cadre du référentiel c2i métiers du droit il s'agit de compléter et de développer

ces compétences en les rapprochant au contexte des métiers du droits. L'utilisation de la cryptographie à l'aide de certificats ou l'utilisation d'un pare-feu pour surveiller le trafic sur son réseau viennent par exemple compléter les compétences du c2i niveau 1.

Enfin il est utile de situer l'item du référentiel correspondant à ces notes par rapport aux autres items. Plusieurs notions abordées dans ces notes se retrouvent dans d'autres compétences du référentiel où elles doivent être traitées de manière plus approfondie.

Il s'agit de :

- Respecter le secret professionnel.
- Maitriser les droits des personnes : la protection de la vie privée et des données à caractère personnel, le droit au secret des correspondances.
- Maitriser les échanges numériques entre acteurs judiciaires ou juridiques et les services offerts aux citoyens
- Archiver l'information : préserver l'intégrité des contenus ; assurer la stabilité du contenu informationnel dans le temps.
- Prévenir des actes de cybercriminalité dans un contexte professionnel : face aux attaques externes ; face aux comportements internes.

D. Les attaques informatiques

1. Introduction

Même si les attaques informatiques relèvent plus de la cybercriminalité, un domaine prévu dans le référentiel du c2i métiers du droit, il est utile d'en rappeler ici les principales attaques auxquelles peuvent être exposés les professionnels du droit assorties d'exemples et de quelques mesures de protection.

Une attaque informatique est une action qui vise à exploiter les failles éventuelles d'un système d'information pour un accès frauduleux au système informatique. Le but peut être

- de voler des données personnelles ou des documents classés secrets
- ou encore d'entraver le bon fonctionnement du système ou l'utiliser pour mener d'autres attaques.

Une attaque peut être directe ou indirecte.

Attention

Elle est indirecte quand le système attaqué est utilisé pour mener d'autre attaques ou activités illégales telles que le téléchargement ou la mise à disposition de contenus protégés par la propriété intellectuelle.

C'est alors l'IP du système attaqué qui est directement mise en cause, d'où la nécessité de protéger son système. Les attaques informatiques quand elles sont commises via l'Internet relèvent de la cybercriminalité (voir le module correspondant).

2. La recherche des mots de passe

La première tâche d'un pirate qui cherche à s'introduire dans un système informatique est la recherche du mot de passe qui le protège. Plusieurs procédures peuvent mener à la découverte d'un mot de passe:

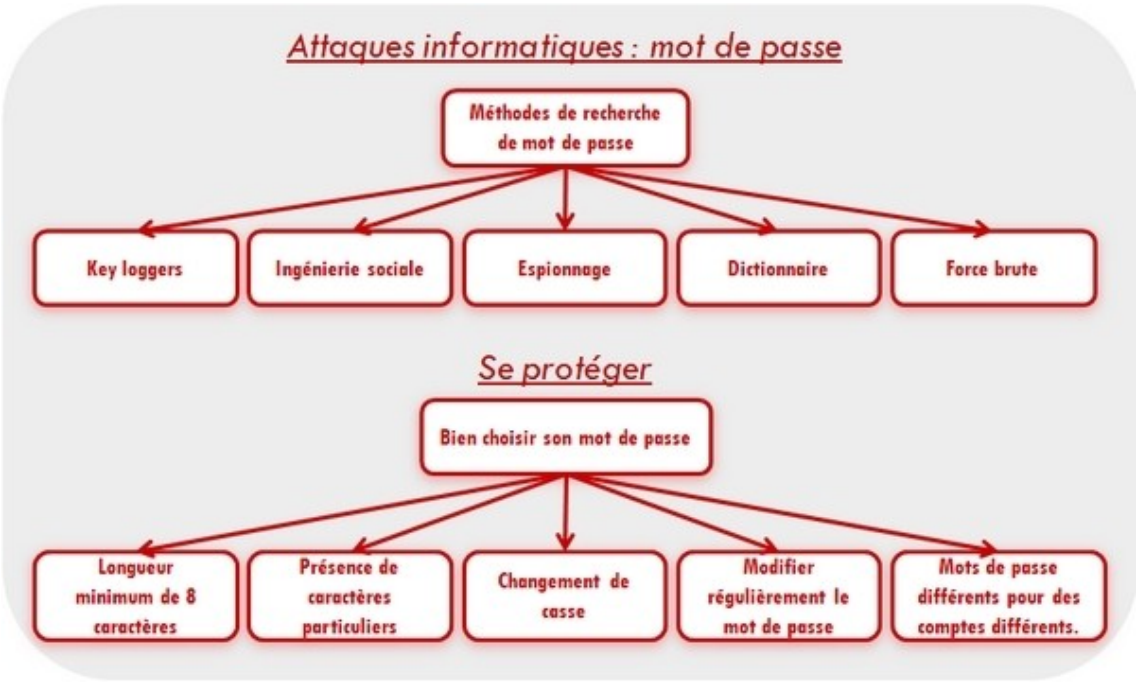
- des enregistreurs de frappes (keyloggers),
- l'ingénierie sociale ou l'espionnage
- mais aussi des techniques utilisant des dictionnaires et la force brute.

Les parades contre ces attaques relèvent plus de la bonne conduite.

Conseils, trucs et astuces

Bien choisir les mots de passe :

- Une longueur minimale de 8 caractères
- La présence de caractères particuliers
- Un changement de casse (minuscules et majuscules)
- Modifier régulièrement le mot de passe
- Mots de passe différents pour des comptes différents



3. Attaque de l'homme du milieu (Man in the Middle)

La plupart des attaques de type *HDM* consistent à écouter le réseau à l'aide d'un logiciel appelé sniffer.

Exemple

Les attaques dites « *par rejeu* ».

Le pirate intercepte les paquets et les réutilise même si le contenu est chiffré.

Exemple

Le rejeu d'un mot de passe chiffré.

Le vol de sessions est un autre exemple d'attaque HDM.

Pour mener à bien son attaque, le pirate doit en général avoir le contrôle sur un élément de la route empruntée par le trafic de la session. Ainsi le pirate pourra se faire passer pour l'un des interlocuteurs de la session après que l'authentification des deux parties ait eu lieu.

4. Attaques par déni de service

Attention

Une attaque DoS (Denial of Service ou déni de service) vise à entraver le bon fonctionnement d'un système informatique pour rendre l'organisation incapable de rendre le service attendu. Lors de cette attaque l'accès au système devient impossible.

Remarque

Cela peut nuire à la fois à la réputation de l'organisation et éventuellement aussi à son chiffre d'affaire.

Exemple

Messagerie, Moteurs de recherche, Sites Marchands.

5. Attaque par usurpation

Attention

Dans cette attaque l'adresse IP source des paquets constituants une requête envoyée au système informatique est remplacée par une adresse IP autorisée à traverser le pare-feu protégeant le système.

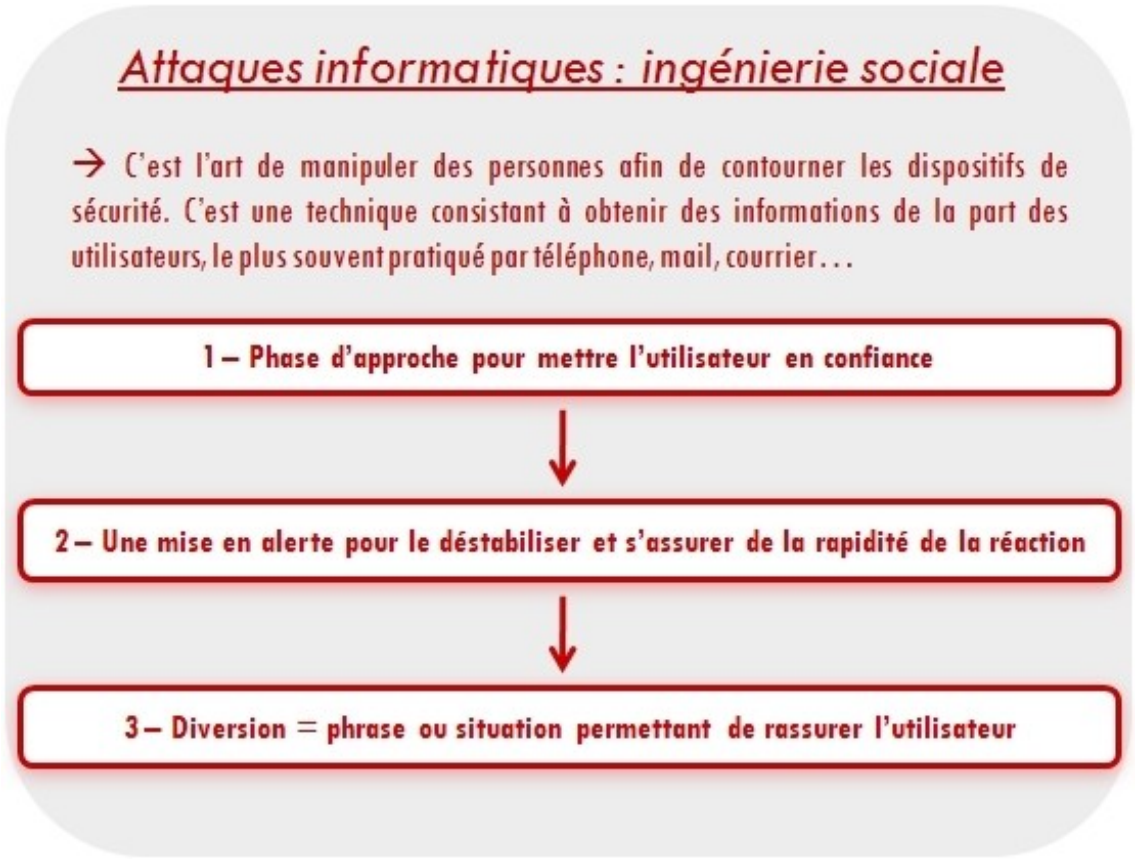
Les parades consistent essentiellement à se protéger contre un quelconque sniffer en chiffrant le contenu. Par ailleurs il existe des outils permettant de détecter un sniffer sur le réseau. Un « *scanner de vulnérabilité* » est un utilitaire qui permet de réaliser un audit de sécurité d'un réseau en effectuant un balayage des ports ouverts sur une machine donnée ou sur le réseau. Le balayage se fait en envoyant des requêtes au système pour déterminer les services actifs.

6. Ingénierie sociale

Important

L'ingénierie sociale désigne l'ensemble des techniques visant à obtenir des informations pouvant servir à mener un acte frauduleux.

L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne autorisée à recevoir l'information. Parmi les techniques : la mise en confiance ou l'alerte. L'hameçonnage (phising) est une forme d'ingénierie sociale.



E. Les enjeux de la cryptographie

1. Introduction

La cryptographie est devenue aujourd'hui presque banalisée et beaucoup de monde l'utilise sans le savoir.

Exemple

Les chaînes de télévision payantes, les cartes bancaires et les moyens de communication téléphonique en sont des exemples de tous les jours.

Conseils, trucs et astuces

Le recours à la cryptographie pour sécuriser les échanges et créer la confiance a lieu à l'entreprise, à l'administration tout comme chez le particulier.

L'objet de ce chapitre est d'apprendre à mettre en œuvre quelques techniques et à utiliser des outils pour la sécurisation des données et des échanges numériques.

2. Chiffrement des fichiers

Remarque

Le caractère mobile de l'ordinateur portable et des mémoires amovibles (disque dur externe, carte mémoire ou clé USB) les expose au risque de perte ou de vol plus que les appareils fixes.

Le danger encouru lors d'un tel incident est d'autant plus grand que certains documents revêtent un caractère confidentiel notamment dans un cadre professionnel.

Certaines mesures de protections sont souvent immédiatement disponibles dans le système d'exploitation et les logiciels bureautiques, à savoir :

- La protection des sessions par mot clé ;
- Le chiffrement des dossiers et des fichiers dans les menus contextuels ;
- La protection d'un document bureautique par mot de passe.

Remarque

Notons que les protections par mot de passe sont toujours accompagnées par le chiffrement des dossiers ou fichiers protégés.

Les fonctionnalités ci-dessus pouvant varier d'un système d'exploitation à un autre, nous recommandons le recours à un logiciel libre multi-plateforme tel que le logiciel TrueCrypt téléchargeable sur le *site officiel*[1] et dont nous résumons les fonctionnalités principales ici :

- Création de disques virtuels
- Chiffrement d'une partition entière ou d'une mémoire amovible, éventuellement du système d'exploitation
- Le chiffrement est automatique, rapide et transparent.
- La possibilité d'opposer un déni plausible à un adversaire qui vous oblige de divulguer le mot de passe protégeant le système ou le volume chiffré grâce à un deuxième mot de passe qui fera ressortir un autre contenu non confidentiel.

3. Chiffrement des transmissions

Un texte qui circule sur Internet passe par plusieurs supports sur lesquels les sujets concernés n'ont pas de contrôle direct. La confidentialité d'un texte clair est en jeu car il peut être intercepté et lu par un tiers. La solution consiste alors à chiffrer le texte pour qu'il ne soit lu que par les seules personnes autorisées. Le chiffrement peut être symétrique ou asymétrique.

a) La notion de chiffrement des données

1 - http://www.truecrypt.org/

Important

Le chiffrement est un procédé cryptographique permettant de rendre la compréhension d'un document impossible en l'absence d'une clé de déchiffrement.

Ce procédé n'est pas apparu avec le développement des TIC. La science qui le définit est la cryptologie. La cryptologie a longtemps été considérée comme une arme militaire utilisée exclusivement par l'État. Le développement du commerce électronique -qui nécessite un système de paiement sécurisé- a entraîné une libéralisation progressive de la cryptologie à partir de la fin des années 1990. Diverses lois et textes réglementaires sont intervenus pour établir un cadre juridique de l'utilisation des moyens cryptographiques ; cadre qui a connu un dernier assouplissement avec la loi n° 2004- précitée, telle qu'elle a été modifiée en 2008.

Il existe deux types principaux de chiffrement :

Chiffrement symétrique -ou chiffrement à clé secrète	Chiffrement asymétrique -ou chiffrement à clé publique
Utilise la même clé pour chiffrer et déchiffrer	Emploie deux clés différentes : une clé publique qui sert au chiffrement, et une clé privée servant à déchiffrer.

Le chiffrement à clé secrète consiste à appliquer un algorithme sur les données à chiffrer à l'aide de la clé partagée. Le principal inconvénient du chiffrement symétrique est qu'il impose un canal d'échange de clés suffisamment sécurisé. Il existe ainsi un système basé sur une clé privée générée aléatoirement et utilisée une seule fois avant d'être détruite.

L'inconvénient du canal sécurisé ne se retrouve pas dans un chiffrement à clé publique.

Conseils, trucs et astuces

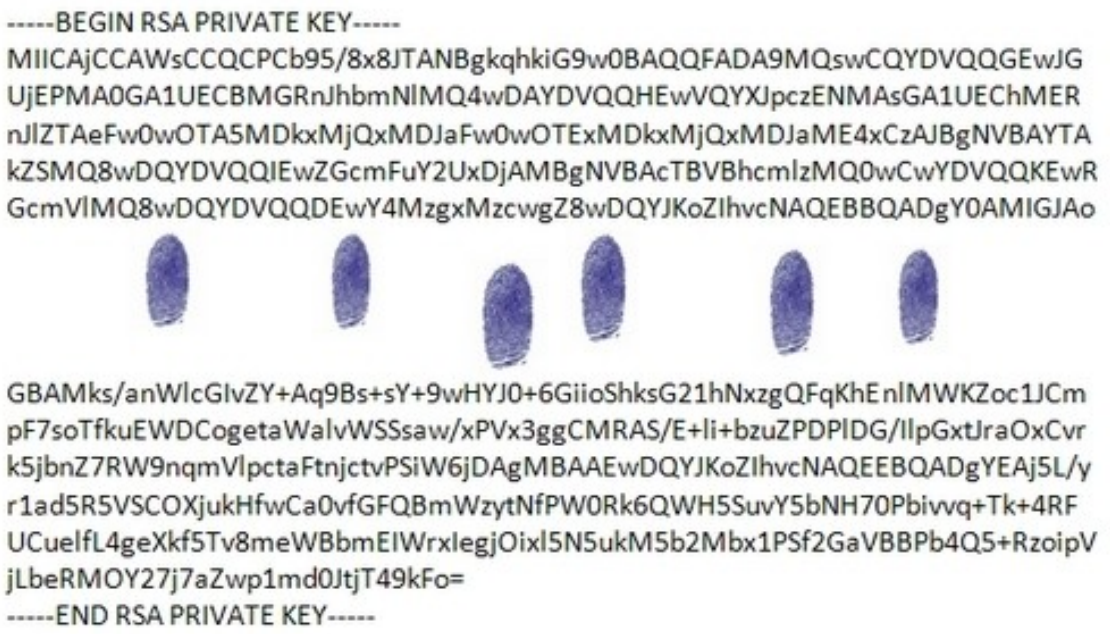
Chaque message sera chiffré au moyen de la clé publique du destinataire qui sera le seul en mesure de le déchiffrer grâce à sa clé privée.

Si l'écueil de la transmission de la clé de déchiffrement n'existe plus, la difficulté dans un chiffrement asymétrique est d'être certain que la clé publique récupérée provient de la personne à qui l'on fait parvenir une information chiffrée. La longueur des clés est calculée en bits. Plus ce chiffre est important, plus faible est le risque de voir la clé découverte par un tiers.

Appropriation des concepts :

- Le chiffrement symétrique
- La force brute
- Exemples d'algorithmes : AES, RC4
- Le chiffrement asymétrique
- Une paire de clés : une clé privée et une clé publique
- Exemples d'algorithmes : RSA, ELG, DSA
- Inconvénients et avantages des chiffrements symétrique et asymétrique
- Cryptosystème mixte.

Exemple



Remarque

Une clé publique a une structure similaire.

La sécurité informatique repose sur des principes considérés comme des critères: La disponibilité, la confidentialité, l'intégrité et la non répudiation. Ce dernier critère implique des notions telles que :

- l'imputabilité,
- la traçabilité ou encore
- l'auditabilité.

Attention

Sous certaines conditions, ces propriétés sont assurées par la signature électronique qui met en œuvre le chiffrement asymétrique.

4. La signature électronique

Important

Un message est signé quand il est accompagné de son empreinte chiffrée à l'aide de la clé privée de l'émetteur. L'empreinte numérique met en œuvre une fonction de hachage.

Le hachage d'un fichier consiste à générer à partir de celui-ci un message plus court appelé empreinte pour ce fichier et qui change au moindre changement dans le fichier. Le hachage est une fonction à sens unique : L'empreinte d'un fichier ne permet pas sa reconstitution.

Exemple

Algorithmes de hachage courants : MD5, SHA, DSA.

Attention

Selon le droit européen, une signature électronique est *« une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification »*.

La loi française de transposition du 13 mars 2000 insère l'*article 1316-4 dans le Code civil*[2] qui confère à la signature électronique la même valeur juridique qu'une signature manuscrite : *« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État »*. Cette définition ne prend pas en compte les aspects techniques qui sont laissés à l'appréciation du pouvoir réglementaire jugé plus à même de réagir face à *« la fugacité de l'état de la technique »*.

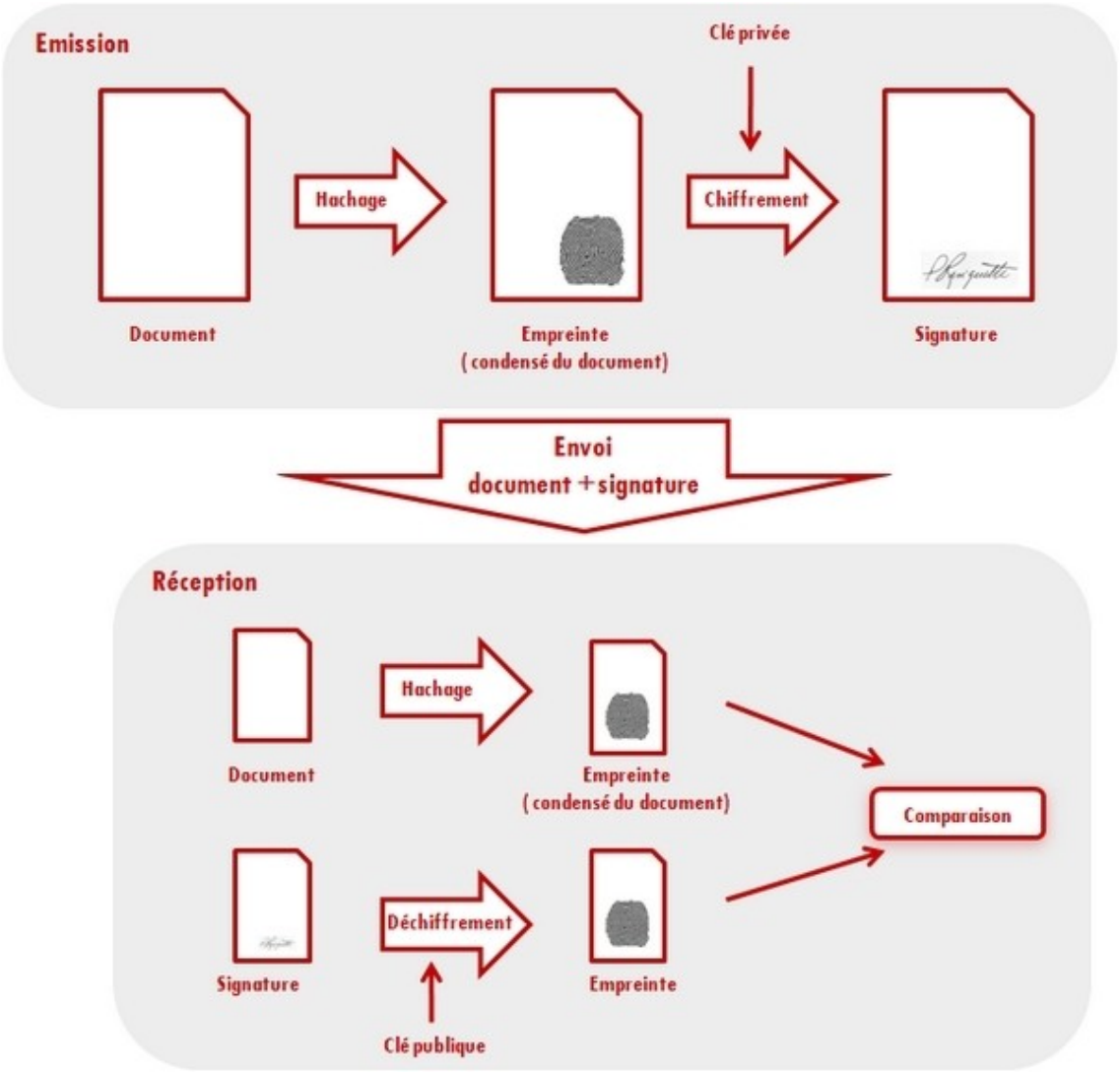
Le décret du 30 mars 2001 donne une définition du signataire, et distingue la signature électronique simple de la signature électronique sécurisée. La signature sera présumée juridiquement fiable si elle est sécurisée au sens du décret, ou avancée au sens de la directive de 1999 ; les deux expressions étant synonymes. Si elle n'a pas de force probante, la signature électronique simple peut néanmoins valoir commencement de preuve par écrit. Le décret distingue deux types de certificats qui correspondent aux deux catégories de signatures électroniques : le certificat électronique simple et le certificat électronique dit qualifié lorsqu'il contient certains éléments.

La signature électronique s'appuie sur une infrastructure de gestion de clés publiques (IGC) qui désigne à la fois un cadre organisationnel et une infrastructure technique. La technologie employée est celle de la cryptographie asymétrique. Le dispositif de création de la signature va émettre deux clés générées par un algorithme mathématique : une clé privée -qui est connue du seul signataire- et une clé publique -qui est accessible par tous. Le dispositif permet le chiffrement des données, c'est-à-dire leur transformation dans le but de les rendre inintelligibles. La clé privée -qui est personnelle- permet de signer électroniquement un document. Elle est stockée sur un support physique comme un disque dur d'ordinateur, une carte à puce ou une clé électronique. Son utilisation peut être combinée avec l'emploi d'un mot de passe, ou d'un système de reconnaissance des caractéristiques biométriques du signataire afin d'accroître le niveau de sécurisation. Lorsque l'on signe électroniquement un message, la signature électronique est créée grâce à la clé privée correspondant à la clé publique contenue dans le certificat. La personne qui a signé son message avec sa clé privée sera donc authentifiée, et ne pourra pas nier l'avoir envoyé.

Remarque

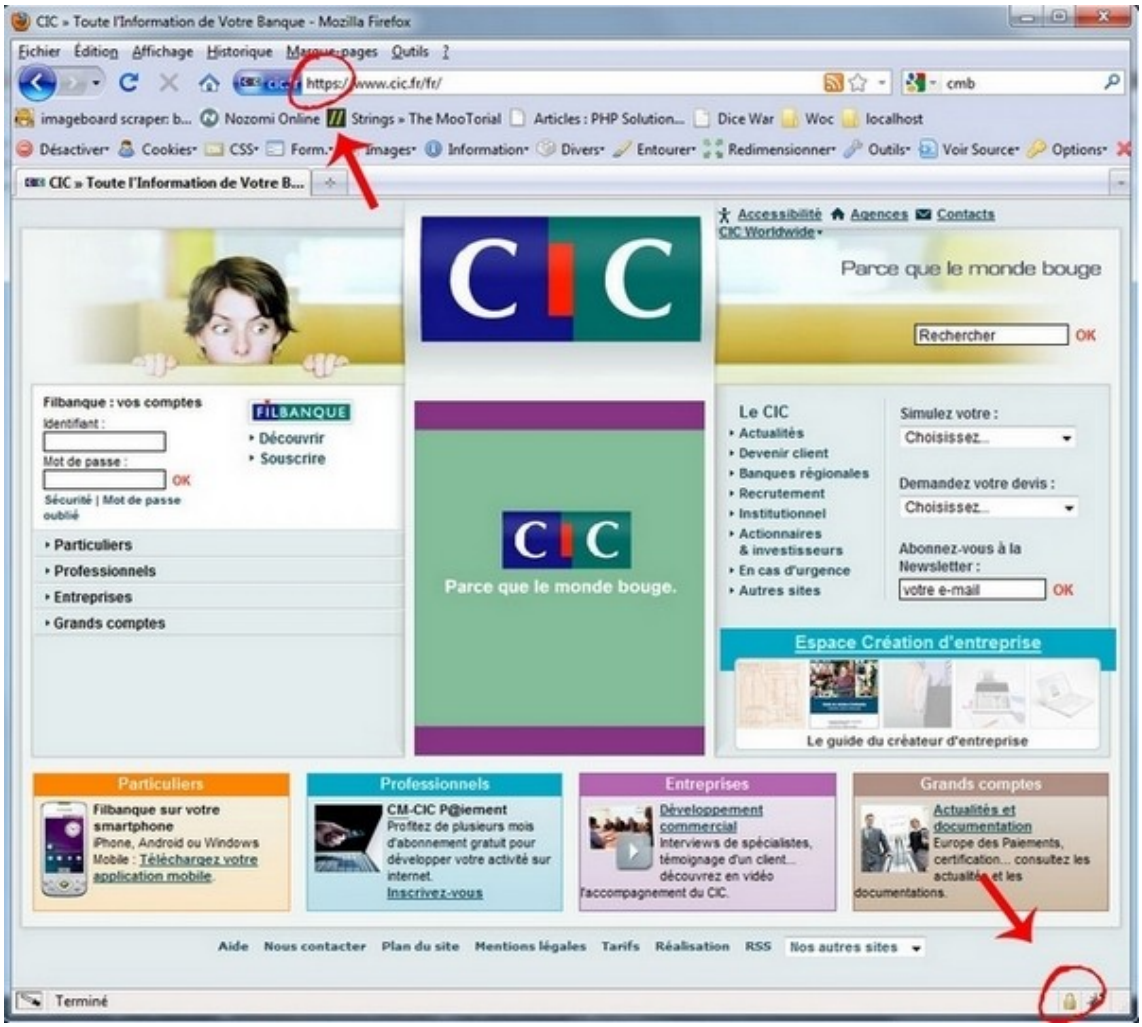
La signature électronique ne saurait se confondre avec une signature numérisée, c'est-à dire avec une signature scannée ou photographiée, puisqu'elle ne permet pas d'assurer le lien avec l'acte auquel elle s'attache ni l'intégrité du message.

2 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=6EE42E5AF6A84310F49239CDD9132537.tpdjo07v_2?idArticle=LEGIARTI000006437841&cidTexte=LEGITEXT000006070721&dateTexte=20100507



5. Les certificats SSL

Pour les transactions sécurisées sur Internet, le protocole SSL est souvent utilisé (https et cadenas). Le dialogue SSL a lieu entre le navigateur et le serveur web.



Les trois propriétés requises pour une communication sécurisée :

- L'authentification : celle du serveur est obligatoire mais pas celle du client
- La confidentialité : assurée par des chiffrements symétriques
- L'intégrité : Hachage des données

6. Les autorités de certification

L'autorité de certification atteste de l'identité du détenteur des clés en lui délivrant un certificat numérique après qu'elle s'en soit assuré de l'identité à l'aide de moyens conventionnels (courrier, téléphone, pièces d'identités...).

Pour que le certificat puisse être validé il faut notamment que :

- Sa date d'expiration soit valide,
- Le nom du serveur soit correct,
- Le CA figure dans la liste des autorités dans lesquelles le client a confiance,
- Le certificat soit authentifié sur la base de son empreinte et de la clé publique du CA.

Passée cette étape, un canal sécurisé est mis en place entre les deux machines.

7. L'infrastructure de gestion de clés publiques

Important

Une infrastructure de gestion de clés publiques (IGC) est un ensemble de moyens matériels, de logiciels, et de procédures humaines, mis en oeuvre par des textes juridiques et des pratiques, dans le but de gérer le cycle de vie des certificats électroniques basés sur la cryptographie asymétrique.

Cette définition s'inspire des travaux menés par l'Internet Engineering Task Force (IETF). Ce groupe informel élabore des RFC, c'est-à-dire des documents appelés à devenir des standards de l'Internet.

Selon l'IETF, une IGC est composée de cinq entités lui permettant de mettre en oeuvre ses compétences :

- les autorités de certification,
- d'enregistrement,
- de dépôt, et
- de séquestre,
- ainsi que l'entité finale.

D'autres entités, ou personnes physiques, interagissent avec l'IGC, comme le responsable du certificat du serveur informatique, du mandataire de certification, de l'utilisateur du certificat, et enfin, de toute personne autorisée. Les compétences de l'IGC doivent favoriser la confiance des usagers dans les téléservices publics. Depuis la libéralisation de la cryptologie, l'IGC peut être assurée par des prestataires privés selon une procédure formalisée. Les téléservices publics étant des prestations d'intérêt général, la constitution de leur IGC doit laisser une place prééminente à la personne publique.

Remarque

La définition de l'IGC montre l'importance des normes et recommandations techniques, ainsi que des documents référents en la matière. Tout comme son utilisation, la création du certificat est dominée par la normativité technique.

8. Les compétences d'une infrastructure de gestion de clés publiques

Si le rôle principal d'une IGC est de produire des certificats électroniques, elle a également en charge des activités connexes, en rapport avec la sécurité informatique.

a) La création de certificats électroniques

La création des certificats électroniques des téléservices publics se conforme au standard X.509 établi par l'Union internationale des télécommunications (UIT). C'est l'autorité de certification (AC) qui peut créer et attribuer des certificats à la demande d'un ou plusieurs utilisateurs. Le droit français parle de prestataire de services de certification électronique (PSCE) pour désigner l'AC.

Exemple

Il s'agit d'un tiers de confiance situé entre le demandeur du certificat -une administration par exemple- et son utilisateur -l'usager.

La demande de certificat est adressée, sous la forme d'un fichier numérique appelé CSR710, à une autorité d'enregistrement (AE) qui l'examine. L'AE a la responsabilité des tâches administratives relatives à la gestion des demandeurs et des porteurs de certificats, comme le contrôle de l'identité des porteurs de certificat. Les différents niveaux de ce contrôle entraînent la création de quatre types de certificats. Les certificats de classe 1 sont obtenus sans vérification d'identité, à l'aide d'un courriel. La classe 2 désigne les certificats qui font l'objet d'un contrôle des informations à caractère personnel fournies par le demandeur.

Exemple

Il peut s'agir, par exemple, du numéro d'identifiant fiscal qui permet au contribuable de déclarer en ligne ses impôts sur le revenu.

Les certificats de classe 3 donnent lieu à une vérification physique des informations données et à un contrôle face à face. La classe 3+ est identique à la précédente, sauf que le certificat est stocké sur un support physique. Les certificats de classe 3 et 3+ sont nécessaires dans le cadre de la dématérialisation des procédures de contrôle de légalité et des circuits comptables et financiers alors que le certificat de classe 2 est admis pour l'achat public dématérialisé.

Les quatre classes entraînent quatre degrés de confiance des destinataires dans le certificat : plus le contrôle est élevé, plus on a l'assurance que le certificat est utilisé par la bonne personne. Si la demande est retenue par l'AE, elle est transmise à l'AC qui vérifie sa validité, et qui la signe avec sa propre clé privée. La signature a pour conséquence de transformer la CSR en un certificat électronique. Le certificat est ensuite publié par l'autorité de dépôt (AD) qui gère également la liste des certificats révoqués.

Conseils, trucs et astuces

Un certificat peut être révoqué à tout moment, durant sa période de validité. La période de validité est variable ; s'agissant du certificat servant à la déclaration de l'impôt sur le revenu par exemple, sa durée est de trois ans. À l'expiration du délai de validité, le certificat peut être renouvelé, soit automatiquement, soit à la demande de son porteur. Les raisons d'une révocation sont multiples et peuvent tenir à la divulgation ou à la perte de la clé privée, ainsi qu'à l'existence d'informations fausses contenues dans le certificat. L'AC révoque alors le certificat en cause et transmet l'information au service de publication. L'utilisateur d'un certificat doit vérifier qu'un certificat qu'il entend utiliser n'a pas été révoqué.

b) Les services connexes

Attention

Outre la délivrance de certificats électroniques, une IGC offre des services complémentaires qui favorisent la confiance des usagers : l'horodatage et l'archivage.

La possibilité de dater avec exactitude un acte unilatéral ou un contrat est primordiale pour la sécurité juridique des individus.

Exemple

La date d'une décision administrative qui ouvre le délai de recours contentieux.

Attention

La dématérialisation des échanges ne modifie pas l'impératif de datation.

Exemple

La procédure de déclaration des impôts sur le revenu doit ainsi disposer d'un système permettant de dater avec certitude les déclarations. À défaut, les usagers risqueraient de devoir des pénalités à l'administration fiscale, ce qui aurait pour conséquence de porter atteinte à leur confiance dans cette téléprocédure. Le système permettant de dater avec certitude les échanges dématérialisés est l'horodatage.

Ce système *« permet d'attester qu'une donnée existe à un instant donné »*.

Exemple

Pour cela, il convient d'associer une représentation sans équivoque d'une donnée, par exemple une valeur de hachage associée à un identifiant d'algorithme de hachage, à un instant dans le temps. La garantie de cette association est fournie au moyen d'une contremarque de temps qui est une structure signée.

Il peut être réalisé selon différentes solutions techniques.

L'horodatage est assuré par l'autorité d'horodatage (AH). Il s'agit d'*« une composante de l'IGC qui délivre et signe des contremarques de temps sur des données qui lui sont présentées »*.

Attention

L'AH est neutre par rapport aux opérations techniques et elle ne vérifie pas l'identité des personnes demandant l'horodatage.

Ce tiers de confiance peut également assumer les fonctions d'archivage électronique. Il peut être utile dans le cadre d'un contentieux de prouver l'existence des pièces relatives à la certification. Cette possibilité est offerte grâce à l'archivage électronique de ces données.

Attention

Les archives peuvent être définies comme *« l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité »*.

La notion d'archives s'applique donc quelle que soit la nature du document concerné. Malgré des travaux de normalisation portant sur l'intégrité et la fiabilité des documents archivés, et de quelques dispositions juridiques figurant dans des textes concernant la certification au sens large, il n'y a pas de cadre juridique spécifique pour les archives électroniques.

La directive européenne du 13 décembre 1999 dispose ainsi que les prestataires de services doivent *« enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par voie électronique »* et *« utiliser des systèmes fiables pour stocker les certificats »*.

Remarque

La directive ne donne cependant pas de précision sur la fiabilité exigée pour le stockage des certificats.

Le décret du 30 mars 2001 est tout aussi vague en énonçant qu'un PSCE doit *« conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique »*. C'est donc aux référentiels qu'incombe la définition des précisions techniques relatives à l'archivage électronique. La matière constitue un défi juridique et technique majeur, dans la mesure où il faut que l'acte archivé conserve sa valeur juridique dans le temps.

Attention

Le référentiel parle d'ailleurs d'archivage électronique sécurisé. Il s'agit de *« l'ensemble des modalités de conservation et de gestion des archives électroniques ayant une valeur juridique lors de leur établissement ; cet archivage garantissant la valeur juridique jusqu'au terme du délai durant lequel des droits y afférents peuvent exister »*.

9. Cadre juridique

Le Code civil (*article 1316-4*[3]) accorde la même valeur juridique (probante) pour la signature électronique que pour la signature manuscrite sous réserve que le procédé de signature électronique soit fiable. Le décret 2001-272 relatif à la signature électronique définit les conditions dans lesquelles une signature électronique est présumée fiable. Parmi ces conditions, l'autorité de certification doit répondre aux exigences de l'arrêté du 26 juillet 2004 relatif à la qualification des prestataires de services de certification électronique. Cette qualification est certifiée par un organisme certificateur indépendant.

Respect des lois nationales en matière d'exportation, d'utilisation ou de détention des logiciels de cryptographie (pays exerçant un contrôle au motif de sécurité intérieure : Chine, Russie et autres Cryptography and Liberty 2000)

« l'écrit sur support électronique a la même force probante que l'écrit sur support papier » (Article 1316-4 du Code civil).

La loi du 13 mars 2000 pose les conditions essentielles que doit remplir un écrit électronique pour être admis à titre de preuve au même titre qu'un écrit papier :

- Permettre l'identification du signataire ;
- Être créé dans des conditions à en garantir l'intégrité ;
- Être conservé dans des conditions à en garantir l'intégrité.

3 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=6EE42E5AF6A84310F49239CDD9132537.tpdjo07v_2?idArticle=LEGIARTI000006437841&cidTexte=LEGITEXT000006070721&dateTexte=20100507

Remarque

La signature électronique devient une preuve pré constituée : il y a renversement de la charge de la preuve en défaveur de celui qui répudie sa signature.

« La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée... » (Article 2 du décret 2001-272 du 30 mars 2001).

10. L'exemple du Journal officiel électronique authentifié

Depuis l'ordonnance n° 2004-164 du 20 février 2004, relative aux modalités et effets de la publication des lois et de certains actes administratifs, le Journal officiel électronique authentifié a la même valeur légale que le Journal officiel sous forme papier.

Tous les textes publiés au Journal officiel, sauf ceux concernant l'état et la nationalité des personnes, sont consultables sur l'*Internet*[4].

4 - http://www.journal-officiel.gouv.fr/association/

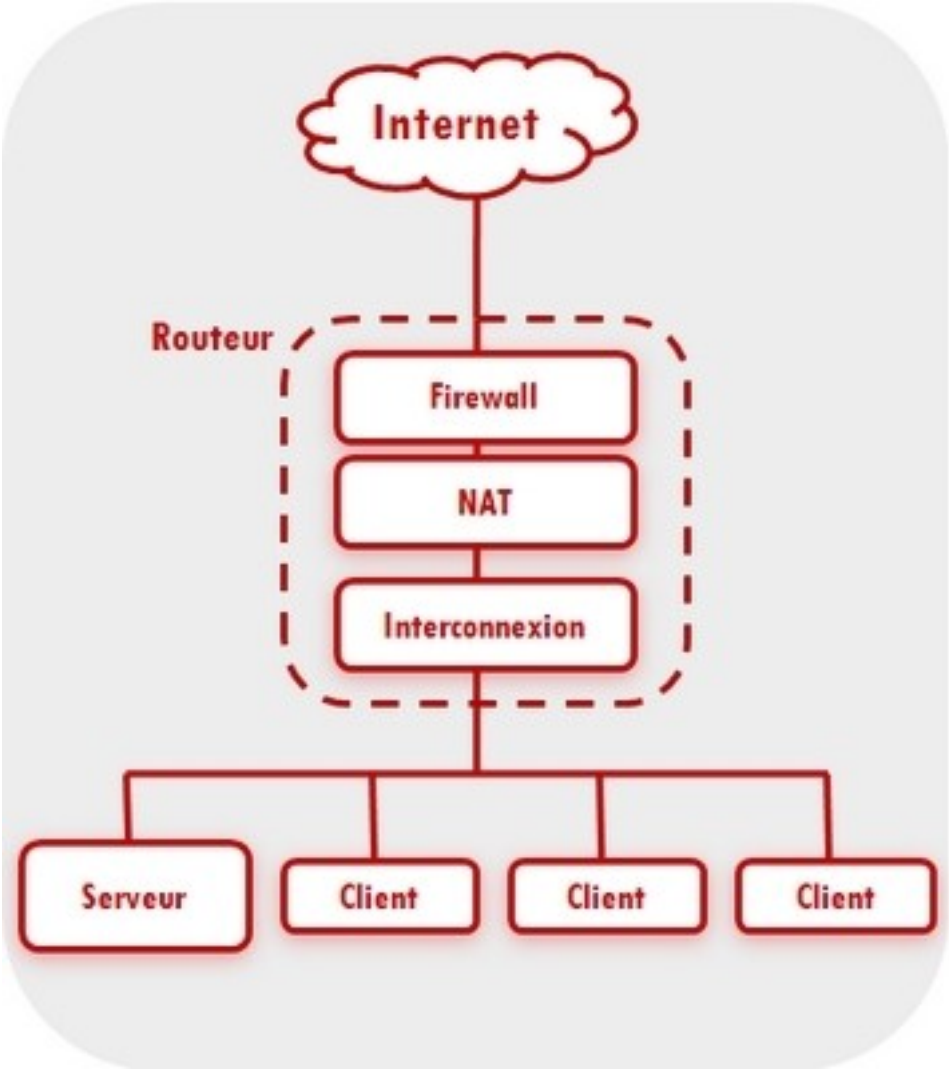
Conseils, trucs et astuces

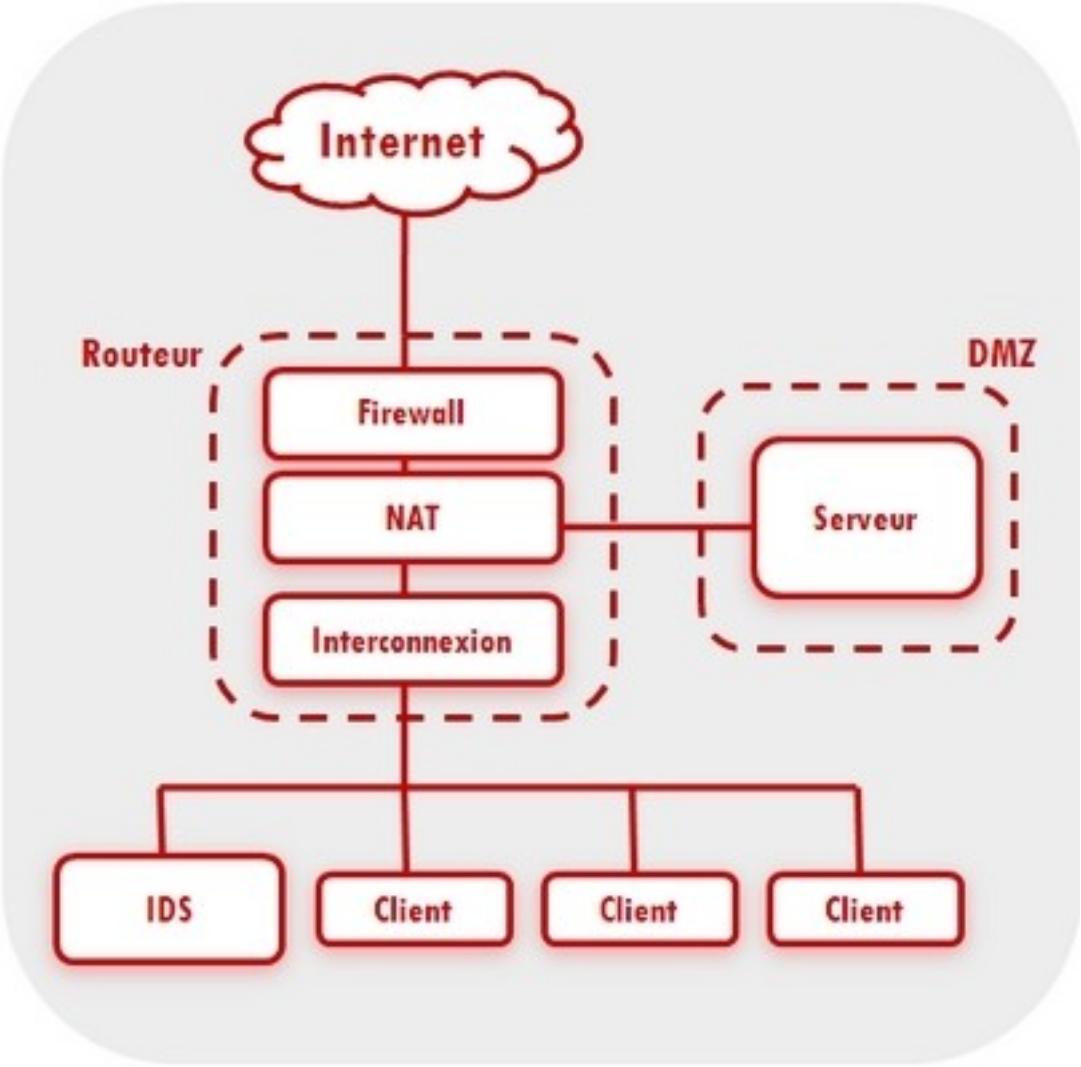
L'authenticité des textes du Journal officiel est attesté par le certificat racine de la Direction des Journaux officiels. C'est la différence avec les textes consultables sur legifrance.fr dont l'authenticité n'est pas assurée.

F. Les réseaux et leur protection

1. Introduction

Il est utile pour une meilleure appréhension de la sécurisation des réseaux de rappeler schématiquement les deux configurations réseau les plus courantes.





La première configuration est presque commune à tous les foyers et petites et moyennes entreprise. La seconde configuration est plus dépouillée que la première au niveau sécurité en mettant en œuvre une zone démilitarisée (DMZ) et un système de détection d'intrusion (IDS). Le système NAT installé généralement sur les routeurs permet de relier un réseau local au réseau Internet en gérant une table de correspondances entre les adresses privées et les adresses publiques. Ceci induit une première protection dans la mesure ou les adresses privées ne sont pas visibles sur Internet car seule l'adresse IP du routeur est publique et si aucune installation de serveur n'est prévue, une connexion avec l'extérieur ne peut être initialisée que par un ordinateur du réseau privé. Dans le cas ou des applications de type serveur doivent être installées, un certain nombre de réglages doivent être effectués au niveau du système NAT. Le recours à une DMZ permet de cantonner ces applications sur des machines ouvertes au trafic depuis et vers le réseau interne et le réseau externe.

2. Les réseaux sans fil

En général les architectures de réseaux ci-dessus sont complétées par le déploiement de réseaux sans fil (Wi-Fi) qui apporte plus de flexibilité de par la

mobilité qu'il procure. La protection du réseau dans sa partie sans fil est double, elle concerne la confidentialité des échanges numériques mais aussi l'accès même au réseau par une personne qui cherche un accès gratuit à Internet. Le risque dans ce dernier cas étant une utilisation de la connexion à des fins illégales, par exemple pour mener des attaques informatiques, pour un téléchargement illégal ou pour mener une compagne de spam. Dans cette situation, la responsabilité du titulaire de la connexion Internet est engagée, c'est son adresse IP qui est utilisée.

La difficulté de confiner les ondes radio propagées par le déploiement d'un réseau Wi-Fi induit des problèmes de sécurité spécifiques du fait notamment de la facilité par laquelle une personne non autorisée pourrait écouter le trafic ou brouiller les communications même en dehors de l'enceinte où le réseau est déployé.

Remarque

De même un réseau Wi-Fi peut être installé discrètement à l'aide d'un point d'accès branché sur une prise de réseau et permettre à une personne malintentionnée d'écouter le réseau quelques pas plus loin.

La protection met en œuvre des solutions de sécurisation :

- Le protocole WPA ou WPA2 pour l'authentification et le chiffrement des données.
- Le filtrage des adresses MAC permet de limiter l'accès au réseau à un certain nombre de machines.
- Dissimulation de l'identifiant du réseau sans fil, le SSID.
- Limiter la zone de couverture du réseau sans fil en réglant la puissance d'émission de la borne d'accès.

Conseils, trucs et astuces

Sécuriser son réseau sans fil : la configuration et donc la sécurisation de celui-ci ce fait via une interface généralement accessible en tapant *« http://192.168.1.1 »* dans la barre d'adresse de votre navigateur.

3. Le pare-feu

Important

Le pare-feu est un logiciel qui peut être installé sur un ordinateur personnel ou, dans le cas d'un réseau local, sur un ordinateur dédié pour surveiller, filtrer et contrôler les connexions entrantes et sortantes de l'ordinateur ou du réseau.

En général, les routeurs incluent un minifirewall.

Exemple

Prenons le cas d'un ordinateur personnel, un bon réglage du firewall permettra de détecter rapidement un programme suspect du type troyen qui tente d'établir une connexion sortante. En effet, une connexion, pour qu'elle puisse être établie doit être explicitement autorisée par l'utilisateur.

Pour une application sollicitant l'accès au réseau et dans laquelle l'utilisateur à confiance, il peut créer une règle qui l'y autorise pour éviter que l'autorisation ne lui soit demandée à chaque accès. Ceci est le cas des applications comme le navigateur ou le logiciel de messagerie.

Ainsi des règles de trafic précises peuvent être définies pour les applications connues. Pour le reste des applications installées sur l'ordinateur, la règle par défaut devrait être la demande expresse de l'autorisation et sur la base de la confiance accordée à l'application, une règle d'autorisation ou d'interdiction pourra être créée.

Une règle qui interdirait par défaut au reste des applications l'accès au réseau pourrait concerner certains accès légitimes telles que les mises à jour de certaines applications qui ne sont pas dédiées spécialement pour l'accès au réseau, les antivirus par exemple. A l'inverse, une règle qui autoriserait par défaut l'accès au réseau à ces applications laisserait la porte grande ouverte aux programmes malicieux éventuels installés sur l'ordinateur.

4. Les réseaux privés virtuels

Les réseaux privés virtuels constituent une solution à moindre coût pour mettre en œuvre un réseau privé. Au lieu de relier les différentes ressources matérielles du réseau par des lignes physiques spécialisées, cette solution mettra à profit leur connexion à Internet pour former un réseau privé virtuel totalement sécurisé. Différents sites d'une organisation pourront ainsi mettre en commun via un RPV leurs réseaux privés au sein d'un même réseau global privé. De même cette solution permet au personnel itinérant de travailler à distance sur son ordinateur personnel comme si il était dans son entreprise et bénéficier ainsi de manière totalement transparente des ressources matérielles et logicielles du réseau privé, par exemple récupérer des dossiers ou les déposer en toute sécurité.

Après authentification des parties, le trafic est encapsulé à l'intérieur de paquets IP en utilisant une connexion tunnel. Deux types de protocoles sont à la base du fonctionnement des VPN, le protocole PPTP et le protocole L2TP couplé avec le protocole IPsec. Ce dernier protocole est souvent utilisée dans les échanges devant être sécurisés en attendant la généralisation d'un autre protocole dont en parle souvent et qui s'impose lentement pour remplacer IPv4, le protocole IPv6.

IPv6 améliore IPv4 au niveau de :

- L'adressage: plus étendu et hiérarchisé
- L'allocation dynamique de bande passante pour le support d'applications multimédia (visio conférence)

Le déploiement à grande échelle de IPv6 rencontre des problèmes d'ordre logistique et économique.

La solution IPsec qui permet donc de garantir la confidentialité et l'authentification des données transférées par IP est compatible IPv4 et IPv6.

Les universités font elles aussi appel à la solution VPN pour permettre aux enseignants et aux étudiants d'utiliser des ressources telles que les bases de données juridiques mise à disposition par le SCD.

Exemple

JurisClasseur ou Lamy.

La configuration de son poste en tant que client VPN ou même en tant que serveur VPN est relativement facile quand tous les paramétrés tels que les protocoles utilisés et l'adresse du serveur sont connus.

G. Les échanges entre professionnels

1. Introduction

La dématérialisation des échanges entre professionnels est avantageuse à plusieurs titres :

- pour des raisons d'économie (papier et affranchissement),
- pour des raisons d'efficacité (rapidité des échanges),
- pour des raisons de sécurité (authentification, confidentialité et intégrité)

Dans une organisation, les échanges numériques avec l'extérieur sont de deux sortes :

- les échanges avec le personnel dans le cadre du télétravail ou d'activités itinérantes pour une meilleure réactivité,
- les échanges avec des partenaires dans le cadre de la dématérialisation des procédures.

Exemple

Le réseau PLANETE pour les notaires, le RPVA pour les avocats et les téléprocédures dans l'administration publique en sont des exemples.

Dans les deux cas, au cœur du dispositif se trouve la notion de réseau privé virtuel RPV ou VPN et la notion d'authentification décrites plus haut pour assurer la confidentialité des échanges. De plus la mise en œuvre de l'authentification nécessite une clé USB qui retient le certificat électronique qui vaut signature électronique du professionnel.

Conseils, trucs et astuces

En cas de perte, déclarer la perte et la faire refaire immédiatement. Les exemples qui suivent se situent plus dans le second cas en raison de leur caractère spécifique, le premier cas étant plus commun.

2. E-BARREAU

Le Conseil National des Barreaux (CNB) a mis en place le RPVA (Réseau Privé Virtuel Avocat) et la plateforme e-barreau. Les avocats ont alors la possibilité de :

- Suivre l'état de leurs procédures Accéder au greffe de leur TGI
- Communiquer par messagerie dans un cadre sécurisé avec les avocats et les greffiers en matière pénale.

A partir de 2010 le RPVA devrait permettre l'échange entre avocats et magistrats et greffiers des cours d'appels. Il est prévu que la procédure devant la cour d'appel soit faite uniquement par voie électronique.

Requis: Accès haut débit, abonnement au barreau pack

Sécurité : L'accès au portail e-barreau nécessite l'installation d'un boitier RSA pour sécuriser le réseau et l'authentification de l'avocat à l'aide de sa clé USB cryptographique délivrée par le barreau auquel il appartient et qui lui permettra aussi de signer électroniquement ses documents. Cette clé contient le certificat électronique personnel de l'avocat, un certificat de classe 3 plus. Elle doit être insérée dans l'ordinateur à chaque accès à e-barreau et y rester durant toute la connexion. Elle permet outre l'archivage électronique des actes d'avocat, l'accès à un certain nombre de services qui font éviter à l'avocat les déplacement et les appels téléphoniques tels que :

- e-greffe pour l'inscription à une audience de référé et la consultation des dossiers en cours devant les chambres civiles ainsi que les décisions rendues.
- e-Carpa pour effectuer un bon nombre d'opérations de mouvements de fonds pour le compte des clients de l'avocat.

En 2009, les chiffres donnés sur le site officiel du CNB révèlent que 122 barreaux sont équipés, que plus de 1 500 cabinets sont raccordés et 3 400 avocats utilisateurs.

Exemple

30% des avocats du barreau de Lille sont abonnés.

3. L'e-notariat

Attention

La gestion de l'office notarial met en jeu plusieurs acteurs générant ainsi des flux internes et externes.

La dématérialisation de ces flux permet, comme dans le cas de l'administration électronique, de gagner au niveau de la productivité, de l'économie, de la sécurité mais aussi une meilleure adéquation aux normes et conventions. Elle a aussi pour conséquence une mise à jour des compétences que, soit dit en passant, le c2i métiers du droit devrait faciliter en amont pour l'ensemble des métiers du droit. Elle doit cependant s'attacher à minimiser le changement matériel et logiciel dans sa mise en œuvre.

PLANETE : C'est un support technique intermédiaire pour les échanges avec l'environnement extérieur du notariat.

Réalisations s'appuyant sur PLANETE :

- Virements électronique au lieu du chèque
- Réquisitions et dépôt électronique
- Dématérialisation des actes, de déclarations...
- Échange Crédits et succession.

Important

PLANETE est un réseau de routage à valeur ajoutée :

- Échange de messages
- Vérification et transformation
- Vérification de la SE
- Fournit des services aux ssii (web services)

Architecture à base de composants/web service.

Comme composants : Référentiel (schéma XML, données de base...) , accès aux annuaires.

La carte Real du notariat contient les certificats d'authentification, de signature et de chiffrement ainsi que le certificat de l'Autorité de Certification.

L'article de presse ci-dessous témoigne de l'importance de la sécurité des échanges numérique, notamment quand il s'agit d'actes authentiques. En guise d'exercice, le lecteur est invité à repérer dans le texte toutes les mesures de sécurité auxquelles a recours la mise en œuvre de la dématérialisation des actes notariés.

4. L'huissier de justice

Les Huissiers de Justice ont entamé leur mutation technologique dès 1975, en équipant une dizaine d'études de systèmes informatiques.

À partir de 1985, les premiers réseaux UNIX sont installés, et au début des années 90, l'informatisation de la Profession est quasiment généralisée.

En 1995, les Huissiers de Justice s'investissent dans l'Échange de Données Informatisées (EDI), et participent au projet EDIJustice, sous l'égide du Ministère de la Justice.

En 2001, les Huissiers de Justice créent l'ADEC, un organisme chargé de la conception, la réalisation, la maintenance, l'administration et la promotion de tous les moyens d'échanges électroniques, produits et services, entre les études et leurs différents partenaires.

L'ADEC met immédiatement en place un « *Centre Serveur* » EDI.

Actuellement, 70 % des études d'Huissiers de Justice pratiquent les échanges de données informatisées avec les grands donneurs d'ordres institutionnels que sont les URSSAF, les Organismes Conventionnés, les sociétés de crédit telles que la Sofinco, Cetelem, Franfinance, Cofinoga, Finaref, et le Trésor public pour le recouvrement des amendes.

En 2008, près de 3 millions de dossiers sont ouverts en EDI, et le volume des flux dématérialisés et des échanges bancaires est très important.

Dès le mois d'octobre 1999, une vingtaine d'études teste la signature électronique en partenariat avec La Poste et Sagem.

En Mars 2005, 100 Autorités d'Enregistrement (une par département) sont installées, en vue de la délivrance de certificats de clé publique à l'ensemble de la Profession.

La CNHJ a choisi l'Opérateur de Services de e-Confiance CertEurope pour son expérience dans la conception et la mise en œuvre d'applications de signature électronique pour les professions réglementées : avocats, greffiers des tribunaux et experts comptables, par exemple.

Dès la parution du décret du 10 août 2005, relatif à l'acte authentique sur support électronique de l'Huissier de Justice, la Profession lance le cahier des charges du projet Minutier Central.

Le 2 décembre 2008 – 35 jours après les Notaires - les Huissiers de Justice déposent officiellement au Minutier Central leur premier acte authentique sur support électronique.

Attention

Les Huissiers de Justice disposent de la Signature Électronique Sécurisée, emportant présomption de fiabilité, conforme aux dispositions de l'article 1316-4 la Loi du 13 mars 2000 et du décret du 30 mars 2001.

En décembre 2008, les Huissiers de Justice obtiennent le Prix de l'Innovation décerné par la Fédération Nationale des Tiers de Confiance, pour leur service DepoMail : un message électronique dont l'envoi est constaté dans un procès-verbal, et dont le contenu peut être fourni au Juge en cas de litige.

Ce service permet de conférer une forte valeur ajoutée au *« mail »*, qui devient ainsi un nouvel élément de preuve dans le cadre d'un procès.

DepoMail – et le service AuthentiDoc, destiné à protéger les créations de l'esprit – sont accessibles par un portail www.jedepose.com.

Fort de leur expérience en matière d'EDI, les Huissiers de Justice achèvent la mise en place du projet d'injonction de payer dématérialisée avec les Tribunaux d'Instance (LIP-TI/IP Web), en partenariat avec TRANSJURIS de la Caisse des Dépôts.

Par ailleurs, la Profession participe activement aux travaux de sécurisation de l'écrit électronique dans l'espace et dans le temps (signature électronique et archivage électronique), au sein d'organismes Nationaux (Afnor) et Internationaux (ISO).

C'est ainsi qu'elle a contribué à l'élaboration des normes sur *« la preuve électronique »*, l'horodatage, l'archivage électronique (norme Z42-013), et qu'elle intervient au sein de la délégation Française de l'ISO sur l'archivage électronique (TC171).

En savoir plus: Extrait du site officiel de CertEurope

La Chambre Nationale des Huissiers de Justice délivre des certificats C@rteurope à ses membres. (3800 membres). En assurant cette fonction, elle devient par là même, Autorité d'Enregistrement. Elle permet donc à ses membres, d'utiliser des certificats électroniques lors des communications électroniques inter-huissiers de justice, ainsi que lors des échanges électroniques entre chaque huissier de justice et ses donneurs d'ordre.

Prochainement, le certificat permettra la signature des actes authentiques sur support électronique.

Dans un second temps, la CNHJ souhaite, à travers l'ADEC, permettre aux huissiers de justice de distribuer des dispositifs de signature électronique à leurs donneurs d'ordre. Dans cette perspective, la CNHJ souhaite faire évoluer son Intranet afin d'offrir à ses membres de nombreux services en ligne au travers de l'ADEC.

Afin de contrôler l'accès à ces services et pour sécuriser les communications électroniques, la CNHJ souhaite utiliser des certificats électroniques :

- Pour authentifier les Huissiers de Justice,
- Pour permettre aux Huissiers de Justice de signer des documents

En vue de répondre à ces attentes, CertEurope propose :

- la fourniture de certificats électroniques sur support électronique assurant l'authentification forte des Huissiers de Justice, et leur permettant de signer les actes authentiques
- des formations. En tant qu'organisme de formation habilité, CertEurope s'engage à concevoir et à réaliser des séances de formation des Autorités d'enregistrement pour la délivrance des certificats électroniques.
- Un service d'assistance téléphonique

Important

Nous remercions Maître Alain Bobant, Huissier de justice, Président de la fédération nationale des tiers de confiance pour le contenu de ce paragraphe.

5. L'échange de Données Informatisées

L'Échange de Données Informatisées (EDI) constitue le plus ancien des protocoles pour l'échange des données entre systèmes informatiques bien avant le standard XML et les transmissions internet sécurisées. La sécurisation des échanges y est assurée sur la base des accords d'interchange qui sont des accords entre partenaires qui définissent les conditions juridiques et techniques d'utilisation de l'EDI.

L'EDI peut se pratiquer via un Réseau à Valeur Ajoutée (protocole x400) ou directement via Internet (protocole AS2) sans passer par un RVA et avec les même garanties de sécurité liées à la confidentialité, l'authentification et l'intégrité. La transmission des données est asynchrone avec un RVA (Réseau à Valeur Ajoutée) où un prestataire intermédiaire met à la disposition de chaque partenaire abonné une boîte aux lettres électronique. Cette solution offre l'avantage de la responsabilité juridique du RVA en plus de sa valeur ajoutée: le chiffrement des données transitant par le RVA garantit la confidentialité et l'intégrité des dossiers traités de même que l'authentification des parties et la conservation et le restitution des messages qui y transitent garantissent la non répudiation.

Attention

Le recours à l'EDI est très présent dans les activités BtoB du secteur industriel et commercial pour la la facturation, la passation des commandes et les avis d'expédition par exemple.

Chez les professionnels du droit, ce sont incontestablement les huissiers qui ont le plus recours à l'EDI pour faire face au nombre important des dossiers de recouvrement. Le client de l'étude pourra saisir ses dossiers de recouvrement directement sur internet via la plateforme e-recouvrement en se connectant au Centre Serveur. C'est l'ADEC (Association Droit Electronique et Communication), une association sans but lucratif, regroupant des Huissiers de Justice qui administre le Centre Serveur appelé SIREES : Serveur Inter-actif pour le Recouvrement et les Echanges Electroniques Sécurisés. Il permet la mise en œuvre de trois types d'échanges:

- échanges électroniques de type EDI,
- échanges de documents dématérialisés (InterAct),
- échanges inter profession du droit (Transjuris).

EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) : c'est l'ensemble des normes et recommandations internationales concernant pour l'EDI.

H. La dématérialisation des marchés publics

1. Introduction

Attention

Les échanges qui interviennent dans le processus d'achat public peuvent avoir lieu par voie électronique (*dossier de consultation des entreprises, candidature et offre*[5]).

De fait depuis le 1er janvier 2005, le code des marchés publics dans son *article 56*[6] fait obligation aux acheteurs publics d'être en mesure de recevoir des offres électroniques.

La démarche type à suivre par une entreprise pour répondre à une offre est :

- Téléchargement du dossier de consultation.
- Connexion avec son certificat pour s'identifier et garantir la confidentialité de l'échange.
- Signature électronique avec son certificat du dossier de candidature.
- Dépot du dossier sur la plate-forme.

La confiance dans les échanges dématérialisés entre les acheteurs (personnes publiques, collectivités locales) et les entreprises est instaurée grâce aux sécurités juridique et informatique.

2. Sécurité juridique

Reconnaissance de l'écrit et la signature électroniques par le Code Civil :

- Le législateur reconnaît l'écrit électronique.
- L'article 1316-4 du Code civil pose l'équivalence de la signature électronique et de la signature manuscrite.

5 - http://www.e-marchespublics.com/
6 - http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=6EE42E5AF6A84310F49239CDD9132537.tpdjo07v_2?idArticle=LEGIARTI000019948089&cidTexte=LEGITEXT000005627819&dateTexte=20100507

Attention

Ainsi, un acte d'engagement sur papier signé à la main a la même valeur qu'un acte d'engagement électronique signé électroniquement.

Remarque

Une signature manuscrite scannée n'a pas la valeur juridique d'un original. Signer le *« dossier »* électronique qui contient plusieurs documents électroniques est insuffisant (les originaux sont signés mais pas les photocopies). En fait un document papier signé manuellement puis scanné est assimilé à une copie.

3. Sécurité informatique

La signature électronique et le chiffrement :

- La signature électronique, comme nous l'avons déjà vu, garantit les trois fonctions :
  - l'identité de l'émetteur du message,
  - la non répudiation - le signataire ne peut renier sa signature
  - l'intégrité du document signé.
- Le chiffrement, comme nous l'avons également déjà vu, permet de s'assurer de la confidentialité des données échangées.

La mise en œuvre de la signature électronique nécessite :

- Un certificat électronique comprenant notamment l'identité du titulaire, la période de validité, la clé publique et la signature de l'autorité de certification. Des catégories référencées sont *listées*[7].
- Un logiciel de signature qui permet d'apposer sa signature sur un document électronique. Il est intégré aux plate-formes de marchés publics qui assurent en même temps le chiffrement des données.

Pour déchiffrer l'offre, la clé est en possession d'une personne de confiance qui est membre de la commission d'appel d'offre (CAO). Une copie de la clé peut être déposée chez un tiers pour pouvoir la restituer en cas de perte.

Selon e-marchespublics.com, la signature est valide lorsque les conditions suivantes sont remplies :

- la signature est apposée,
- le certificat utilisé est référencé et listé sur la *liste publiée*[8],
- le certificat utilisé est valide à la date de la signature du document, en d'autres termes, à ladite date, le certificat n'a pas été révoqué et le certificat n'a pas expiré,
- le certificat est établi au nom d'une personne physique autorisée à signer.

En tant que prestataire de services de certification électronique (PSCE), Ceteurope offre sur son site http://www.certeurope.fr/ un certain nombre de services et certaines catégories de certificats. Pour la candidature à une offre publique le certificat certigreffe, certificat de classe 3+, pourra être utilisé.

7 - http://www.dgcis.redressement-productif.gouv.fr/secteurs-professionnels/economie-numerique/securite-et-transaction
8 - http://www.dgcis.redressement-productif.gouv.fr/secteurs-professionnels/economie-numerique/securite-et-transaction

4. La plate-forme FAST

Certains services de l'administration publique tels le contrôle de légalité ou la comptabilité utilisent la plateforme FAST (pour Fournisseur d'accès sécurisé transactionnel) qui assure la sécurisation des échanges électroniques et des services de preuves à longue échéance. Les collectivités peuvent accéder, grâce à un certificat électronique, à différentes téléprocédures. Les prestations de sécurité concernent, notamment, l'authentification, l'intégrité et la non-répudiation des échanges, la confidentialité des données, l'horodatage, et l'archivage. Le scénario type d'une telle utilisation passe par les étapes suivantes :

- Authentification de l'émetteur et contrôle des habilitations
- Validation des signatures
- Horodatage de la demande de télétransmission
- Transmission sécurisée des données au destinataire
- Constitution de la preuve de télétransmission
- Archivage
- Indexation

FAST est une infrastructure de confiance permettant la sécurisation des échanges dématérialisés au niveau local. Elle est interopérable avec les plates-formes ACTES du ministère de l'Intérieur et HELIOS du MINEFI.

FAST permet d'échanger des actes administratifs soumis au contrôle de légalité et relie les collectivités à leur Trésorerie générale. L'objectif est d'offrir aux collectivités une solution leur permettant à terme de dématérialiser leurs échanges administratifs et donc de réaliser des économies d'échelle. FAST est intégré par les principaux éditeurs de logiciels métier utilisés par les établissements publics et les collectivités. De ce fait cette solution s'intègre facilement dans le système d'information de l'organisation. Il est aussi directement accessible sur le *site officiel*[9].

Aujourd'hui, l'offre FAST comprend trois services :

- le Service Contrôle de légalité,
- le Service Convocation aux élus,
- le Service Comptabilité publique.

L'offre devrait s'étendre à d'autres domaines de l'administration publique.

S2LOW est un autre service du même type qui est sécurisé et inter-opérable pour la vérification et la validation d'un ensemble de téléprocédures administratives des collectivités. A la différence de Fast, S2LOW est développé dans le monde du logiciel libre contribuant ainsi à la transparence recherchée théoriquement par l'administration publique. Les services fournis par la plateforme S2LOW, appelés à

9 - http://www.cdcfast.fr/

s'enrichir au fur et à mesure de l'avancement du projet adèle, comprennent principalement

- la procédure de contrôle de légalité des actes (ACTES) et
- le traitement des flux comptables (HELIOS).

I. La sécurité informatique et l'interopérabilité dans l'administration électronique

1. Introduction

Attention

La mise en réseau de l'administration revient à relier virtuellement ses différentes composantes.

L'administration se présente alors comme un tout homogène, dont les éléments communiquent entre eux par des échanges dématérialisés en interne et en externe, grâce à leur interopérabilité.

Remarque

Si l'interopérabilité facilite la circulation de l'information, elle entraîne des risques d'atteinte à la sécurité des échanges.

La mise en réseau de l'administration est dominée par la technique. Le risque en matière d'utilisation des TIC par l'administration est le dommage éventuel que peuvent subir les usagers, l'administration et ses personnels, ainsi que ses prestataires de services, dans le cadre de l'utilisation des TIC.

La sécurité des échanges concerne quatre niveaux :

- la confidentialité,
- l'intégrité,
- la non répudiation, et
- l'authentification.

C'est l'utilisation du certificat électronique qui permet la sécurisation des échanges.

La mise en réseau de l'administration, qui a pour objet de faciliter la communication interne et externe de ses services, afin de favoriser la mise en œuvre des téléservices publics, cherche à effectuer l'interopérabilité de l'administration, et à sécuriser les échanges administratifs dématérialisés par l'utilisation d'un certificat électronique.

2. L'interopérabilité

a) Les critères et les enjeux de l'interopérabilité

L'interopérabilité désigne la capacité de systèmes différents ou identiques à pouvoir communiquer facilement entre eux. Deux systèmes informatiques sont donc interopérables, dès lors qu'ils communiquent ensemble.

Exemple

Dans l'exemple des systèmes informatiques, la communication entraîne la transmission d'informations.

Une information est un élément de connaissance pouvant *« être représenté à l'aide de conventions pour être conservé, traité ou communiqué »*. Il s'agit du contenu sémantique d'une donnée qui elle, est la représentation de l'information sous une forme conventionnelle, afin d'en faciliter le traitement. La forme conventionnelle est appelée le format.

L'enjeu économique de l'interopérabilité n'est pas négligeable.

Les concepteurs impliqués dans les différents systèmes ne peuvent ou ne veulent pas toujours favoriser l'interopérabilité, afin de défendre leurs parts de marchés respectives. Il est en effet difficilement concevable pour une entreprise qui détient des brevets sur une application de consentir à rendre publique sa conception, dans le but de permettre à d'autres entreprises de travailler sur cette application. Pourtant, cela permettrait de rendre au consommateur sa liberté de choix, et donc de réguler le marché au plus juste.

Attention

Il s'agit du second enjeu de l'interopérabilité, celui de la liberté.

Cet enjeu est battu en brèche du fait de positions de monopoles de certaines entreprises. Au regard de ses enjeux, l'interopérabilité n'est possible que s'il y a accord entre ses différents protagonistes, c'est-à-dire entre tous ceux qui ont un intérêt à favoriser -ou au contraire à empêcher- l'interopérabilité, quel que soit le secteur concerné. Il peut s'agir de sociétés propriétaires de licences, d'associations de consommateurs, du gouvernement, ou encore, d'organismes de normalisation nationaux et internationaux. L'élaboration de l'interopérabilité fait donc intervenir ces différents acteurs.

b) L'élaboration de l'interopérabilité

Attention

Le niveau international est incontournable pour l'élaboration de l'interopérabilité, car ses effets ne connaissent pas de frontière ; ils ont même pour conséquence de les lever.

Tout intéressé peut, en général et sous certaines conditions, participer aux groupes de travail qui élaborent la documentation technique qui constituera la norme. Il s'agit de normes ouvertes à opposer aux formats propriétaires qui sont élaborés dans le secret. Le World Wide Web consortium (W3C) est un consortium fondé en 1994 dans le but d'élaborer les standards du web. Il est géré par le MIT, l'ERCIM, et l'université japonaise de Keio.

Exemple

Il comprend plus de 400 membres, principalement des industriels comme Apple, Adobe, Nokia, Microsoft, ou Sony.

Il ne définit pas des normes, mais des recommandations, car il ne possède pas de programme de certification. En pratique, ses recommandations sont des normes et leur respect est quasiment acquis du fait de son monopole en la matière, et de l'interdépendance mondiale du web. Même s'ils n'en sont pas à l'origine, les États sont tenus de facto de respecter ces normes. Le développement des téléservices publics doit donc les prendre en compte, ainsi que celles édictées par d'autres organismes de normalisation. Le Référentiel général d'interopérabilité (RGI) concerne *« l'interopérabilité des services offerts par voie électronique »*. Il a pour objet de fixer *« les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives »*. Les conditions d'élaboration du RGI sont fixées par un décret.

3. L'interopérabilité des technologies de l'information et de la communication

L'interopérabilité des TIC peut cependant être distinguée des autres types d'interopérabilité par l'examen de ses éléments constitutifs, éléments qui soulèvent la question du choix entre les formats propriétaires et ouverts.

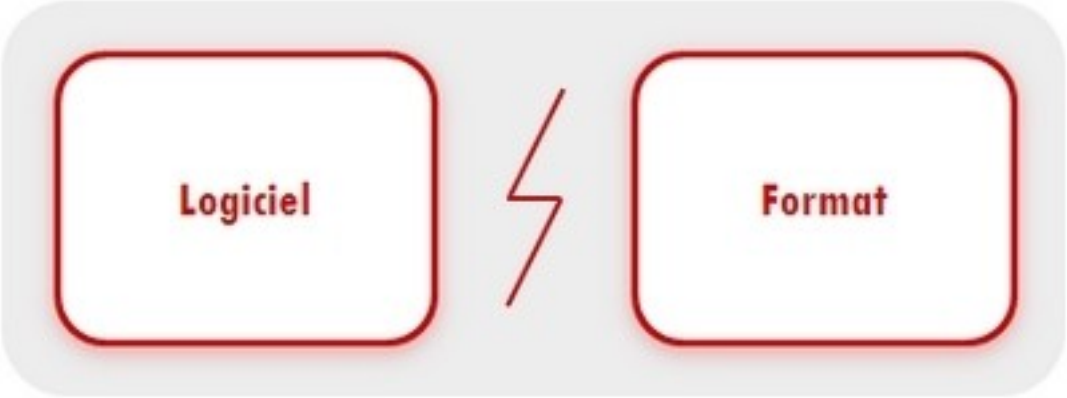
a) Les éléments constitutifs de l'interopérabilité des technologies de l'information et de la communication

Les TIC sont composées de nombreux éléments matériels, comme des ordinateurs ou des téléphones, et immatériels comme des logiciels. Le matériel n'est pas interopérable en soi ; il le devient à l'aide d'un élément immatériel : un logiciel. L'interopérabilité des TIC porte donc sur les logiciels, mais également sur les informations qu'ils traitent, informations inscrites dans des formats différents. Cette dualité logiciel/format se retrouve dans divers secteurs des TIC comme le web, le multimédia et la bureautique. L'accès au web se fait par le biais d'un navigateur dont le plus répandu est l'Internet Explorer de Microsoft ; il en existe d'autres, dont le code source est ouvert, comme Mozilla. Le langage informatique servant à écrire les pages web -qui est le HTML- peut être interprété par tous les navigateurs web.

Le multimédia, qui désigne *« l'ensemble des techniques et des produits qui permettent l'utilisation simultanée et interactive de plusieurs modes de représentation de l'information (textes, sons, images fixes ou animées) »*, connaît également de multiples logiciels et formats. En la matière, c'est la gestion des GDN (Gestion des droits numériques) qui peut poser des difficultés en terme d'interopérabilité. Un fichier audio contenant un GDN peut parfois n'être lu que par un seul type de matériel.

La bureautique est l'ensemble *« des techniques et des moyens tendant à automatiser les activités de bureau et principalement le traitement et la communication de la parole, de l'écrit et de l'image »*. Dans ce domaine, il existe plusieurs logiciels dont les plus répandus sont constitués par la suite Microsoft Office qui comprend le logiciel de traitement de texte Word, dont le format *« .doc »*

qui lui est rattaché pose, comme il a été démontré précédemment, des problèmes d'interopérabilité (réglés dans les dernières versions avec le format .docx).



Important

L'interopérabilité des TIC est donc freinée par les formats propriétaires, de sorte que se pose la question du choix entre ces formats et les formats ouverts.

b) Le choix entre des formats propriétaires et des formats ouverts

Un format est l'*« agencement structuré d'un support de données »* et la *« disposition des données elles-mêmes »*. Il s'agit d'une convention -éventuellement normalisée- qui sert à représenter les données. Le format est rattaché au moins à un logiciel qui en assure la lecture. Le format est ouvert lorsque son implémentation est libre ; il est fermé quand son implémentation n'est possible que par son propriétaire. L'un et l'autre correspondent à une norme -ou standard- qui est ouverte dans le premier cas et fermée dans le second. La tendance actuelle du développement européen de l'administration électronique et des téléservices publics est de favoriser l'emploi des formats ouverts. C'est la condition sine qua non d'une interopérabilité efficace.

La Commission européenne estime ainsi que l'interopérabilité des systèmes informatiques dans les administrations est une nécessité, et que pour y parvenir l'utilisation des formats ouverts et des logiciels libres est une priorité.

La France, à travers l'élaboration du RGI, souhaite privilégier le format concurrent du format *« .doc »* : le format *« Open document »* ou *« ODF »*.

4. L'interopérabilité de l'administration électronique

L'interopérabilité de l'administration électronique concerne les TIC, de sorte que sa définition peut se nourrir des développements précédents ; il faut cependant la compléter en étudiant les différents domaines concernés par cette interopérabilité.

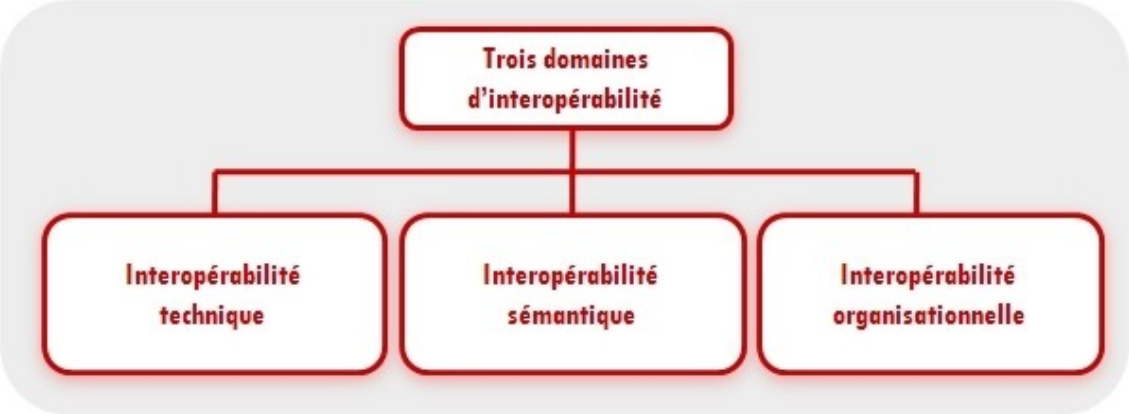
La mise en oeuvre de l'interopérabilité n'est pas cantonnée à tel ou tel téléservice public : elle touche toute l'administration -qu'elle soit locale, nationale ou européenne- ainsi que les usagers et même des acteurs induits. Il existe par conséquent différents niveaux d'interopérabilité reliés entre eux, et qui conduisent progressivement à une interopérabilité globale de l'administration.

a) Les domaines concernés par l'interopérabilité de l'administration électronique

La Commission européenne, qui identifie trois domaines de l'interopérabilité devant être pris en compte lors de la mise en oeuvre de l'administration électronique -les domaines technique, sémantique et organisationnel-, relève l'importance des normes techniques en la matière.

L'interopérabilité technique	L'interopérabilité sémantique	L'interopérabilité organisationnelle
L'interopérabilité technique désigne *« l'interpénétration de systèmes technologiques et de logiciels, la définition et l'utilisation d'interfaces, de normes et de*	L'interopérabilité sémantique consiste à *« faire en sorte que la signification des informations échangées ne soit pas perdue dans la procédure, qu'elle soit préservée et*	L'interopérabilité organisationnelle identifie *« les acteurs et les procédures organisationnelles intervenant dans la fourniture d'un service spécifique d'administration en*

L'interopérabilité technique	L'interopérabilité sémantique	L'interopérabilité organisationnelle
protocoles ouverts en vue de créer des systèmes d'information fiables, efficaces et performants ». Dans ce contexte, le volet technique du RGI recommande l'emploi du langage XML qui se prête bien aux besoins des échanges dématérialisés et l'interopérabilité. Le langage XML permet de définir la structure des documents en s'appuyant sur des catégories définies par l'utilisateur et matérialisées par des balises. Conformément à une circulaire du 21 janvier 2002, il existe un répertoire des schémas XML de l'administration dont la dernière version date du 2 juillet 2007.	*comprise par les personnes, les applications et les institutions concernées* ». Il faut donc donner une sémantique -ou sens aux informations échangées, et la transmettre à tous les systèmes concernés par les échanges. Ces systèmes combinent alors les informations reçues avec d'autres afin de les traiter de manière appropriée par rapport à la sémantique. Il ne s'agit donc plus seulement de permettre la communication entre systèmes et applications informatiques, mais de garantir une cohérence entre leurs manières de décrire et d'interpréter les informations échangées.	*ligne* », et cherche à « *parvenir à un accord entre ces acteurs et procédures sur la manière de structurer leur interaction* ». Elle nécessite que soient fixées les conditions d'accès aux informations interopérables, ainsi que les politiques d'intégrité et de confidentialité de ces informations. Elle conduit également à prendre en compte la culture propre à chaque service -au sens de culture de l'entreprise-, c'est-à-dire à « *l'ensemble des traditions de structure et de savoir-faire* » du service.



b) De l'interopérabilité des téléservices publics à une interopérabilité globale de l'administration

Attention

Chaque téléservice public doit être interopérable, c'est-à-dire que les domaines d'interopérabilité qui le composent doivent pouvoir communiquer entre eux facilement.

Exemple

La dématérialisation des procédures d'achat public suppose, par exemple, que les entreprises soumissionnaires arrivent a faire parvenir leur offre par voie électronique à l'administration qui elle, doit être en mesure de les comprendre, mais également de les faire circuler au sein de différents services pour examen, classement, ou archivage.

L'interopérabilité concerne donc le front office, le back office et les relations entre les deux. Le principe d'égal accès aux services publics commande une attention particulière pour le choix des formats et des logiciels utilisés. L'égalité dans l'accès et l'utilisation des services publics est un principe général du droit (PGD) qui doit être respecté pour l'accès et l'utilisation des téléservices publics. Les téléservices publics ne sont pas isolés les uns des autres ; ils peuvent être appelés à communiquer entre eux et doivent donc être réciproquement interopérables. Il en est ainsi des téléservices publics locaux reliés par le procédé du co-marquage au portail Service-public.fr. Il s'agit de *« la possibilité de rediffuser sur un site public local les contenus et les services offerts par le portail de l'administration française et de les enrichir de données et de services locaux complémentaires, afin d'offrir à l'usager un accès unique et adapté à son contexte local, pour ses droits et démarches »*. L'interopérabilité entre les collectivités locales et l'État se retrouve également dans les différents projets d'administration électronique, comme le contrôle de légalité et le contrôle des circuits financiers et comptables.

Attention

Ces dématérialisations sont interopérables par le biais de la plateforme sécurisée FAST abordée plus haut.

5. Interopérabilité et interconnexion dans l'administration électronique

Bien que souvent confondues, les notions d'interopérabilité et d'interconnexion sont différentes : la première vise la capacité de deux systèmes à pouvoir communiquer entre eux, alors que la seconde consiste à mettre en relation les données de différents fichiers. C'est la combinaison des deux notions qui permet les rapprochements de fichiers et qui suscite des craintes pour la vie privée des usagers. En fait il faut observer, d'une part, l'utilité des rapprochements de fichiers entre les administrations par la constitution et l'utilisation de bases de données interopérables et interconnectables, et d'autre part, l'existence de principes de protection de la vie privée des usagers.

a) L'utilisation des bases de données interopérables et interconnectables au sein de l'administration électronique

Une base de données interopérable et interconnectable est très utile pour le service

public, car elle permet de regrouper, de façon thématique, des données éparpillées entre différents endroits et de les valoriser. La base de données, ou plus exactement son utilisation, peut être un outil potentiellement liberticide : les possibilités de recoupements entre plusieurs bases issues d'administrations différentes permettent de « *tracer* » facilement les administrés.

Pour des raisons de lutte contre le crime, certains fichiers ont cette finalité.

Exemple

Le STIC.

Créé par un décret du 5 juillet 2001, ce système est un fichier de recherches criminelles, destiné à faciliter les enquêtes, en permettant de relier entre elles plusieurs affaires présentant des similitudes. Des erreurs, relativement à l'utilisation du STIC, ont pu être déplorées, ce qui permet de douter du respect de sa finalité.

Attention

Ce n'est donc pas l'interopérabilité ni l'interconnexion qui portent atteinte à la vie privée des individus, mais l'absence ou le non-respect de la finalité, ainsi que les erreurs humaines.

En d'autres termes, ce ne sont pas les TIC qui sont en cause, mais l'utilisation qui en est faite.

À cet égard, la constitution du portail « *mon.service-public.fr* » focalise les craintes d'atteintes à la vie privée. C'est un portail commun aux administrations à partir duquel chaque usager pourra remplir l'intégralité de ses formalités administratives. Ce projet suppose que les informations administratives soient issues de bases de données disséminées dans différentes administrations. D'où la question de l'existence de bases de données croisées. Les possibilités d'interconnexions sont en effet nombreuses, portent sur des domaines sensibles comme la santé ou les impôts, et surtout sont susceptibles de dépasser le cadre stricto sensu de l'administration pour concerner des acteurs privés tiers. La généralisation de l'interopérabilité, alliée à l'interconnexion, permettent, en ayant la possibilité de valoriser les données, de rendre un meilleur service aux usagers. Ils peuvent également conduire à des rapprochements abusifs de données pouvant aboutir à un État omniscient. Que ses utilisateurs soient l'administration, les usagers, ou des tierces personnes, la technique doit être sécurisée et juridiquement encadrée par le biais de principes de protection de la vie privée des usagers.

b) Les principes de protection de la vie privée des usagers

Le module D1 consacre un item entier aux questions liées à la notion complexe et contingente de vie privée. Dans ces notes, nous revisitons cette notion dans le cadre précis de l'administration électonique. Il n'existe pas de définition légale du concept, et c'est la jurisprudence qui vérifie, au cas par cas, le respect de la vie privée.

Attention

Seule une raison d'ordre public, compatible avec une Société démocratique, peut porter atteinte à la vie privée.

Le Conseil constitutionnel a ainsi eu l'occasion de vérifier le respect de la vie privée des usagers par le dispositif de la carte SESAM-Vitale.

Il a estimé que les diverses garanties entourant la mise en place de ce système *« sont de nature à sauvegarder le respect de la vie privée »*. C'est précisément l'existence de garanties dans un projet de téléservice public qui permettent l'équilibre entre l'efficacité administrative et le respect de la vie privée des usagers. La CNIL est d'ailleurs favorable au développement d'une administration électronique : *« Dès lors qu'il s'agit de rendre un meilleur service aux usagers de l'administration, de rendre celle-ci plus efficace et plus transparente, de simplifier les démarches tout en garantissant les droits et libertés de chacun, la CNIL est, bien entendu, pleinement favorable au développement de l'administration électronique et encourage toutes les initiatives menées en ce sens »*.

Attention

La Commission estime que l'administration électronique ne peut se faire au détriment de la protection de la vie privée.

Dans son avis portant sur le Projet ADELE, la CNIL a fixé les principes protecteurs de la vie privée des usagers ; principes que la personne publique doit respecter lorsqu'elle souhaite constituer des bases de données.

Attention

Il s'agit des principes

- de proportionnalité,
- de transparence,
- de pluralité des identifiants, et
- de sécurité graduée.

La proportionnalité signifie que la finalité de l'interconnexion doit être conforme à un intérêt public, ce qui implique un contrôle étendu de la CNIL qui vérifie, notamment, *« la pertinence des données échangées, les destinataires habilités à connaître des données, l'information claire et explicite des personnes concernées par ces échanges »*. La CNIL redoute l'utilisation généralisée d'un numéro national d'identification et incite à la pluralité des identifiants pour l'accès aux téléservices publics. Sa position est résumée dans cette formule : *« à chaque sphère son identifiant, pas d'utilisation généralisée d'un numéro national d'identification »*. Ce principe permet d'éviter la création de profils d'administrés. Le principe de sécurité graduée revient à moduler les exigences de sécurité selon les démarches administratives.

Exemple

Certaines d'entre elles, comme le téléchargement de formulaires, ne nécessitent pas d'identification préalable de l'usager qui peut rester anonyme. Même si des personnalités s'autorisent à penser que l'anonymat des usagers *« n'est pas indispensable quand on n'a rien à se reprocher »*, il s'agit d'un principe important qui permet d'assurer l'égalité des usagers dans l'accès et l'utilisation des téléservices publics.

Le niveau suivant est celui de l'identification de l'usager qui *« consiste pour l'usager à indiquer qui il est avant d'accéder à une information ou à un service »*. L'administré accède alors au service après avoir renseigné son identifiant et son mot de passe.

Le degré de sécurité le plus élevé est celui de l'authentification qui *« consiste pour l'usager à prouver son identité, ce qui lui permet éventuellement de signer des transactions ou des actes »*.

Attention

L'authentification est rendue possible par l'utilisation du certificat électronique.

L'interopérabilité de l'administration, qui est indispensable pour la mise en œuvre des téléservices publics, est conditionnée par les normativités technique et juridique. Le droit étatique intervient pour prévenir les risques d'atteinte à la vie privée engendrés par l'interopérabilité et l'interconnexion. La loi du 6 janvier 1978 précitée, ainsi que le rôle de la CNIL en matière de projet de téléservice public, constituent un cadre juridique de protection des usagers. La portée normative des dispositions de la CNIL peut varier selon les types de textes qu'elle élabore. La norme technique prime la norme juridique qui se contente de l'entériner.

Attention

La norme technique domine, de par son domaine d'intervention -la technique-, l'interopérabilité de l'administration, et par conséquent la mise en oeuvre des téléservices publics. La sécurisation des échanges administratifs dématérialisés, par l'utilisation du certificat électronique, confirme le constat de cette spécificité.

6. La sécurisation des échanges administratifs dématérialisés par l'utilisation du certificat électronique

Le certificat électronique, dont l'utilisation dans les téléservices publics a pour but de sécuriser les télétransmissions, est créé par une infrastructure de gestion de clés publiques. L'élaboration du certificat électronique se fonde sur les normativités juridique et technique.

L'ordonnance n° 2005-1516 du 8 décembre 2005, prise sur le fondement de la loi de simplification du droit du 9 décembre 2004, prévoit ainsi l'élaboration d'un référentiel général de sécurité (RGS). Ce référentiel doit fixer *« les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage »*. Les travaux du RGS s'appuient sur des normes ou des recommandations techniques, ainsi que sur la version 2.1 de la Politique de référencement intersectorielle de sécurité (PRIS) qui est un document référent. La version 1.0 du RGS a été entérinée par un arrêté du Premier ministre du 6 mai 2010.

Attention

Reprenant la définition de la directive européenne de 1999, le décret du 30 mars 2001 définit le certificat électronique comme *« un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire »*.

Afin de prouver ce lien, le certificat -qui est un bloc de données- contient plusieurs parties : une paire de clés asymétriques servant au chiffrement des données échangées afin d'en conserver l'intégrité ; des informations sur le porteur de cette paire de clés comme son nom ; et la signature électronique qui permet la création de l'authentification. Le certificat a donc deux utilisations majeures :

- l'authentification au moyen d'une signature électronique,
- l'intégrité et la confidentialité des données grâce à leur chiffrement.

a) L'authentification au moyen d'une signature électronique

La signature électronique permet d'authentifier son auteur et, corrélativement, sa non répudiation. Utilisée dans un premier temps pour favoriser le commerce en ligne, la signature électronique trouve des applications dans les téléservices publics. Encadrée par des normes juridiques et techniques, elle est utilisée dans le but de favoriser la confiance des usagers. L'emploi de la signature électronique au sein des téléservices publics est explicitement prévu par l'*article 8 de l'ordonnance n° 2005-1516*[10] : *« Les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte »*.

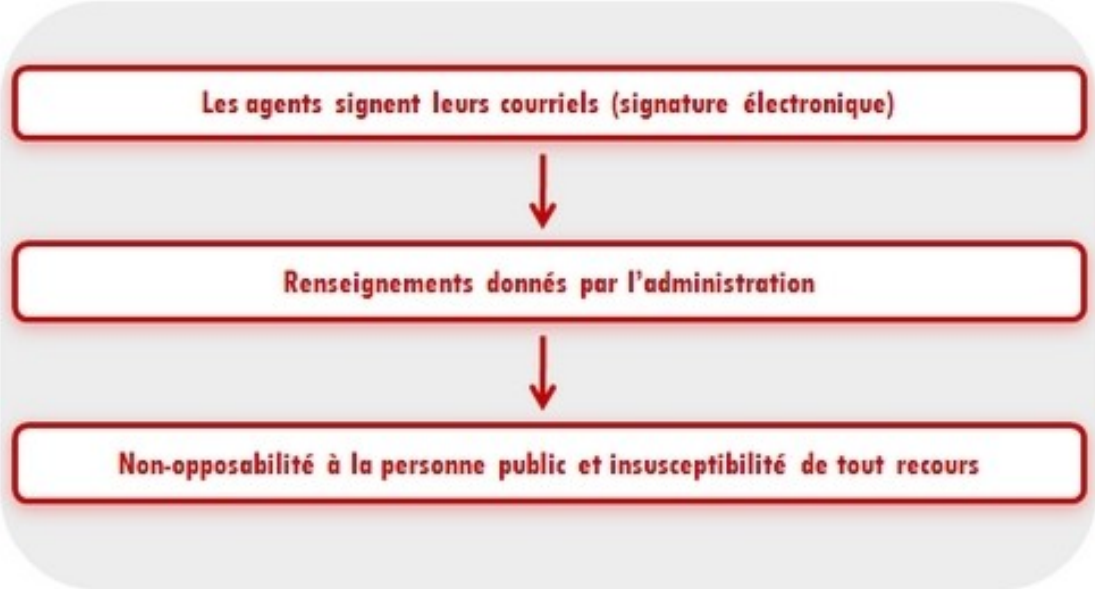
Ce texte est une consécration légale de l'utilisation de ce type de procédé par l'administration. Le RGS préconise pour l'administration électronique, l'utilisation du format de signature XAdEs défini, notamment, par le W3C et l'IETF.

10 - http://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=6EE42E5AF6A84310F49239CDD9132537.tpdjo07v_2?idArticle=LEGIARTI000006317195&cidTexte=LEGITEXT000006052816&dateTexte=20100507

Attention

L'administration utilise la signature électronique pour sécuriser les échanges internes et externes.

Cet outil est ainsi utilisé par les agents pour signer leurs courriels, dont certains sont à destination des usagers. Ce ne sont pas des décisions administratives, mais des renseignements donnés par l'administration. Il en découle leur non-opposabilité à la personne publique, et l'insusceptibilité de tout recours à leur encontre.



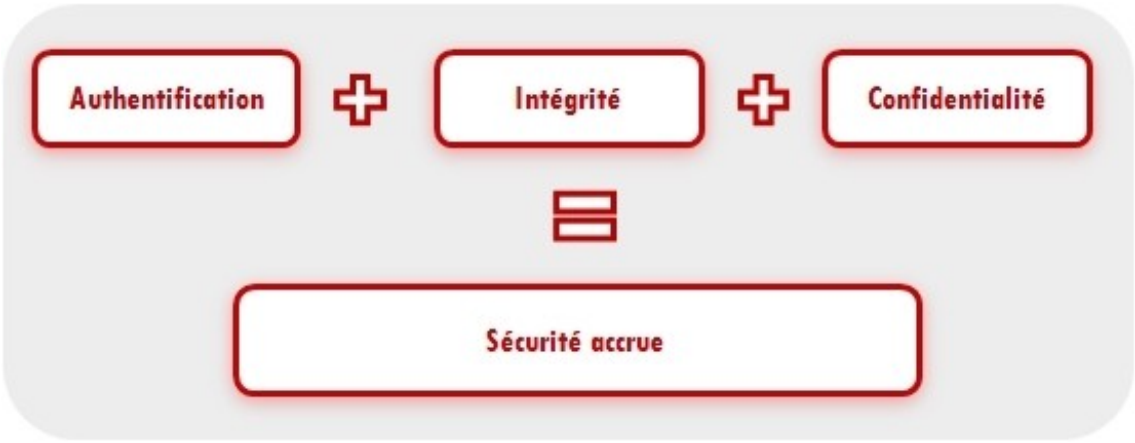
Afin de permettre le développement des téléservices publics, le gouvernement souhaite favoriser la confiance des usagers dans ce type de prestations. Dans cette optique, le niveau de sécurité d'une téléprocédure administrative doit être, sinon supérieur, du moins égal à celui qui est offert lors d'un échange sous forme papier. Les moyens cryptographiques ne doivent cependant pas être employés d'une manière irréfléchie, avec le seul prétexte d'offrir une sécurité maximale.

Attention

C'est pourquoi la CNIL indique que la signature électronique *« est indispensable là où un impératif d'authentification s'impose dans le souci de la confidentialité des données et pour éviter toute usurpation d'identité »*.

Cette idée est reprise par le principe de sécurité graduée.

La signature électronique permet à certaines procédures administratives, touchant à des données sensibles -comme la déclaration de l'impôt sur le revenu-, d'avoir un degré de sécurisation accrue grâce à l'authentification du signataire, à l'intégrité et à la confidentialité des données transférées.



b) L'intégrité et la confidentialité des données au moyen de leur chiffrement

Important

L'intégrité est la qualité d'une chose *« qui a toutes ses parties, qui n'a pas subi d'altération »*.

Cela signifie que les données échangées lors de dématérialisations ne doivent pas subir d'altération accidentelle ou intentionnelle. La confidentialité implique que les données échangées ne soient connues que des seules personnes qu'elles concernent.

Le moyen pour parvenir à ces deux objectifs de sécurité est le recours à la notion de chiffrement des données qui trouve sa pleine application dans les téléservices publics.

Attention

L'encadrement du chiffrement des données se fonde sur les textes législatifs et réglementaires concernant la cryptographie.

Le système de chiffrement retenu est celui des clés asymétriques. Le chiffrement des données étant le corollaire de la signature électronique, il n'est pas étonnant de trouver le même type d'encadrement normatif.

Remarque

Il faut remarquer une nouvelle fois l'influence de la CNIL en matière de sécurité informatique des téléservices publics. La Commission considère que la libéralisation de la cryptologie est un point positif pour les administrés qui peuvent de la sorte bénéficier de produits de sécurité sûrs et performants. Le principe de confiance implique donc l'application d'un procédé de chiffrement *« fort »*, c'est-à-dire d'un chiffrement dont la clé est d'une longueur jugée suffisante; spécialement quand le téléservice public est obligatoire, ou lorsque les données collectées sont sensibles. En se prononçant sur la légalité d'un traitement de données personnelles mis en œuvre par l'administration, la Commission affirme son attachement à un système de chiffrement fort.

7. L'élaboration d'une infrastructure de gestion de clés publiques pour les besoins des téléservices publics

Attention

Les solutions cryptographiques peuvent être propres à chaque téléservice public.

Ceci s'explique par la libéralisation de la cryptologie et par l'autonomie dont disposent les collectivités locales pour mettre en œuvre leurs projets d'administration électronique.

La multiplication des solutions de confiance, si elle est une marque de la liberté de la personne publique en la matière, risque de rendre l'interopérabilité des différents projets plus difficile. D'où l'élaboration d'une politique commune de sécurité dans les téléservices publics.	Ce type de politique est cependant malaisé à mettre en œuvre -spécialement pour les collectivités locales-, dans la mesure où elle nécessite une expertise technique et juridique pointue. C'est notamment pour cette raison que le gouvernement encourage la constitution d'infrastructures de confiance permettant de sécuriser la télétransmission des actes des collectivités locales.

a) L'élaboration d'une politique commune de sécurité dans les téléservices publics

Le secteur de la cryptologie étant libéralisé, la personne publique a la possibilité d'externaliser ses besoins en la matière auprès d'entreprises privées.

L'avantage	L'inconvénient
L'avantage de cette externalisation est de pouvoir bénéficier d'un savoir-faire juridique et technique.	L'inconvénient majeur est le risque de perdre le contrôle des questions de sécurité informatique dans l'administration.

Attention

Une solution médiane, qui consiste en une externalisation partielle d'une IGC bâtie sous une forme pyramidale et contrôlée par la personne publique, est préconisée.

Attention

L'enjeu est double : l'élaboration d'un système d'archivage pouvant être mutualisé et le renforcement de la plate-forme d'archivage électronique des Archives nationales.

b) Le recours à une infrastructure de confiance pour la télétransmission des actes des collectivités locales

Une infrastructure de confiance désigne un ensemble de moyens matériels, de logiciels, et de procédures humaines, mis en oeuvre par des textes juridiques et des pratiques, dans le but d'assurer la télétransmission des actes et les fonctions relatives à leur sécurité.

Cette notion dépasse celle d'IGC. Elle ne doit pas être confondue avec celle d'autorité ou de tiers de confiance qui n'assure qu'un nombre limité de fonctions relatives à la sécurité, comme l'archivage et l'horodatage. Même si l'infrastructure de confiance exécute la télétransmission des actes, elle ne saurait se confondre avec le tiers de télétransmission (TDT) qui n'assure, par principe, que cette activité sans prendre en compte les fonctions relatives à la sécurité. Même si ces notions sont souvent confondues, il n'en demeure pas moins qu'elles sont différentes. Le Plan ADELE retient l'expression d'*« infrastructure de confiance »*, car il souhaite privilégier des solutions globales pour la confiance dans les échanges dématérialisés des collectivités locales. Ceci n'empêche pas l'application des référentiels sur la sécurité informatique -et spécialement le RGS- au niveau local.

Attention

Une solution globale et mutualisée a pour but de favoriser le développement de l'administration électronique locale, dans la mesure où elle est une réponse concrète au manque de moyens matériels et humains des collectivités, ainsi qu'à leur demande de savoir-faire.

Savoir-faire

III

A. Testez vos connaissances

Question 1

1

Quels sont les objectifs d'une malveillance informatique?

Indice :

Voir : La sécurisation des échanges numériques (cf. La sécurisation des échanges numériques p 10)

Question 2

2

Comparer les systèmes suivants : Wifi, Pare-feu et réseaux virtuels privés.

Indice :

Voir : Les réseaux et leur protection.

- *Les réseaux sans fil (cf. Les réseaux sans fil p 47).*
- *Le pare-feu (cf. Le pare-feu p 50).*
- *Les réseaux privés virtuels (cf. Les réseaux privés virtuels p 51).*

Question 3

3

La politique du CNHJ en matière de dématérialisation s'apparente plus de celle du CNB ou de celle du CSN? Justifiez votre réponse.

Indice :

Voir : Les échanges entre professionnels.

- *L'huissier de justice.*

Question 4

4

Définir le projet Transjuris en effectuant une recherche sur le web.

Indice :

Voir : Les échanges entre professionnels.

- *L'huissier de justice.*

Question 5

5

Quels sont pour un certificat accepté par l'acheteur public la durée de validité moyenne? Le coût moyen? Les modes de commande? Le délai moyen?

Indice :

Voir : La dématérialisation des marchés publics.

- *Sécurité informatique.*

Question 6

[*Solution n°1 p 103*]

6

Quels sont les 4 niveaux concernés par la sécurité des échanges ?

Indice :

Voir : La sécurité informatique (cf. Sécurité informatique p 63) et l'interopérabilité dans l'administration électronique (cf. L'interopérabilité de l'administration électronique p 73).

B. Exercice : L'utilisation des bases de données

[*Solution n°1 p 105*]

Complétez les mots ou expressions manquants.

Une base de données _____ et _____ est très utile pour le _____, car elle permet de regrouper, de façon thématique, des données éparpillées dans différents endroits et de les _____.

La base de données, ou plus exactement son _____, peut être un outil potentiellement _____ : les possibilités de recoupements entre plusieurs _____ issues d'_____ différentes permettent de _____ facilement les administrés.

Pour des raisons de lutte contre le _____, certains _____ ont cette finalité.

C. Exercice : Cas pratique dirigé

[*Solution n°2 p 105*]

Bob et Alice dirigent une société de développement de logiciels.

Cependant Alice vivant à Paris et Bob à Tahiti la plupart de leurs échanges se font par mail.

Afin de prévenir tout espionnage de la part de leurs concurrents ils décident donc de sécuriser leurs ordinateurs et leurs échanges.

Question 1

Tout d'abord Bob propose à Alice de télécharger un logiciel de type troyen afin de sécuriser son ordinateur.

- ○ Bob a raison
- ○ Bob a tort

Question 2

Quel type de logiciel analyse le trafic réseau afin de détecter et bloquer les intrusions ?

- ○ Antivirus
- ○ IDS
- ○ VNP

Question 3

Maintenant que leurs ordinateurs sont sécurisés ils veulent se renseigner sur le chiffrement de leurs échanges et décident de rechercher quels sont les standards en la matière.

Par quel moyen pourront-il le faire?

- ○ IETF
- ○ IGC
- ○ Un certificat électronique

Question 4

Après avoir lu les RFC sur les différents types de chiffrement, Bob et Alice s'interrogent sur celui qu'ils vont utiliser.

Redoutant une interception de données ils se demandent quel type de chiffrement est le moins sensible à des attaques de type Man in the Middle ou par usurpation ?

- ○ Algorithme symétrique
- ○ Algorithme asymétrique

Question 5

Bob et Alice décident donc d'utiliser un chiffrement asymétrique pour crypter leurs échanges.

Quelle clé Bob doit-il utiliser pour crypter les messages qu'il enverra Alice ?

- ○ La clé publique d'Alice
- ○ Sa clé privée

D. Quiz

Exercice 1

[*Solution n°3 p 107*]

Bluetooth, Wifi, Wimax, Infrarouge et Ethernet permettent tous de faire un réseaux sans fil

- ○ Vrai
- ○ Faux

Exercice 2

[*Solution n°4 p 108*]

Il existe le chiffrement symétrique et asymétrique, ils correspondent respectivement aux notions de clé secrète et clé publique.

○	Vrai
○	Faux

Exercice 3

[*Solution n°5 p 108*]

Il y a deux types de cybercriminalité : celle qui utilise l'outil informatique et celle qui le vise.

○	Vrai
○	Faux

Exercice 4

[*Solution n°6 p 108*]

Interopérabilité : plusieurs systèmes différents peuvent communiquer.

○	Vrai
○	Faux

Exercice 5

[*Solution n°7 p 108*]

L'attaque par déni de service (DOS) consiste à écouter les échanges entre le client et le serveur afin de se faire passer pour le clients.

○	Vrai
○	Faux

Exercice 6

[*Solution n°8 p 108*]

Le logiciel "PLANETE" est un support technique intermédiaire pour échanges avec l'environnement extérieur du notariat.

○	Vrai
○	Faux

Exercice 7

[*Solution n°9 p 108*]

Les autorités de certification permettent d'assurer l'identité du détenteur des clés en lui délivrant un certificat numérique.

○	Vrai
○	Faux

Exercice 8

[*Solution n°10 p 109*]

Les échanges numériques ne se font que par Internet ?

○	Vrai
○	Faux

Exercice 9

[*Solution n°11 p 109*]

Pour protéger mon mot de passe, il doit être long, avec des caractères spéciaux, des majuscules et minuscule. Il est donc assez complexe pour que je l'utilise partout et tout le temps.

○	Vrai
○	Faux

Exercice 10

[*Solution n°12 p 109*]

Une fois un certificat délivré, il est toujours valide.

○	Vrai
○	Faux

Solution des exercices rédactionnels

> Solution n°1 *(exercice p. 98)*

- La confidentialité
- L'intégrité
- La non répudiation, et
- L'authentification

Correction des exercices auto-évalués

> Solution n°1 *(exercice p. 98)*

Une base de données interopérable et interconnectable est très utile pour le service public, car elle permet de regrouper, de façon thématique, des données éparpillées dans différents endroits et de les valoriser.

La base de données, ou plus exactement son utilisation, peut être un outil potentiellement liberticide : les possibilités de recoupements entre plusieurs bases issues d'administrations différentes permettent de tracer facilement les administrés.

Pour des raisons de lutte contre le crime, certains fichiers ont cette finalité.

> Solution n°2 *(exercice p. 99)*

Question 1

○	Bob a raison *Commentaire :* *Un troyen ne sert en aucun cas à sécuriser son ordinateur !* *Pour cela il faut installer des logiciels de type IDS, antivirus, pare-feu, anti-spyware.*
◉	Bob a tort *Commentaire :* *Un troyen est un logiciel malveillant.* *Il n'est pas considéré comme un virus informatique car ne se reproduit pas par lui-même, cependant ce type de logiciel sert en général à installer un autre logiciel malveillant permettant à l'attaquant de prendre le contrôle de l'ordinateur infecté.*

Question 2

○	Antivirus *<u>Commentaire :</u>* *Le rôle d'un antivirus est bien de détecter et bloquer les logiciels malveillants, cependant leurs recherches s'effectuent sur les signatures des logiciels ou en analysant leur comportement (méthode heuristique).*
◉	IDS *<u>Commentaire :</u>* *Un système de détection d'intrusion (ou IDS : Intrusion Detection System) permet de repérer des activités anormales ou suspectes dans le réseau qu'il protège.*
○	VNP *<u>Commentaire :</u>* *Un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est un réseau privé reposant sur un protocole de tunnelisation.* *On parle de VPN lorsqu'un organisme interconnecte ses sites via une infrastructure partagée avec d'autres organismes.*

Question 3

○	IETF *<u>Commentaire :</u>* *L'Internet Engineering Task Force est un groupe informel d'experts technique qui produit la plupart des nouveaux standards d'Internet.*
○	IGC *<u>Commentaire :</u>* *Une infrastructure de gestion de clés publiques (IGC) est un ensemble de moyens matériels, de logiciels, et de procédures humaines, mis en oeuvre par des textes juridiques et des pratiques, dans le but de gérer le cycle de vie des certificats électroniques basés sur la cryptographie asymétrique.*
◉	Un certificat électronique *<u>Commentaire :</u>* *Un certificat électronique peut servir à l'authentification mais aussi à chiffrer un contenu.*

Question 4

○	Algorithme symétrique *Commentaire :* *Afin qu'Alice puisse lire le message de Bob il faudra que Bob lui envoie la clé de chiffrement.* *Cette clé doit donc circuler sur le réseau et est donc potentiellement récupérable par une attaque de type Man in the Middle ou par usurpation, permettant ainsi à l'attaquant de déchiffrer n'importe quel message crypté avec cette clé.*
◉	Algorithme asymétrique *Commentaire :* *Dans un algorithme asymétrique, seule la clé de chiffrement circule sur le réseau et n'est donc pas sujette à ce type d'attaque.* *Dans le cas d'une attaque de type Man in the Middle ou par usurpation l'attaquant ne pourra pas déchiffrer le message.*

Question 5

◉	La clé publique d'Alice *Commentaire :* *Un des rôles de la clé publique est de permettre le chiffrement.* *C'est donc cette clé qu'utilisera Bob pour envoyer des messages chiffrés à Alice.*
○	Sa clé privée *Commentaire :* *Le rôle de la clé privée est de déchiffrer un message envoyé par Alice.* *Cette clé permet de générer la clé publique que Bob communiquera à Alice.* *Ainsi, Bob, et lui seul, peut prendre connaissance des messages d'Alice.*

> Solution n°3 *(exercice p. 100)*

○	Vrai
◉	Faux

> Solution n°4 *(exercice p. 100)*

◉	Vrai
○	Faux

> Solution n°5 *(exercice p. 101)*

◉	Vrai
○	Faux

> Solution n°6 *(exercice p. 101)*

◉	Vrai
○	Faux

> Solution n°7 *(exercice p. 101)*

○	Vrai
◉	Faux

> Solution n°8 *(exercice p. 101)*

◉	Vrai
○	Faux

> Solution n°9 *(exercice p. 101)*

◉	Vrai
○	Faux

> Solution n°10 *(exercice p. 102)*

○	Vrai
◉	Faux

> Solution n°11 *(exercice p. 102)*

○	Vrai
◉	Faux

> Solution n°12 *(exercice p. 102)*

○	Vrai
◉	Faux

Recueil de textes

Type de texte	Autre
Date	29/10/2008

Type de texte	Loi
Date	13/03/2000

Type de texte	Loi
Date	06/01/1978

Type de texte	Ordonnance
Date	08/12/2005

Type de texte	Ordonnance
Date	20/02/2004

Type de texte	Décret
Date	30/03/2001

Bibliographie

[Catala] CATALA (P.), ET AL.,*L'introduction de la preuve électronique dans le Code civil. Étude par un groupe d'universitaires : Catala (P.), Gautier (P.-Y), Huet (J.), de Lamberterie (I.), Linant de Bellefonds (X.), Lucas (A.), Lucas de Leyssac (C.), Vivant (M.)*, JCP G, 24 novembre 1999, n° 47, pp. 2069-2075.

[GHERNAOUTI-HELI] GHERNAOUTI-HELI (S.), *Sécurité informatique et réseaux*, Dunod.

[JOLY-PASSANT] JOLY-PASSANT (E.), *Le décret du 31 mars 2001 pris pour application de l'article 1316-4 du Code civil et relatif à la signature électronique*, Lamy : droit de l'immatériel, 2000, n° 137, 2001, pp. 1-9.

[RIETSCH] RIETSCH (J-M), ET AL., *Dématérialisation et archivage électronique : mise en oeuvre de l'ILM*,Dunod.

[SCHWARTZ] SCHWARTZ (T.), *Dématérialisation et archivage électronique : mise en oeuvre de l'ILM*, Micro Application.

Sitographie

[TRUDEL] TRUDEL (P.), *De la "surveillance" à la qualité : les fondements actualisés du droit de la protection des données personnelles dans le gouvernement en ligne*, in *Administration électronique et qualité des prestations administratives*, Tunis, 2006, pp. 29-44.

[w_Certeurope] *http://www.certeurope.fr/*

[w_CNIL] *http://www.cnil.fr/*

[w_Legifrance] *http://www.legifrance.gouv.fr*

[w_Service Public] *http://mon.service-public.fr/*