SSL - authentification forte - signature électronique - protection BOYD et Cloud : le livre blanc

Contenu

1. Introduction

Les usages découlant des technologies de la cryptographie asymétrique sont aujourd'hui devenus d'une simplicité enfantine. Les Autorités de Certifications jouent un rôle essentiel sur Internet. La mise en œuvre de ces technologies s'avère immédiate et sans complexité. Ce document présente dans une première partie les fondements de la technologie puis dans une deuxième partie les applications, les usages et les gains obtenus.

2. Références

1. L'avènement de la signature électronique : 2014

2. La cryptographie et la PKI enfin expliquées simplement
3. Bien choisir ses certificats SSL
4. L'authentification forte ou vers la fin du mot de passe
5. Pourquoi migrer ses certificats Symantec vers une autre Autorité de Certification
6. L'avènement de la signature électronique : 2014
7. Les solutions de PKI en SaaS permettent l'avènement des usages des certificats électroniques
8. La NSA et les Autorités de Certification : Mythe ou réalité ?
9. La vérité sur Heartbleed

3. Règles de confiance établies depuis la nuit des temps …

A travers l'Histoire, nous avons établi des relations de confiance, signé des contrats, fait appel à des tiers de confiance tels que des notaires, à des témoins, délivré des documents officiels, mis en place des processus de délivrance, instauré la poignée de main et la rencontre face à face, utilisé des documents confidentiels cachetés, etc. Toutes ces règles de confiance sont bouleversées par le monde numérique. De nouvelles règles se sont établies. Des risques majeurs demeurent. Des opportunités également majeures apparaissent.

Lire La cryptographie et la PKI enfin expliquées simplement

4. L'encodage des messages : depuis l'antiquité …

Depuis l'Antiquité, les hommes ont encodé des messages envoyés, afin que ceux-ci ne puissent être interceptés. La littérature et le cinéma sont remplis d'histoires militaires, d'espionnages, ou amoureuses sur des messages codés (Note : dans le jargon actuel, l'on dit chiffrés, et l'on parle de chiffrement). Le code le plus connu demeure le code César. Le principe dit cryptographique (du grec : crypto, caché et graphos, dessin) consiste à appliquer une combinaison à un texte, afin que personne ne puisse le lire, puis à la personne qui le reçoit à appliquer la combinaison inverse afin de le décoder. Les Castor Junior possédaient de nombreuses techniques de chiffrement avec des jeux associés. César, lui, utilisait cette technique pour communiquer avec les différentes entités de son armée sur les champs de bataille.

Lire La cryptographie et la PKI enfin expliquées simplement

5. Les limites de la cryptographie symétrique

La cryptographie symétrique pour laquelle la clé de chiffrement est la même (ou l'inverse) de la clé de déchiffrement comportait des problèmes majeurs. Il fallait échanger la combinaison de chiffrement (la clé dite de chiffrement) avec la personne qui devait déchiffrer. Il fallait une clé de chiffrement différente pour communiquer avec chaque interlocuteur de façon confidentielle. Ces clés risquaient être divulguées. Il fallait maintenir une liste parfois importante de clés. Il est apparu très vite que cette technique ne convenait pas au monde numérique.

Lire La cryptographie et la PKI enfin expliquées simplement

6. La cryptographie asymétrique ouvre de nouveaux horizons

En 1975, Witfiled Diffie et Martin Hellman mirent au point un algorithme mathématique pour lequel l'algorithme pour chiffrer un document et celui pour le déchiffrer pouvaient être différents. Il existait ainsi une clé permettant de chiffrer, et une autre différente permettant de déchiffrer le document. En quelque sorte, une clé permettait de fermer le coffre-fort et une autre, de l'ouvrir. Cette technique fût nommée la cryptographie asymétrique par opposition à la cryptographie symétrique où la clé pour chiffré et celle pour déchiffrer étaient les mêmes. Cette découverte eut un impact considérable.

La cryptographie asymétrique ouvre de nouveaux horizons. Désormais, chaque personne possède sa clé dite privée que personne d'autre ne connaît plus et sa clé publique que tout le monde connait et qui est identifiée par tous comme lui appartenant. Il est possible d'échanger librement la clé publique. Si l'on chiffre un message avec la clé publique, seule la personne possédant la clé privée correspondante peut déchiffrer le message. Il n'est alors plus nécessaire pour chaque personne de garder confidentiellement un ensemble de clés symétriques pour chaque interlocuteur avec lequel on souhaite communiquer de façon chiffrée.

Lire La cryptographie et la PKI enfin expliquées simplement

7. La signature électronique

Mais cette technologie de cryptographie asymétrique permet aussi une nouvelle application ! Si une personne envoie à son interlocuteur un document chiffré avec sa clé privée et que la clé publique correspondante réussit à déchiffrer, alors c'est que le message provient bien de la personne ayant chiffré le document. En effet, seule la clé publique correspondant à la clé privée permet de décoder le document. La signature électronique est née avec ses très nombreuses applications.

LOI n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

« Art. 1316. - La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.
« Art. 1316-1. - **L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier**, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.
« Art. 1316-2. - Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. »

Exemple de mise en œuvre de la signature électronique

Vous pouvez commander auprès d'une organisation Tiers de Confiance (telle que DigiCert) une clé USB cryptographique de signature électronique. Le Tiers de Confiance est une organisation habilitée par le gouvernement ou les éditeurs d'outils numériques (Adobe, Microsoft, etc.) à délivrer des certificats électroniques après un audit poussé. Dans cet exemple particulier, le certificat de signature électronique est délivré sur clé USB cryptographique. Le Tiers de Confiance a également développé des accords avec les éditeurs de logiciels tels que Microsoft ou Adobe afin que leurs certificats soient reconnus de confiance dans leurs outils. Le Tiers de Confiance vérifiera votre identité en vous demandant une pièce d'identité, vous trouvera dans les pages jaunes et vous appellera par téléphone pour vérifier que c'est bien vous, etc. Il vous remettra alors cette clé USB cryptographique ainsi qu'un code PIN secret, comme pour une carte bleue.

Pour signer vos document et vos emails, vous insérerez votre clé cryptographique dans votre ordinateur, signerez à partir du menu de votre éditeur de document ou d'emails, devrez saisir votre code PIN, et vos documents ou emails seront signés. Cela garantira à vos destinataires que vous êtes bien l'émetteur du document et que ce document n'a pas été modifié. Un horodatage en utilisant via l'Internet un serveur d'horodatage attachera au document l'heure et la date à laquelle a été effectuée cette signature. Le document pourra être modifié, mais il perdra alors la signature. Un document électronique signé peut être dupliqué autant de fois que nécessaire. Plusieurs signatures peuvent être apposées à un document électronique.

Note: Attention à ce qui est communément admis. Un document PDF est contrairement à ce que l'on croit modifiable avec un éditeur de texte adapté. Seul, un document PDF signé électroniquement ne peut pas être modifié sans perdre sa signature.
Note: Le scan d'une signature manuscrite dans un document électronique n'a aucune valeur.

Lire L'avènement de la signature électronique : 2014

8. L'authentification forte – Cloud et BYOD

La cryptographie permet aussi de réaliser de l'authentification forte. Je vous envoie un document, je vous demande de le signer avec votre clé privée. Si c'est bien vous qui l'avez signé, je vous donne par exemple accès au réseau.

L'authentification forte est définie comme une authentification à au moins 2 facteurs parmi les 3 suivants :

- ce que je sais (un code PIN par exemple),
- ce que je possède (une clé cryptographique par exemple),
- ce que je suis (via une détection biométrique par exemple : votre empreinte digitale, votre rétine, etc.).

A noter qu'il faut différencier l'identification (je dis qui je suis) et l'authentification (je le prouve). Cette méthode est aujourd'hui indispensable pour identifier toutes les machines sur le réseau et en particulier pour gérer les problématiques de Cloud ou BYOD.

Lire : L'authentification forte ou vers la fin du mot de passe

9. Le chiffrement pour éviter que vos emails circulent en clair

Lorsque vous envoyez des emails à vos interlocuteurs intra-entreprises ou inter-entreprises, ceux-ci circulent en clair sur l'Internet. Vous pouvez utiliser des certificats électroniques pour chiffrer vos emails. Vous vous assurez ainsi que seul votre interlocuteur pourra le lire.

10. La protection indispensable des sites web passe par le SSL

Si vous ne protégez pas votre serveur web de votre Extranet, Intranet ou Internet par un certificat SSL installé sur ce serveur, les informations circulent en clair sur l'Internet ou le réseau. Attention, il convient que de s'assurer que votre certificat est correctement installé, provient d'un Autorité de Certification de confiance, et n'a pas expiré !

Lire Bien choisir ses certificats SSL

11. La mise en place de solutions de signature, d'authentification forte et de chiffrement

Le Cloud et le BOYD sont autant de nouveaux challenges pour les organisations. Heureusement, ces organisations peuvent aujourd'hui se protéger efficacement via des approches de certificats électroniques proposés en mode SaaS. Une approche orientée usage, des certificats reconnus par les autorités de certification publiques, une sécurité accrue, une simplicité de mise en œuvre et une plus grande souplesse, des modes de financement adaptés permettent aujourd'hui une adoption bien plus grande des usages des certificats électroniques.

Lire Les solutions de PKI en SaaS permettent l'avènement des usages des certificats électroniques

1. Conclusion : De nombreux usages !

Toutes ces technologies ouvrent de nouveaux horizons. Tandis qu'un document scanné n'a pas de valeur légale, un document signé électroniquement revêt une valeur probante. Ainsi, les organisations commencent à faire signer à des internautes qu'ils ne connaissaient pas des contrats à la volée, directement sur des sites web. Les contrats peuvent également être signés sur des tablettes dans les agences des banques, chez les commerçants, etc. Désormais, l'envoi de lettres recommandées électroniques, de façon totalement numérique, est parfaitement légal.

Ceci n'est qu'un tout premier tour d'horizon d'usages ouverts par les nombreuses applications de la cryptographie asymétrique. Contactez-nous pour découvrir tous ceux qui peuvent correspondre à votre organisation. http://www.aliceandbob.fr/support-outils/workshop-d%C3%A9mat%C3%A9rialisation/ .

La sécurisation des identités et des échanges numériques est un des enjeux majeurs d'aujourd'hui. Nous ne sommes qu'à l'aube des utilisations possibles de solutions fondées ou permises par ces technologies. Nul doute que l'innovation associée à toutes ces technologies nous étonnera dans les toutes prochaines années. Notre mission et notre ambition sont de vous accompagner avec la dimension de sécurisation dans ce fantastique voyage au cœur de la transformation numérique!