



CASES articles

Maniement aisé pour les personnes privées et les entreprises

Signature, carte d'identité et Chiffrement sur l'Internet

Pour plus de sécurité, adoptez les réflexes CASES !

L'infrastructure à clé publique (« public key infrastructure ») rend la vie dure aux escrocs

Que ce soit pour accélérer des processus de traitement, développer des connaissances ou échanger des informations, le monde numérique fait désormais partie intégrante de notre quotidien. Les avantages sont indéniables, mais les falsifications, l'espionnage et les escroqueries font malheureusement également partie du quotidien sur l'Internet car ces activités illégales sont, hélas, rentables. La signature numérique, le chiffrement des données ainsi que l'identification sans équivoque de l'utilisateur sur l'Internet, comparable à une véritable carte d'identité, ont été développés en réponse à cette évolution. Une solution conviviale, reposant sur une infrastructure à clé publique (ICP), ou « public key infrastructure (PKI) », est offerte aux utilisateurs privés et aux entreprises.

Comment décrivait-on des personnes, il y a quelques siècles, afin que d'autres puissent les reconnaître ? Comment pouvait-on alors être sûr de l'authenticité d'un document ? L'espionnage, l'usurpation d'identité et les falsifications existaient déjà bien avant l'apparition de la photographie, de la carte d'identité, des empreintes digitales, des analyses ADN et de l'Internet.

Les descriptions de personnes, les documents d'identité, les sceaux et les portraits ont été développés entre le 13^e et le 17^e siècle pour évoluer vers des systèmes de rédaction et de certification. Cela devait compliquer considérablement la vie aux

imposteurs et autres escrocs. Au fil du temps, il est ainsi devenu possible d'établir noir sur blanc l'identité d'une personne, l'authenticité et la validité de documents.

Au même titre, il est de nos jours possible de certifier l'identité d'une personne, l'authenticité, l'exhaustivité et la provenance de données ou encore l'identité d'applications et d'ordinateurs sur l'Internet. À cet effet, l'on a recours à un organisme de certification, permettant à un utilisateur de disposer d'une signature numérique reconnue légalement. Cet organisme propose aussi des solutions permettant de garantir la confidentialité des informations ; ce sont alors des mécanismes de chiffrement efficaces qui sont employés. Afin de rendre tout ceci possible, l'organisme de certification fonctionne sur la base d'une infrastructure à clé publique.

Pourquoi une ICP est-elle nécessaire ?

L'ICP permet d'améliorer la sécurité des communications numériques. Les utilisateurs et les applications sont identifiés sans équivoque. L'authenticité de l'identité d'une personne, d'une application, d'un document ou d'autres données peut ainsi être confirmée, ce qui complique significativement une éventuelle usurpation d'identité par un escroc.

De même, la modification de documents ou de données numériques par des cybercriminels peut être détectée immédiatement.

Une ICP permet également de garantir la « confidentialité » dans le monde numérique. Les données, telles que le contenu d'un e-mail par exemple, peuvent être chiffrées de façon à assurer un niveau de sécurité très élevé et à garantir que seul le

destinataire légitime de l'e-mail soit en mesure de les déchiffrer.

Une ICP est donc un outil important lorsqu'il s'agit de garantir authenticité, intégrité et confidentialité dans le monde numérique.

Quelles sont les possibilités d'une ICP ?

Pour le chiffrement et la signature de données, l'ICP emploie un système dans lequel chaque utilisateur dispose d'une paire de clés numériques : une « clé publique » et une « clé privée ».

Lorsqu'un utilisateur souhaite envoyer des données, par exemple un e-mail, tout en s'assurant que son contenu ne soit pas accessible à des tiers, il doit chiffrer l'e-mail en question. Pour cela, il utilisera la « clé publique » du destinataire légitime. Seul ce dernier (car il possède la « clé privée » correspondante) sera ensuite en mesure de déchiffrer le message.

L'expéditeur chiffre donc son message à l'aide de la clé publique du destinataire et celui-ci peut le déchiffrer à l'aide de sa clé privée. La clé privée n'étant pas accessible à des tiers, ce procédé permet de garantir que le message ne pourra être déchiffré que par le seul destinataire légitime.

La clé privée est habituellement stockée dans une puce électronique spécifique. Cette puce est conçue de façon à exclure toute lecture illicite de la clé secrète et peut par exemple se trouver sur une carte à puce. Afin de pouvoir utiliser la clé privée, il est nécessaire d'activer la puce en introduisant un mot de passe. La personne désirant utiliser la clé privée doit donc disposer de la puce électronique et du mot de passe d'activation.

Lorsqu'un utilisateur souhaite transmettre un message chiffré à une personne, il doit donc disposer de la clé publique de ce destinataire légitime. Mais comment l'utilisateur peut-il obtenir la clé publique d'une autre personne ? C'est très simple : l'utilisateur obtient la clé publique de l'organisme de certification. Il peut ainsi être certain qu'il s'agit bien là de la clé publique du destinataire légitime, et non d'une contrefaçon provenant d'un escroc.

Mais la clé privée n'a pas pour unique vocation de déchiffrer des données : elle est principalement utilisée pour signer des données, comme des lettres ou des factures. Grâce à la clé publique de la même paire de clés, les autres utilisateurs peuvent alors vérifier l'authenticité de cette signature.

Comment fonctionne une ICP ?

Comment un utilisateur peut-il obtenir une paire de clés, correspondant aux deux clés numériques décrites ci-dessus ? Il lui suffit de s'identifier auprès d'un

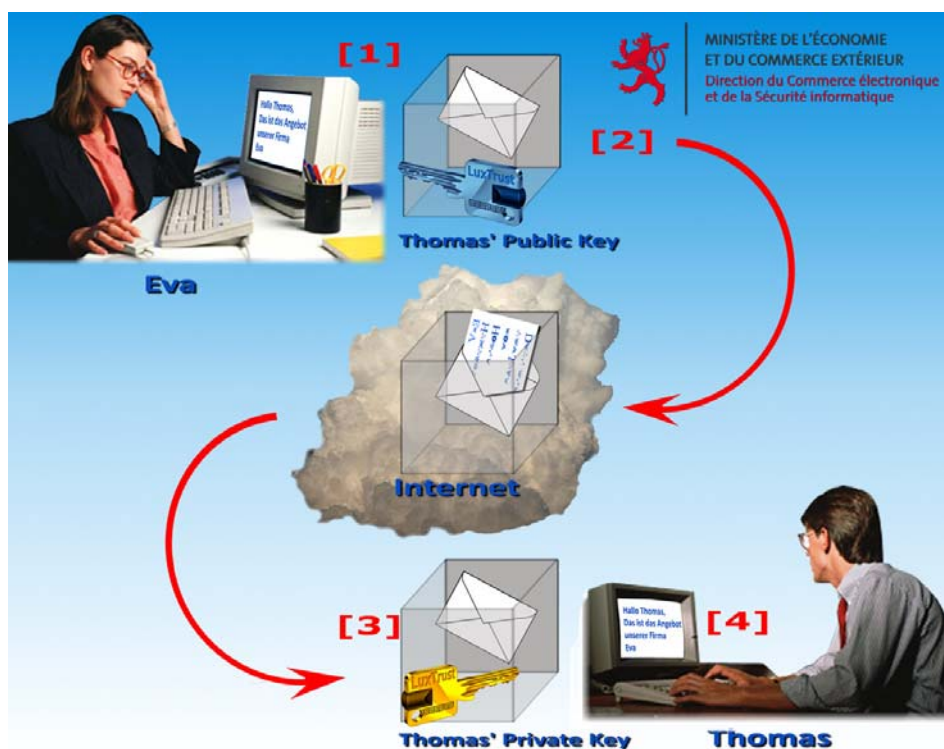
« organisme de certification » à l'aide de sa carte d'identité. Cet organisme procède ensuite à la vérification des données, approuve la demande de certification et génère la paire de clés correspondante sur la puce. La clé publique est de plus authentifiée par un certificat confirmant sans équivoque qu'elle a été attribuée à une personne spécifique. L'utilisateur obtient ainsi une clé numérique publique ainsi que la clé privée correspondante. La clé publique demeure à la disposition des autres utilisateurs auprès de l'organisme de certification.

L'utilisateur obtient donc une signature électronique, une identification sans équivoque sur l'Internet, ainsi que la possibilité de chiffrer et de déchiffrer des documents et d'autres données.

Exemples concrets : Signature et vérification de la signature

Une utilisatrice, que nous nommerons Eva, peut signer des documents et des données à l'aide de sa clé privée. Un deuxième utilisateur, nommons le Thomas, peut vérifier l'authenticité de la signature d'Eva grâce à la clé publique de celle-ci.

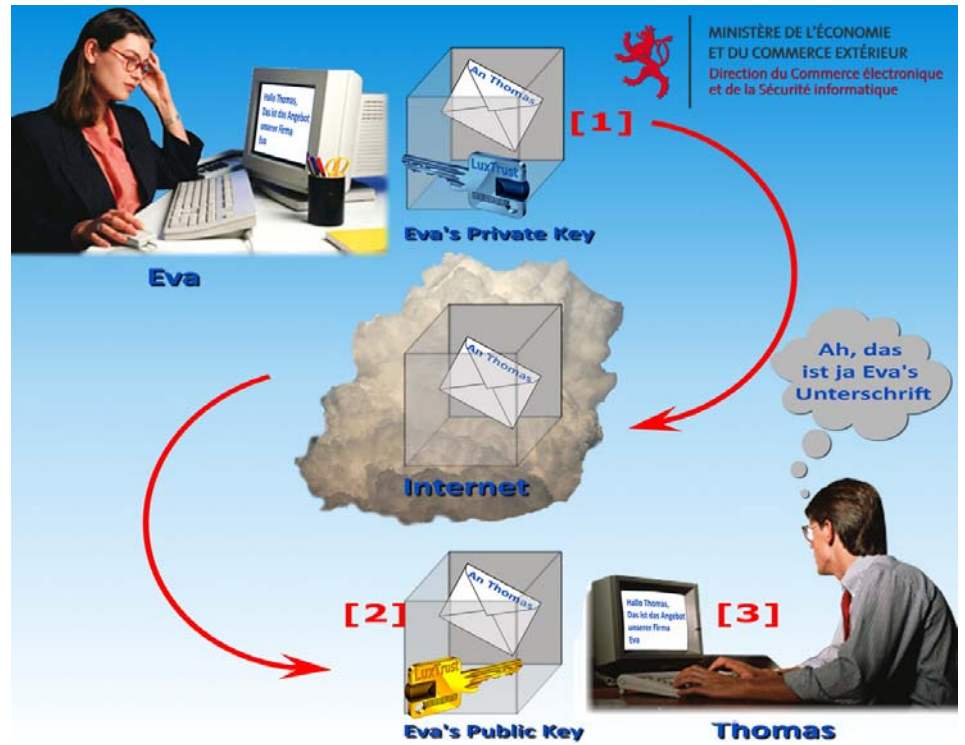
Une imposture n'est guère possible, car la clé en question a été attribuée à Eva par l'organisme de certification.



Graphique 1 : Eva signe un document à l'aide de sa clé privée [1], puis l'envoi à Thomas. Thomas utilise la clé publique d'Eva [2] pour authentifier la signature de celle-ci [3].

Envoi de documents chiffrés

Eva souhaite transmettre un document chiffré à Thomas. C'est très simple : Eva utilise la clé publique de Thomas mise à sa disposition par l'organisme de certification pour chiffrer le document puis l'envoie à Thomas. Une tierce personne ne peut accéder au contenu de ce message, car elle ne possède pas la clé privée de Thomas, nécessaire pour le déchiffrer. La clé privée de Thomas n'est possédée que de lui seul. Thomas reçoit le message chiffré d'Eva et peut le déchiffrer grâce à sa clé privée.



Graphique 2 : Eva envoie un e-mail à Thomas. L'Internet n'étant pas sûr, elle souhaite chiffrer cet e-mail. À cet effet, elle utilise la clé publique de Thomas [1] et chiffre l'e-mail [2]. Seul Thomas, à l'aide de sa clé privée [3], est ensuite en mesure de déchiffrer l'e-mail [4].

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu