Les contrats

Qu'est ce que c'est ?

Convention, accord de volontés ayant pour but d'engendrer une obligation d'une ou de plusieurs personnes envers une ou plusieurs autres.

Qu'est ce que c'est ?

Quatre conditions sont nécessaires pour la validité du contrat :

-le consentement des parties,

-la capacité de contracter,

-un objet certain,

-une cause licite.

Qu'est ce que c'est ?

Acte authentique qui constate cette convention : Signer un contrat. **Contrat notarié**.

Simple accord fondé sur la seule bonne foi : **Contrat verbal**.

La phase pré-contractuelle

La phase pré-contractuelleest la phase préliminaire à l'élaboration du contrat.

La phase pré-contractuelle

Elle est marquée par les négociations, parfois acharnées, au cours desquelles les parties doivent veiller à ne pas s'engager, même de manière implicite.

La phase pré-contractuelle

De plus, les échanges d'informations sensibles entre le client et le professionnel ne devrait pas amener l'une ou l'autre des parties à révéler des données privées ou confidentielles – ne pas en dire trop, en somme.

La phase pré-contractuelle

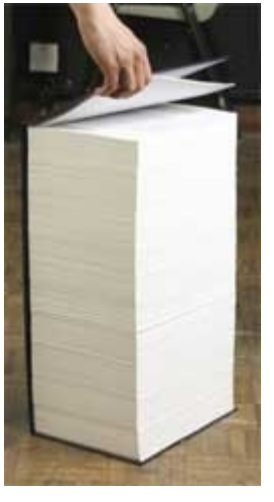
Enfin, le professionnel ou le client ne doivent pas s'induire l'un ou l'autre en erreur, sinon le contrat, une fois signé, pourrait être invalidé pour cause de mauvaise information ou d'information insuffisante.

De cette manière, si ces trois conditions sont respectées, le socle du contrat est correct pour les deux parties.

Obligations fondamentales

Les deux tenants du contrats ont deux obligations fondamentales :

L'obligation d'information : le professionnel doit s'efforcer de donner toute information susceptible d'aiguiller le client dans son engagement, en enrichissant le cahier des



Obligations fondamentales

L'obligation de moyen et l'obligation de résultat :

Pour l'**obligation de moyen**, on s'oblige à mettre en œuvre tous les éléments à sa disposition dans l'état de l'art pour atteindre le résultat

exemple : un médecin mettra tout en œuvre pour soigner son patient.

L'**obligation de résultat** : le signataire ne s'engage pas sur les moyens utilisés, il peut utiliser ce qu'il veut, mais il s'engage à un résultat fixé, à une date donnée.

De manière alternative, il est judicieux de nuancer les deux obligations en fixant un résultat minimum (50% à 80% de ce qui est prévu), avec une obligation de moyen.

Eléments du contrat

Forme du contrat

- Il est obligatoire de bien définir la **langue** de rédaction. Il faux choisir une langue commune aux deux partis.
- Signalons également que le contrat doit être **signé** par les deux partis afin d'être valide...
- Iil faut éviter **ratures** ou **surcharges**.
- Ceci est particulièrement valable pour les contrats à distance, ou les négociations ne mettent pas toujours les deux contractants en présence physique.

Territoire

- Il est essentiel de spécifier le territoire sur lequel le logiciel doit être installé, notamment pour les problèmes de gestion et de contrôle des licences.
- Ceci est valable pour les exploitants, mais à plus forte raison pour les distributeurs de logiciel.

Durée du contrat

- Il faut définir la durée de l'engagement, s'il est renouvelable automatiquement ou tacitement, ainsi que gérer les dépassements de temps.

Fin du contrat et modalités de résiliation

- Elle concernent la fin anticipée de l'accord, et donc quelles sanctions sont encourues.
- Les clauses pénales prévoient le plus souvent des sanctions financières, par exemple dans le cas où l'un ou l'autre des cocontractant mettrait fin au contrat de manière inopportune, ou en cas de non respect d'une obligation.
- Il vaut mieux encore poser des clauses qui s'appuient sur un découpage de prestations de l'objectif, par exemple découper en modules, dans le cas d'un logiciel.

Prix et modalités de paiement

- C’est mieux de spécifier le prix dans le contrat, mais aussi la devise utilisée, si les taxes sont incluses ou pas, et indiquer également les modalités et les techniques de paiement : chèque, carte bancaire, virement, liquide, lettre de change, en nature, ou troc.

Clause de propriété intellectuelle sur le produit

- Cette clause règle définitivement le problème de l'étendue ce que l'on confère au client : la pleine propriété du logiciel, ou simplement des licences d'utilisation.
- Il peut également y avoir litige sur la propriété intellectuelle des outils de développements ou de recherche d'informations employés, outils qui ont été développés le plus souvent par la SSII pour son usage personnel, et qui désire les garder pour continuer à développer. Il faut alors être très prudent et ne pas laisser penser au client que ces outils lui sont concédés, en spécifiant explicitement que les documents et les outils de travail sont protégés par les droits de propriété intellectuelle.

Limitation de responsabilité

- le fournisseur peut limiter sa responsabilité, mais en aucun cas l'annihiler.

  dommage dû au produit développé par le fournisseur.

Clause de confidentialité

- Elle délimite un périmètre d'information pour le prestataire et le client, pour que des éléments sensibles ne tombent pas entre des mains indélicates (listes de clients, de tarifs préférentiels, de numéro de cartes de crédit, etc.).

Clause de garantie

- Pour tout ce qui est prestation de service, il s'agit d'un contrat d'entreprise, qui ne contient aucune garantie implicite, contrairement aux garanties contractuelles qui bénéficient de la garantie légale, la garantie des vices cachés (erreur de conception, etc.), valable à perpétuité.
- souvent très courte : de trois moins à un an. respect du manuel maintenance...

Clause de non-concurrence

- L'entreprise s'engage à ne pas prospecter un certain type de marché pendant un temps déterminé. Ce type de clause ne vise qu'à empêcher la concurrence malhonnête, déloyale, sans porter atteinte à la concurrence normale entre entreprises de même secteur d'activité.

Clause de non sollicitation de personnel

- Il peut arriver qu'une entreprise cliente trouve plus rentable de prendre à son compte un employé de la société de service, plutôt que de payer le service lui-même.

Clause de cession et de circulation du contrat

Cette clause règle le sort de contrats signés avec une entreprise qui s'est faite par la suite rachetée par une autre, ou bien qui s'est divisée en plusieurs entreprises. Elle est utile pour se prémunir des contraintes économiques engendrées lorsque, par exemple, c'est un concurrent qui met la main sur le contrat. Du point de vue du client, il n'a pas forcément à interdire la circulation du contrat si son fournisseur fait faillite. Il y a également possibilité de se réserver le droit de réserve sur un éventuel transfert. Lorsqu'une condition suspensive est intégrée, soit il y a agrément du tiers (pour les fusion et les scission), soit application des conditions de rupture.

Clause de livraison et de recette

On parle de recette quand il s'agit d'application, de logiciels pour un client (contrats 'clé en main') ; et de livraison pour ce qui concerne le matériel. Cette clause détermine le support employé pour livrer le produit (implique selon le cas des compétences d'installation spécifiques), les dates des étapes de la recette ou livraison, les conditions d'acceptation du produit. Il faut savoir que la garantie démarre à l'acceptation totale de la recette, donc on a intérêt à faire plutôt des acceptations sous réserve en cas de doute. Si la recette est partielle, la garantie est retardée d'autant de temps : le contrat n'est pas totalement accepté. La méthode couramment employée est d'instituer une Vérification Service Régulier (VSR) entre la recette provisoire et la recette définitive. Pendant cette période, qui peut durer jusqu'à deux ans dans certains cas, le système est utilisé dans les conditions normales de l'entreprise, mais il est encore à l'essai. Après, si le client est satisfait, il signe la recette définitive, puis la garantie contractuelle prend le relais pour quelques mois encore.

Clause compromissoire

Cette clause est un technique juridique qui consiste à soustraire à l'autorité des juges les problèmes pouvant survenir entre les cocontractants. Ils choisiront un tribunal arbitral, dont la composition sera déterminée. L'intérêt de cette clause repose sur sa vitesse, ses compétences (en effet, on pourra choisir des juristes qui ont des connaissances informatiques, par exemple), et que la décision est exécutable dans les pays des contractants au même titre qu'une condamnation judiciaire dite classique, et mettra en œuvre la force publique.

Licence

Definition

- Une licence de logiciel est un contrat par lequel le titulaire des droits d'auteur sur un programme informatique définit avec son cocontractant (exploitant ou utilisateur) les conditions dans lesquelles ce programme peut être utilisé, diffusé ou modifié.

Types de licences

- Licence fixe
- La licence fixe est conçue pour être installée sur un ordinateur particulier. Elle peut utiliser une caractéristique spécifique à cet ordinateur, comme son adresse Media Access Control (MAC) pour vérifier et contraindre la conformité de l'usage de la licence.
- Licence nominative
- La licence nominative, qui a remplacé la licence fixe, a pour but de permettre l'utilisation d'un logiciel sur un ordinateur définie avec une adresse MAC par exemple.
- Licence flottante
- La licence flottante fonctionne avec un ordinateur serveur de licence(s). Celui-ci décompte le nombre de licences utilisées à un instant « T » sur le réseau. Tant qu'au moins une licence reste disponible, tout ordinateur du réseau réclamant une licence se la verra affecter temporairement durant le temps d'utilisation du logiciel concerné.

Types de licences

- Shareware
- La licence shareware, ou partagiciel, attribue un droit temporaire et/ou avec des fonctionnalités limitées d'utilisation. Après cette période d'essai, l'utilisateur devra rétribuer l'auteur pour continuer à utiliser le logiciel ou avoir accès à la version complète.
- Licences libres
- Les licences de logiciel libre sont une forme particulière de licence : les licences libres qui garantissent quatre droits fondamentaux aux utilisateurs :
- usage de l'œuvre ;
- étude de l'œuvre pour en comprendre le fonctionnement ou l'adapter à ses besoins ;
- modification (amélioration, extension et transformation) ou incorporation de l'œuvre en une œuvre dérivée ;
- redistribution de l'œuvre, c'est-à-dire sa diffusion à d'autres usagers, y compris commercialemen

Licences de logiciels libres

- GPL ;
- Licence BSD ;
- Licence Apache ;
- Licence X11 ;
- Licence Publique Eclipse.
- Licences sur les « contenus » libres et/ou ouverts :
- GFDL ;
- Licence Art Libre ;
- Licence Creative Commons ;
- Skyolicense [archive] ;
- (en) Public Documentation License [archive].
- WTFPL ;

Méthode d'agrément du contrat

- Deux modes d'agréments, très couramment utilisés, sont critiqués car souvent considérés comme de la vente forcée :
- il peut y avoir un encart sur l'emballage du logiciel précisant que lorsqu'on ôte le cellophane ou un sceau autocollant, on accepte de fait le contrat qui est dans la boîte (qui n'a donc pas été lu). Elles sont nommées shrink-wrap licences en anglais ;
- pour les logiciels pré-installés ou ceux qui sont téléchargés à partir d'Internet, au moment de l'installation un écran informe de l'acceptation d'un texte écrit dans la fenêtre avant de pouvoir continuer. Certains logiciels d'installation refusent de continuer si l'on n'a pas fait défiler le texte jusqu'en bas (équivalent logiciel du « si vous n'avez pas tourné toutes les pages du contrat »). Elles sont nommées click-through licences en anglais.

La signature électronique

- La signature numérique (parfois appelée 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.

- Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères.

Fonctions de la signature

- Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature (propriété d'identification).
- Il doit garantir 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 (propriété d'intégrité).
-

Fonctions de la signature

Pour cela, les conditions suivantes doivent être réunies :

- Authentique : l'identité du signataire doit pouvoir être retrouvée de manière certaine.
- Infalsifiable : la signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre.
- Non réutilisable : la signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
- Inaltérable : un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
- Irrévocable : la personne qui a signé ne peut le nier.

La signature électronique dans le code algérien

- Depuis 2015, l'Algérie dispose d'un texte de loi nommé "Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er fèvrier 2015 fixant les règles générales relatives à la signature et à la certification électroniques" conférant à la signature électronique une légalité juridique c-à-d que la signature électronique est désormais comparable (aux yeux de la justice et de l'administration) à une signature manuscrite si elle est vérifiable par un tiers de confiance.
- Le texte se compose de 5 titres

Titre 1

- Le premier titre s'attache à définir les différents termes inhérents à la cryptographie et au domaine de la signature électronique ainsi que les principes généraux des dispositions de ce texte .

Titre 2

- Le deuxième titre se décompose en trois chapitres. Le premier chapitre s'intéresse aux principes d'assimilation et de non-discrimination de la signature électronique qui précisent la fonction et la qualification de la signature électronique élevée à l'occasion au même niveau que la signature manuscrite. Le second chapitre décrit les conditions de sécurité et de fiabilité des dispositifs de création et de vérification de la signature électronique qualifiée.

Titre 3

- Le troisième titre intitulé "Certification électronique" se décompose en deux chapitres distincts. Le premier chapitre précise la qualité d'un certificat électronique certifié par un tiers de confiance ou un prestataire de services de certification électronique conformément à la politique de certification électronique approuvée. Le deuxième chapitre annonce et définit le rôle de l'autorité administrative indépendante jouissant de la personnalité morale et de l'autonomie financière, dénommée autorité nationale de certification électronique. C'est un tiers de confiance officiel et gouvernemental directement rattaché au premier-ministre. Ce chapitre annonce aussi la création d'un second tiens de confiance gouvernemental rattaché au ministère de la poste et des technologies de la communications.

Titre 4

- Le quatrième titre composé de deux chapitres. Le premier instaure des sanctions pécuniaires et administratives à la charge du prestataire de services de certification électronique qui ne respecte pas les dispositions de son cahier des charges ou de sa politique de certification électronique approuvée par l'Autorité économique de certification électronique. Cette dernière prononce a son encontre une sanction pécuniaire dont le montant varie de deux cent mille dinars (200.000 DA) à cinq millions de dinars (5.000.000 DA), selon la classification des manquements, prévue dans le cahier des charges du prestataire et le met en demeure de se conformer auxdites dispositions dans un délai allant de huit (8) jours à trente (30) jours, selon le cas.

Titre 4

- Le second chapitre instaure des dispositions pénales, comme par exemple, à l'encontre de toute personne qui use de fausses déclarations pour l'obtention d'un certificat électronique qualifié. L'acte est puni d'une peine d'emprisonnement de trois (3) mois à trois (3) ans et d'une amende de 20.000 DA à 200.000 DA ou de l'une de ces deux peines seulement. Plusieurs autres cas sont aussi abordés comme par exemple : la divulgation des secrets de création d'une signature, le manquement à l'obligation d'identifier le demandeur du certificat ou enfin le fournissement au public des services de certification électronique sans autorisation ou tout prestataire de services de certification électronique qui reprend ou poursuit son activité après retrait de l'autorisation.

Titre 5

- Le dernier titre conclue avec les dispositions transitoires et finales qui finit de définir le caractère ofifciel de la signature électronique.

Annexe : Fonctionnement typique de la signature éléctronique

Supposons qu'Alice souhaite envoyer à Bob un message dont il puisse vérifier l'authenticité.Le message que souhaite envoyer Alice est un fichier binaire M de nature quelconque (texte, image, exécutable…) qui peut être assimilé à un fichier texte. Voici la description d'une méthode classique de signature par chiffrement asymétrique.

Mise en place d'une architecture de signature:

Alice et Bob ont convenu au préalable des choix :

un chiffrement asymétrique constitué d'une fonction de chiffrement C et d'une fonction de déchiffrement D ;

une fonction de hachage que nous noterons H.

Pour le chiffrement choisi, Alice a généré une clé privée Kpr et une clé publique Kpb :

elle transmet la clé Kpb à Bob par un canal non sécurisé (la clé publique n'est pas secrète) ;

elle garde la clé Kpr secrète.

C, D, H et Kpb n'ont pas besoin d'être secrets.

Préparation du message chiffré:

Alice prépare un message signé pour cela

elle produit un condensat du message par la fonction de hachage choisie H(M) ;

elle chiffre ce condensat grâce à la fonction de chiffrement C en utilisant sa clé privée Kpr. Le résultat obtenu est la signature du message : SM = C(Kpr,H(M)) ;

elle prépare le message signé en plaçant le message en clair M et la signature SM dans un conteneur quelconque : Msigné=(SM,M).

Alice transmet Msigné, le message signé, à Bob par un canal non sécurisé.

Réception du message signé

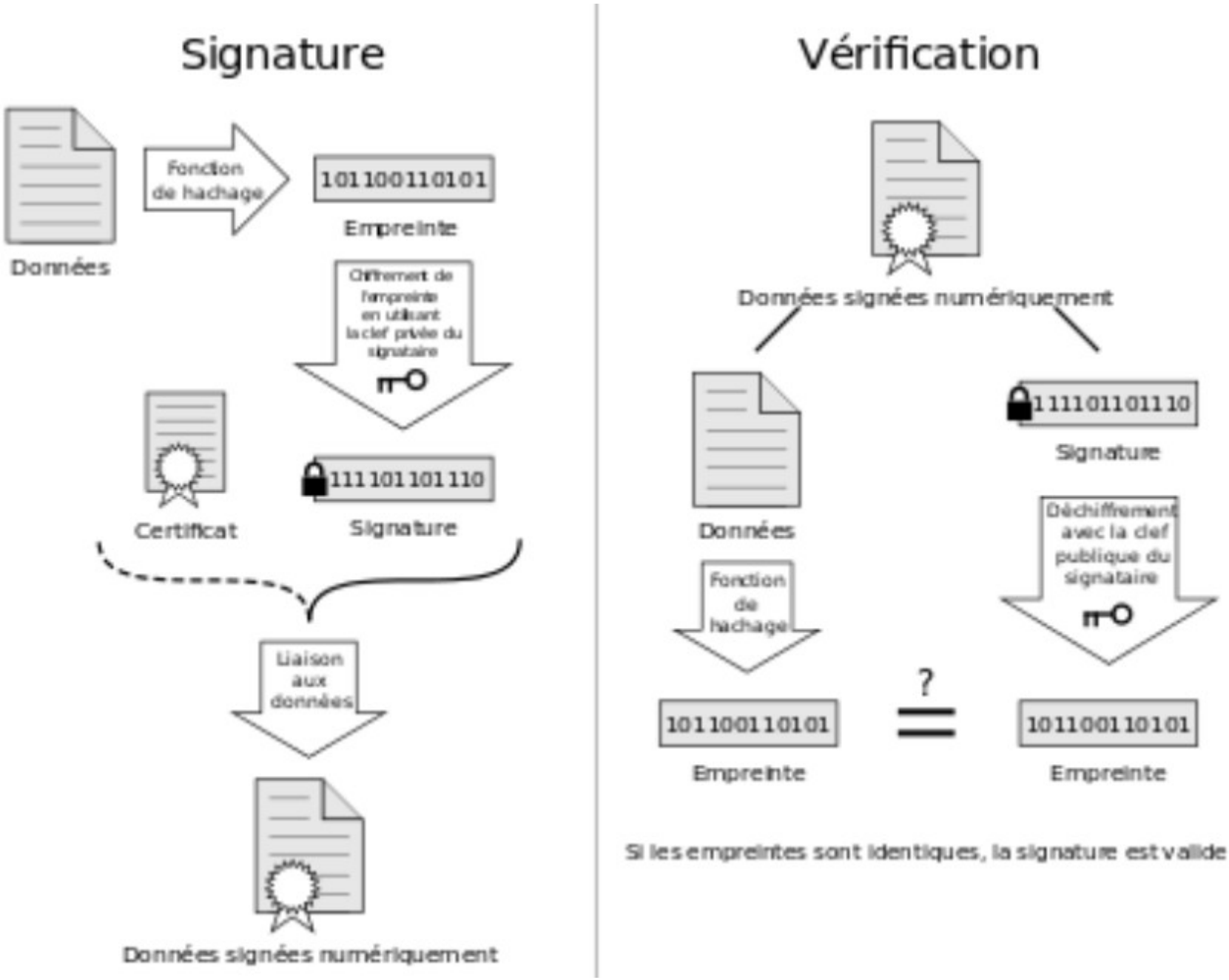
Bob réceptionne le message signé, pour vérifier l'authenticité du message

il produit un condensat du texte clair en utilisant la fonction de hachage convenue : H(M) ;

il déchiffre la signature en utilisant la fonction de déchiffrement D avec la clé publique Kpb soit : DSm=D(Kpb,SM) ;

il compare DSm avec H(M).

Dans le cas où la signature est authentique, DSm avec H(M) sont égaux car, par les propriétés du chiffrement asymétrique : DSm=D(Kpb,SM)=D(Kpb,C(Kpr,H(M)))=H(M), le message est alors authentifié.


Signature
Données
Fonction de hachage
101100110101
Empreinte
Chiffrement de l'empreinte en utilisant la clef privée du signataire
Certificat
111101101110
Signature
Liaison aux données
Données signées numériquement
Vérification
Données signées numériquement
Données
Fonction de hachage
101100110101
Empreinte
111101101110
Signature
Déchiffrement avec la clef publique du signataire
?
101100110101
Empreinte
Si les empreintes sont identiques, la signature est valide