DÉMATÉRIALISATION ET CRYPTAGE

Dématérialisation des documents et des procédures :

Techniques de dématérialisation et logiciels employés ;
Cryptage et techniques d'authentification ;
Transmission sécurisée.

Par
Vanessa GIACOMONI
Mars 2016

DÉMATÉRIALISATION DES DOCUMENTS :

I.1.DEFINITION:

DÉMATÉRIALISER un document consiste à transférer le contenu textuel et graphique d'un document codé d'une façon "analogique" sur un support de type "papier" vers un support informatique supportant cette information codée sous forme DIGITALE.

Par extension, la DÉMATÉRIALISATION DES DOCUMENTS tend à favoriser l'utilisation de documents sous forme numériques dans le cadre d'une activité donnée, jusqu'à extinction de l'utilisation des supports "papier" où à leur réduction au strict nécessaire.

I.2.DEMATERIALISATION DANS L'ADMINISTRATION FRANÇAISE:

- L'année 2012 a marqué l'achèvement du processus de dématérialisation des procédures de marchés publics (Les collectivités locales ne sont assujetties à cette mesure que pour les marchés d'un montant supérieur à 90 000 € HT).
- Les administrations peuvent depuis le 1er janvier 2012 être en mesure de recevoir des factures dématérialisées;
- Le PLAN FRANCE NUMÉRIQUE 2020 prévoit que « le papier devra être définitivement abandonné et l'intégralité des démarches administratives devront être dématérialisées.».

I.3.DÉMATÉRIALISATION NATIVE ET DÉMATÉRIALISATION A POSTERIORI:

- Lorsque les documents (par exemple les factures) arrivent ou sont créés sous forme électronique dans l'organisation, on parle de dématérialisation NATIVE.
- En revanche, la DÉMATÉRIALISATION A POSTERIORI permet de traiter un document entrant sous forme "papier" dans l'entreprise, moyennant une étape de NUMÉRISATION

En général, une démarche de dématérialisation ne peut se passer d'une première phase de dématérialisation à posteriori, afin de gérer l'existant (documents entrants et archives sous forme papier, documents ayant une valeur légale, etc.).

DÉMATÉRIALISATION DES DOCUMENTS :

I.4.AMELIORATIONS ATTENDUES:

I.4.1.ECONOMIES DE RESSOURCES:

- Un document dématérialisé nativement devrait engendrer des économies sur les coûts liés au papier, à la photocopie, etc., **à condition qu'il ne soit jamais imprimé en interne**. Cependant, un support électronique consomme aussi des ressources (espace de stockage, connexion réseau pour accéder au contenu, etc.) ;
- Un document dématérialisé a posteriori existe bien sous forme papier : il n'y a donc pas vraiment déconomie de ce côté là.

I.4.2.PARTAGE D'INFORMATIONS PLUS RAPIDE ET PLUS AISE:

Plusieurs personnes peuvent consulter simultanément un document numérisé sur un serveur. D'autre part, faire une copie en local devient extrêmement facile et peu coûteux, même si on imprime le document (économies de photocopie)

I.4.3.AMÉLIORATION DE L'INDEXATION DES DOCUMENTS:

Lorsqu'un document électronique est placé dans une structures de type BASES DE DONNÉES, son indexation est beaucoup plus facile qu'une indexation manuelle de documents papier. Cela facilite et accélère également les opérations de classement, de constitution d'index, etc., grâce à des procédures automatisées beaucoup plus rapides que leurs équivalentes manuelles.

I.4.4.AMELIORATION DES LES PROCÉDURES DE SAUVEGARDE:

Il est bien plus facile et moins coûteux d'assurer la protection de documents électroniques que de documents "papier" :

- La duplication d'un document électronique est très rapide et pratiquement gratuite ;
- Les documents électroniques sont INALTÉRABLES (à condition de bien traiter leurs supports et de renouveler régulièrement les sauvegardes) ;
- Les documents et leurs sauvegardes utilisent beaucoup moins de volume de stockage ;
- Les procédures de sauvegarde peuvent être automatisées, ce qui rend moins fastidieux pour les utilisateurs ce type d'activité.

DÉMATÉRIALISATION DES DOCUMENTS :

I.4.AMELIORATIONS ATTENDUES:

I.4.5.DIMINUTION DES COÛTS ET DE LA DURÉE DES TRAITEMENTS :

- Les applications de WORKFLOW (contrôle du flux de travail) permettent de contrôler et d'optimiser la circulation des documents entre les différents utilisateurs (créateur, approbateur, etc.), ce qui permet de minimiser certaines tâches fastidieuses (séances de paraphage des documents...)
- Diminution des FRAIS D'ENVOI par utilisation de la messagerie.

I.4.6.AMELIORATION DE LA SÉCURITÉ:

La possibilité de CRYPTER les documents numériques contenant des informations personnelles sensibles ou des informations protégée est bien évidemment un facteur d'amélioration de la sécurité contre les vols de supports ou les intrusions dans le système d'information.

I.4.7.FACILITE D'ÉVOLUTION DU CONTENU :

Il est évidemment beaucoup plus facile et beaucoup moins onéreux de faire évoluer le contenu d'un document numérique que celui d'un document "papier". Il faut toutefois mettre en place un mécanisme de GESTION DES VERSIONS pour éviter la perte d'informations au fur et à mesure des évolutions.

I.5.CONTRAINTES:

- ***AUTHENTIFICATION*** : Lorsque des documents ont besoin d'être AUTHENTIFIES, il faut utiliser des systèmes de SIGNATURE NUMÉRIQUE, basés sur des algorithmes de cryptage asymétriques. Ces systèmes permettent de certifier l'IDENTITÉ du signataire et l'INTÉGRITÉ du contenu ;
- ***HORODATAGE :*** lorsque la date de début de validité d'un document est importante, il faudra recourir à un HORODATAGE automatique ;
- ***SÉCURITÉ DE TRANSMISSION*** : les documents à contenu sensible devront être CRYPTES (Cryptage asymétrique) et transmis sur des canaux sécurisée (HTTPS – TSL/SSL).

II.DEMATÉRIALISATION DES PROCÉDURES:

II.1.DEFINITION:

La dématérialisation des DOCUMENTS n'entraîne pas forcément la dématérialisation des PROCÉDURES qui utilisent ces documents.

Ainsi, dans le cadre d'une entreprise, les employés peuvent avoir la possibilité de remplir leurs demandes de congés sur des FORMULAIRES MODIFIABLE (documents numérisés) récupérés sur un serveur, puis d'adresser ces documents par mail à la DRH : il s'agit là d'une dématérialisation des demandes de CP mais non d'une dématérialisation de la PROCÉDURE de demande de congés payés : pour parler de la dématérialisation de cette procédure, il faut que l'utilisateur puisse saisir EN LIGNE sa demande et simplement la valider pour qu'elle soit insérée dans la liste des demandes en attente.

La DÉMATÉRIALISATION DES PROCÉDURES est réalisée par le biais d'applications transactionnelles hébergées par des SERVEURS et accessibles aux utilisateurs par le biais de réseaux : réseau local pour les procédures internes à une entreprise, réseau internet pour les procédures publiques (déclaration URSSAF, etc.). On parle alors de TÉLÉPROCÉDURES.

Ces applications transactionnelles sont en général des SITES WEB (internes ou publics).

II.2.AVANTAGES DES TELÉPROCÉDURES:

- Les téléprocédures imposent de fait une dématérialisation des documents, avec tous les avantages liés à ces pratiques.
- Les téléprocédures facilitent et accélèrent les démarches des utilisateurs (dans la mesure où ceux-ci maîtrisent l'outil informatique).
- Les téléprocédures dispensent les utilisateurs de conserver des archives de leurs documents : en effet, ces documents numérisés sont conservés au niveau des serveurs qui assurent également leur sauvegarde. Les utilisateurs peuvent y accéder à tout moment.

II.DÉMATÉRIALISATION DES PROCÉDURES:

II.3.CONTRAINTES LIÉES AUX TÉLÉPROCÉDURES:

II.3.1.IDENTIFICATION DES ACTEURS :

Lors d'une transaction utilisant une téléprocédure, il est indispensable que le CLIENT (Utilisateur) et le SERVEUR (Logiciel délivrant le service) soient formellement identifiés. En effet :

- Un utilisateur peut tenter d'usurper l'identité d'un autre utilisateur afin d'accéder à ses données personnelles sur le serveur et effectuer diverses actions frauduleuses (transfert de fonds, etc.) ;
- Par diverses manœuvres, un serveur peut être substitué au serveur gérant une téléprocédure, dans le but de "pirater" les données du client (code de carte de crédit, etc.).

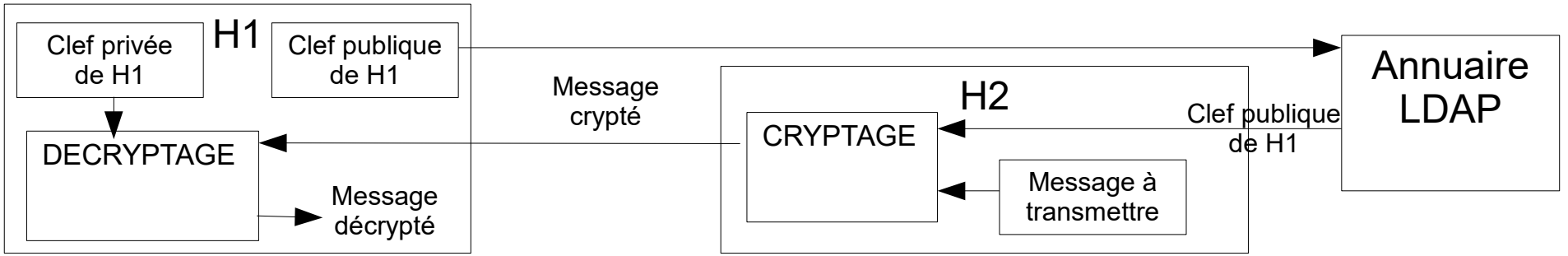
L'identification du client et du serveur peut être effectuée par le mécanisme des CERTIFICATS, en utilisant le protocole HTTPS, basé sur le protocole de tranports TSL/SSL.

II.3.2.PROTECTION DES DONNEES ECHANGEES:

Les données échangées entre le client et le serveur peuvent faire l'objet de tentatives d'INTERCEPTION lorsqu'elles circulent sur les réseaux. Le seul moyen de protéger les données sensibles est de recourir aux techniques de CRYPTAGE des données, également intégrée dans le protocole HTTPS.

Le système de cryptage le plus répandu (et le plus sûr actuellement) est le CRYPTAGE ASYMÉTRIQUE Ce mode de cryptage est basé sur le système suivant :
Tout utilisateur désirant communiquer par message crypté doit être muni de 2 CLEFS :

- Une CLEF PUBLIQUE qui est accessible à tout utilisateur et qui permet de CRYPTER les données.
- Une CLEF PRIVÉE ou SECRÈTE qui ne doit être connue que de cet utilisateur et qui lui permet de DÉCRYPTER les données cryptées par sa CLEF PUBLIQUE.



II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.1.LES LOGICIELS DE DÉMATÉRIALISATION:

III.1.1.DÉFINITION:

Ils permettent de transformer un document "Papier" en un document NUMÉRIQUE. Ils interviennent donc dans le cadre de la dématérialisation NON NATIVE.

III.1.2.ETAPES DE LA DÉMATÉRIALISATION:

Les logiciels de dématérialisation travaillent à partir d'un FICHIER IMAGE NUMÉRIQUE du document papier, obtenue soit en SCANNANT ce document, soit en le PHOTOGRAPHIANT (à l'aide d'un téléphone portable, par exemple). Une fois cette image obtenue, les logiciels procèdent en 5 étapes:

ETAPE	CONTENU
PRE-ANALYSE	Consiste à améliorer les caractéristiques de l'image (contraste, balance des couleurs, etc.) pour faciliter la suite des traitements.
SEGMENTATION	Le logiciel essai de segmenter l'image numérique en différentes zones (lignes et caractères, zone d'image, cadre, etc.)
RECONNAISSANCE DE CARACTERES	Dans les zones identifiées comme correspondant à des caractères, le logicielapplique des algorithmes de reconnaissance de formes pour essayer d'identifier le caractère représenté.
POST-TRAITEMENT	Ces traitements consistent à appliquer sur les suites de caractères obtenues des rêgles linguistiques ou tenant compte du contexte pour essayer de réduire le nombre des erreurs laissées par la reconnaissance de formes.
GENERATION DU FORMAT DE SORTIE	Enfin, le document est remis en forme dans le format choisi par l'utilisateur.

II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.1.LES LOGICIELS DE DEMATERIALISATION:

III.1.3.LOGICIELS DE DEMATERIALISATION:

Logiciels libres: TESSERECT, GOCR, etc.
Logiciels commerciaux: Suite DOCUMALIS, DOCUMENT READER, FINEREADER, etc.

III.1.4.TECHNIQUES DE RECONNAISSANCE DE CARACTÈRES:

OCR: Optical Character Recognization.

- CLASSIFICATION PAR CARACTÉRISTIQUES: la forme est représentée par un vecteur de valeurs numériques représentatif des caractéristiques de cette forme et comparée à une bibliothèque de formes.
- MÉTHODE MÉTRIQUE: les caractéristiques métriques de la forme (proportions des différents éléments, etc.) sont comparées à un ensemble de modèles de formes.
- MÉTHODE STATISTIQUE: Cette méthode est basée sur des probabilités.

II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.2.NOTIONS DE CRYPTAGE:

III.2.1.CLEF DE CHIFFRAGE:

Supposons que nous ayons un message M à crypter, M étant composé d'une série d'éléments représentables par des nombres entiers (Par exemple, une série de caractères) : M = { C_1, C_2, …,C_n}. Une méthode de cryptage peut consister à appliquer aux différents éléments une fonction mathématique dont le résultat sera également un nombre entier :

Ex : pour tout caractère X du message, $\mathbf{X_c = M*X - N}$ (M et N étant des nombres entiers, $\mathbf{X_c}$ étant la valeur cryptée).

Dans ce cas, on peut dire que:

- L'algorithme : $\mathbf{M*X - N \rightarrow X_c}$ est l'ALGORITHME DE CRYPTAGE
- le couple de valeurs (M, N) constitue la CLEF DE CRYPTAGE

On peut donc définir une CLEF DE CRYPTAGE comme une suite de valeurs qui permettent de paramétrer un ALGORITHME DE CRYPTAGE.

III.2.2.CRYPTAGE SYMÉTRIQUE:

Dans le cas précédent, l'algorithme qui permet de décrypter les éléments cryptés se déduit facilement de l'algorithme de cryptage et de la valeur de la clef : $\mathbf{(X_c + N)/M \dashrightarrow X}$.

Ex :
X = 5, M=2, N=1
$X_c = 2*5-1 = 9$
X = (9+1)/2 = 5

Pour décrypter le message transmis, le récepteur n'a donc besoin que de connaître la valeur de la CLEF DE CRYPTAGE et le type d'algorithme de cryptage utilisé. Un tel CRYPTAGE où la clef sert à la fois pour crypter et pour décrypter est dit SYMÉTRIQUE

Le problème principal d'un cryptage symétrique est que la clef doit rester secrète, sauf pour l'émetteur et pour le récepteur. Ceci pose 2 problèmes :

- La TRANSMISSION SÉCURISE de la clef au récepteur ;
- Le fait qu'une clef ne peut **servir qu'une fois.**

II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.2.NOTIONS DE CRYPTAGE:

III.2.3.CRYPTAGE ASYMÉTRIQUE:

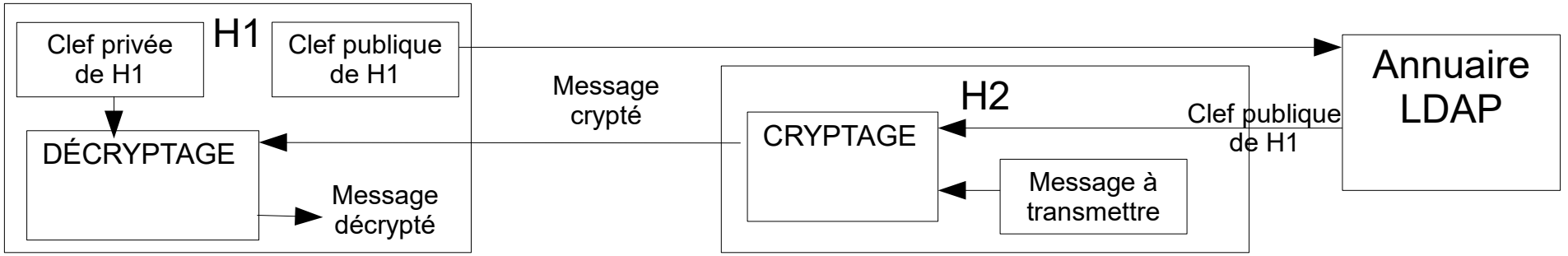
Le CRYPTAGE ASYMÉTRIQUE utilise des algorithmes de chiffrage DIFFICILEMENT RÉVERSIBLES, c'est à dire pour lesquels il est extrêmement difficile de retrouver la **fonction de déchiffrage** à partir de la **fonction de chiffrage**. C'est le cas par exemple de l'algorithme RSA qui se base sur la difficulté de retrouver le **facteur premier de plus grande valeur** d'un très grand nombre N à partir de la donnée de ce nombre (le seul moyen est d'essayer tous les nombres inférieurs à N).

De ce fait, dans ce type de chiffrage, on utilise 2 algorithmes : un algorithme pour chiffrer et un autre pour déchiffrer, chacun de ces algorithmes possédant sa propre clef de chiffrage :

- A l'ALGORITME DE CHIFFRAGE est associé la CLEF PUBLIQUE;
- A l'ALGORITME DE DÉCHIFFRAGE est associé la CLEF PRIVÉE (Ou CLEF SECRÈTE) ;

La CLEF PUBLIQUE d'un utilisateur A peut être connue de tous : elle peut être transmise à un utilisateur sur un canal non crypté (mail) ou encore être mise à disposition du public dans un ANNUAIRE LDAP: tout utilisateur B peut donc récupérer cette clef pour adresse à A un message crypté.

En revanche, la CLEF PRIVÉE ne doit être connue que de A, qui va l'utiliser pour décrypter les messages cryptés avec sa clef publique (De fait, il n'y a aucun besoin de transmettre cette clef privée)



II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.3.SIGNATURE NUMÉRIQUE:

III.3.1.DEFINITION :

La SIGNATURE NUMÉRIQUE (ou SIGNATURE ÉLECTRONIQUE) est un mécanisme permettant de garantir l'**intégrité** d'un document électronique et d'en **authentifier** l'auteur, par analogie avec la signature manuscrite d'un document papier. En pratique, elle correspond à une **suite de caractères**.

Un mécanisme de signature numérique a pour fonctions de garantir :

- L'IDENTIFICATION DE L'AUTEUR : le lecteur d'un document doit pouvoir identifier la personne ou l'organisme qui a apposé sa signature, c'est à dire l'AUTHENTIFIER.
- L'INTÉGRITÉ DU DOCUMENT: c'est à dire prouver que le document n'a pas été altéré entre l'**instant où l'auteur l'a signé** et le moment où le **lecteur le consulte**.

III.3.2.PROPRIETES :

Pour avoir la même valeur qu'une signature graphique manuelle, une SIGNATURE ÉLECTRONIQUE doit également être :

- **Infalsifiable :** ou du moins très difficile à falsifier ;
- **Non réutilisable :** la signature **fait partie du document signé.** Elle ne peut être associée à un autre document par quelque procédé que ce soit ;
- **Inaltérable :** Une fois qu'un document est signé, on ne peut plus le modifier.
- **Irrévocable :** (ou encore **non répudiable**) la personne qui a signé un document ne peut le nier.

II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.3.SIGNATURE NUMÉRIQUE:

III.3.3.METHODE DE GÉNÉRATION D'UNE SIGNATURE ÉLECTRONIQUE :

La plupart des procédés de génération de signature numérique s'appuie sur la **cryptographie asymétrique.** Ce qui suit décrit les étapes de la mise en place d'une signature électronique :

Supposons qu'un particulier ou un organisme quelconque E veuille envoyer à un autre particulier ou un organisme R un message dont l'AUTHENTICITÉ puisse être vérifiée (par exemple, un fichier M quelconque qui peut être assimilé à un fichier texte) :

CHOIX D'UN SYSTÈME DE SIGNATURE :

E et R doivent avoir convenu du choix d'un système de signature, caractérisé par :

- Un système de chiffrement asymétrique avec clef publique (Cpu) et clef privée (Cpr). Soit Fc la fonction de chiffrement et Fd la fonction de déchiffrement;
- une FONCTION DE HACHAGE notée H. Une fonction de Hachage permet de construire à partir d'un message quelconque une "image simplifiée" de ce message appelée EMPREINTE ou CONDENSAT (par exemple, une empreinte pourrait être la suite des initiales ses mots composant le message : une empreinte doit être suffisamment caractéristique pour que la probabilité que deux messages différents aient la même empreinte soit très faible).

PRÉPARATION ET ÉMISSION DU MESSAGE SIGNÉ :

- E crée une EMPREINTE (CONDENSAT) du message en utilisant la fonction de hachage : Em = H(M) ;
- E chiffre cette empreinte avec fonction de chiffrement Fc en utilisant sa clé privée Cpr. Le résultat est la SIGNATURE DU MESSAGE (SM = Fc(Cpr, Em) ;
- Le message en clair M et la signature SM sont alors placés dans un conteneur quelconque: CM=(SM, M). Ce conteneur peut alors être transmis à R sur un canal non protégé.

II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

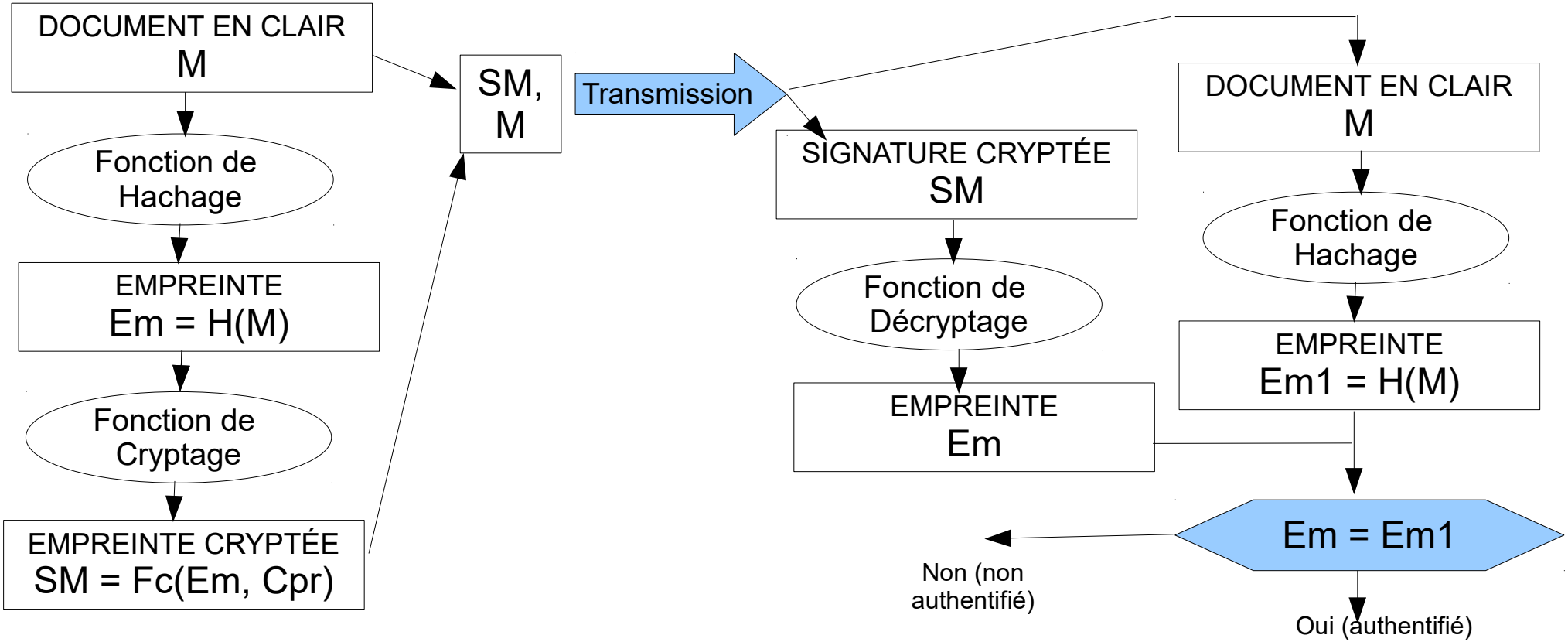
III.3.SIGNATURE NUMÉRIQUE:

III.3.3.METHODE DE GÉNÉRATION D'UNE SIGNATURE ÉLECTROTECHNIQUE :

RÉCEPTION DU MESSAGE ET AUTHENTIFICATION :

R réceptionne alors le message signé (Message en clair M+Signature SM). Il lui reste à vérifier l'AUTHENTICITÉ du message. Pour cela :

- Il crée alors une EMPREINTE du message en clair M qu'il a reçu en utilisant la fonction de hachage convenue: Em1 = H(M) ;
- Il déchiffre la signature en utilisant la fonction de déchiffrement Fd et la clé publique Cpu : DSM =Fd(Cpu,SM) ;
- Si la signature est authentique, DSM doit correspondre à l'empreinte du message M reçu, soit H(M).



II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.4.LES CERTIFICATS:

III.4.1.PRINCIPES :

Les systèmes de CHIFFREMENT ASYMÉTRIQUES (sur lesquels sont basés les système de SIGNATURE NUMÉRIQUES), exigent le partage de CLEFS PUBLIQUES entre l'émetteur et le récepteur : l'émetteur a besoin de la CLEF PUBLIQUE du récepteur pour CHIFFRER le message. Le partage de cette clef se fait en général :

- Soit par l'intermédiaire d'un SITE WEB sécurisé ;
- Soit par l'intermédiaire d'un ANNUAIRE ÉLECTRONIQUE PUBLIC (Annuaire LDAP) sur lequel l'émetteur se procure la clef publique du récepteur.

Dans les deux cas, rien ne garantit formellement que la clef récupérée par l'émetteur soit la bonne. En effet, le site web ou l'annuaire peuvent avoir été piratés et la clef envoyée peut en fait être la clef publique du pirate, ce qui permettra à celui-ci de déchiffrer les messages avec sa clef privée.

Le système des CERTIFICATS tend à éviter ce genre de piratage en associant à la CLEF PUBLIQUE d'une entité un CERTIFICAT qui garantit l'IDENTITÉ DU PROPRIÉTAIRE DE LA CLEF.

Un certificat est donc la CARTE D'IDENTITÉ du propriétaire d'une CLEF PUBLIQUE
il permet d'AUTHENTIFIER cette clef publique.

Les CERTIFICATS sont délivrés par des tiers appelés AUTORITÉS DE CERTIFICATION

II.TECHNIQUES LIÉES A LA DÉMATÉRIALISATION

III.4.LES CERTIFICATS:

III.4.2.STRUCTURE D'UN CERTIFICAT :

La structure d'un certificat est normalisée par la norme X509 de l'UIT (Union Internationnale des Communications). Un certificat est un FICHIER comprenant deux parties. Une partie contient des informations relatives au certificat lui-même, une autre partie contient la signature de l'autorité de certification :

Première partie :

- Version de la norme X509 utilisée
- Numero de série du certificat
- Nom de l'autorité certificatrice ;
- Dates de debut et de fin du certificat ;
- Clef publique du propriétaire du certificat (Ex : 1a:5b:3c:5a:35:4b:d8:54:4c)
- Signature de l'émetteur du certificat ;
- Algorithme de chiffrement utilisé pour chiffrer la signature de l'autorité certificatrice (Ex : Algorithme RC5).

Deuxième partie :

- Signature de l'autorité certificatrice (cette signature permet d'authentifier les informations contenues dans la première partie).

III.4.3.UTILISATION D'UN CERTIFICAT :

- L'utilisateur qui veut communiquer avec une entité E se procure le certificat de cette entité auprès d'une AUTORITE CERTIFICATRICE.
- Il applique alors la **fonction de Hachage** aux informations de la première partie pour obtenir une EMPREINTE de cette première partie telle qu'il l'a reçue.
- D'autre part, il déchiffre la signature de l'autorité certificatrice à l'aide de la CLEF PUBLIQUE de celle-ci : il obtient donc l'EMPREINTE de cette première partie telle que l'autorité administrative la lui a transmise.
- Il lui suffit alors de comparer les deux empreintes pour être sûr que le certificat est AUTHENTIQUE. Ceci entraîne l'authentification de la CLEF PUBLIQUE du PROPRIÉTAIRE du certificat.

III.4.LES CERTIFICATS:

III.4.4.CERTIFICATS AUTO SIGNES :

Certains certificats sont à usage interne à l'intérieur d'une organisation. Dans ce cas, ils peuvent ne pas être délivrés par une autorité certificatrice, mais simplement par un serveur interne ; On parle alors de CERTIFICATS AUTOSIGNÉS

III.4.5.USAGE DES CERTIFICATS :

CERTIFICAT CLIENT :

Il est stocké sur un poste utilisateur ou embarqué sur une carte à puces. Il permet d'identifier cet utilisateur et de lui attribuer des droits. Il est transmis lors de l'ouverture d'une SESSION SÉCURISÉE (HTTPS). C'est la CARTE D'IDENTITÉ du CLIENT.

CERTIFICAT SERVEUR :

Il permet de relier le SERVICE offert par ce serveur au propriétaire du serveur. C'est donc la CARTE D'IDENTITÉ du propriétaire du serveur. En particulier, il permet de certifier que l'URL (et surtout le DOMAINE contenu dans cette URL) appartient bien à l'entreprise qui contrôle le site web. D'autre part, il est utilisé par les protocoles SSL/TSL en dessous de HTTPS.

CERTIFICAT VPN :

Ce type de certificat est installé sur les équipements réseau. Il permet de chiffrer les communications de bout en bout.

II.TECHNIQUES LIÉES À LA DÉMATÉRIALISATION

III.5.LE PROTOCOLE HTTPS:

Le protocole HTTPS (HyperText Transfer Protocol Secure) est la combinaison du HTTP avec une COUCHE DE CHIFFREMENT. HTTPS est implanté au dessus de cette couche de chiffrement (En général SSL ou TSL).

HTTPS permet au visiteur de VÉRIFIER L'IDENTITÉ DU SITE WEB auquel il accède, grâce à un CERTIFICAT D'AUTHENTIFICATION émis par une autorité tierce.

HTTPS garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur. Il peut permettre de valider l'identité du visiteur si celui-ci utilise également un CERTIFICAT D'AUTHENTIFICATION CLIENT.

Transport Layer Security (TLS), et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet. Ils fonctionnent suivant un mode client-serveur et permettent :

- L'authentification du SERVEUR ;
- La CONFIDENTIALITÉ des données échangées (ou session chiffrée) ;
- L'INTÉGRITÉ des données échangées ;
- L'authentification du CLIENT (en réalité celle-ci est souvent assurée par le serveur).

Les protocoles de la couche application, comme HTTP, n'ont pas à être profondément modifiés pour utiliser une connexion sécurisée, mais seulement implémentés au-dessus de SSL/TLS, ce qui pour HTTP a donné le protocole HTTPS.