Missions professionnelles

Mission 2

Déployer les moyens appropriés de preuves électroniques

Des courriels frauduleux sont adressés aux clients, qui prennent l'apparence de messages émis par M@Banque. Ils les invitent à compléter un contrat dématérialisé d'ouverture de compte avec leurs informations personnelles. Si les clients remplissent le document, les pirates peuvent récupérer leurs informations d'identification pour accéder à leurs comptes. M^me^ Schmitt sollicite votre expertise pour trouver une solution technique à cet acte de malveillance et rétablir l'e-réputation de M@Banque.

Travail à faire

1. Identifiez les éléments permettant de détecter que le courriel contenant un contrat dématérialisé est frauduleux.
   > Documents 1 et 2
   > Fiche savoirs CEJMA 4
2. Déterminez le délit et les peines encourues par les pirates pour cet acte de malveillance.
   > Fiche savoirs CEJMA 3

   Un client a adressé un courriel à M@Banque pour confirmer la signature d'un contrat de demande de carte de crédit en utilisant une solution de chiffrement (document 4). Votre responsable s'interroge sur la valeur de ce document en cas de litige.
3. Démontrez que la solution proposée pour les échanges de contrats dématérialisés répond bien aux exigences de la législation.
   > Documents 3 et 4
   > Fiche savoirs CEJMA 4

   M@Banque souhaite proposer à ses clients la mise à disposition d'un coffre-fort numérique pour protéger leurs documents numériques.
4. Présentez les avantages d'une telle solution pour les clients et pour le rétablissement de l'e-réputation de M@Banque.
   > Document 5
   > Fiche savoirs CEJMA 4

CHAPITRE 3

Missions professionnelles

Dossier documentaire

Document 1 Le courriel reçu par les clients de M@Banque

M@Banque

Cher(e)s clients et clientes de M@Banque

Vous trouverez en pièce-jointe le contrat d'ouverture de compte bancaire à compléter et à nous renvoyer pour confirmer votre engagement pris via notre site.
Vous devrez nous confirmer notamment votre identifiant et votre mot de passe d'accès à vos comptes.

Nous sommes heureux de vous compter parmi nos nouveaux clients.

Le service juridique
servicejuridique@mabanques.com

Document 2 Le rappel des conseils de la CNIL figurant sur le site M@Banque

1. Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.

2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.

- **Attention aux expéditeurs inconnus :** soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.
- **Soyez attentif au niveau de langage du courriel :** même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration…).
- **Vérifiez les liens dans le courriel :** avant de cliquer sur les éventuels liens, laissez votre souris dessus. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime.
- **Méfiez-vous des demandes étranges :** posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.
- **L'adresse de messagerie source n'est pas un critère fiable :** une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique.

Extrait de « Phishing : détecter un message malveillant », www.cnil.fr.

› Voir lexique BTS SIO, p. 221

Document 3 Les indications de la direction de M@Banque concernant la gestion des contrats dématérialisés

La direction de la banque a envoyé une note aux employés chargés de la gestion des contrats dématérialisés afin de leur rappeler les règles essentielles à respecter.

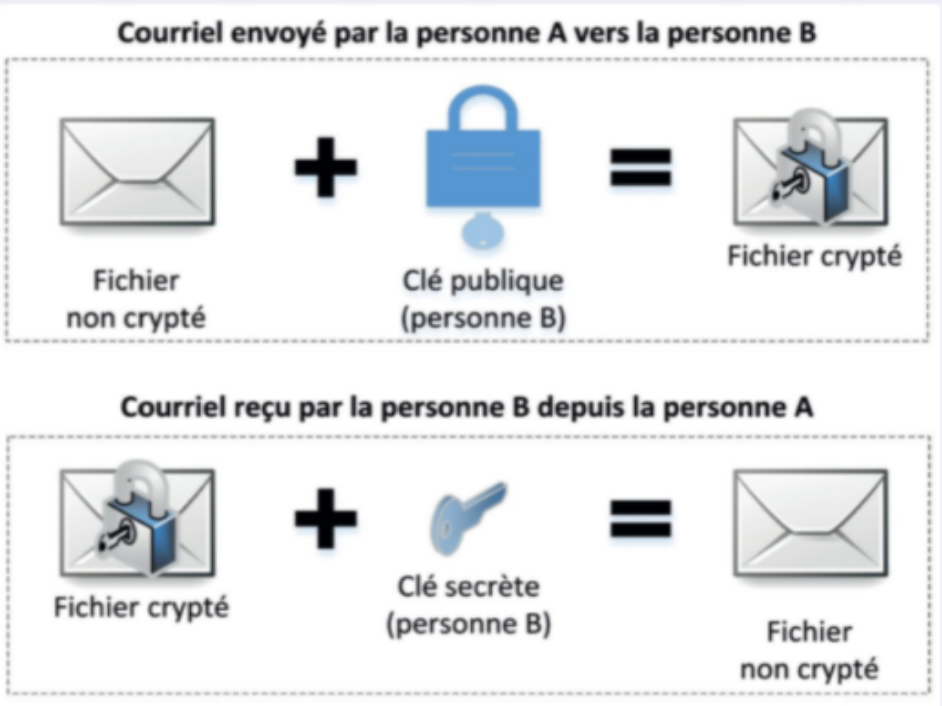
M@Banque

Il est rappelé à tous les collaborateurs qu'il est possible pour les particuliers de souscrire un contrat dématérialisé si les deux règles suivantes sont respectées :
– l'authentification claire des signataires du contrat ;
– l'intégrité du document.
Si ces conditions sont respectées, alors le contrat numérique équivaut à un contrat papier aux yeux de la loi : ils ont donc la même valeur légale.
Vous pouvez ainsi recommander aux clients qui le souhaitent d'utiliser un logiciel de signature électronique (par exemple, GnuPG) et un coffre-fort électronique pour la création, la signature et l'archivage de documents contractuels.

Cordialement,
La Direction M@Banque

Document 4 Une veille pour une solution de cryptage de courriels

Le principe de PGP (*Pretty Good Privacy*) repose sur une cryptographie à clé publique. C'est-à-dire qu'une paire de clés publiques et une paire de clés secrètes sont générées. La clé secrète (*key*) est protégée par un mot de passe et sert à déchiffrer. Elle reste sur l'ordinateur de son propriétaire, tandis que la clé publique sert à chiffrer ses emails et est distribuée au plus grand nombre. Ainsi, la clé publique est mise à disposition des contacts email potentiels, en leur étant distribuée directement ou encore en la téléchargeant via un serveur de clés externe. À l'aide de la clé publique, il est possible de crypter tous les emails que l'on échange avec vous. La clé privée est uniquement en votre possession, et protégée de surcroît par un mot de passe. Pour que vous puissiez communiquer en toute sécurité, il est nécessaire que votre contact utilise également PGP et partage la clé publique avec vous. Le procédé de la clé publique est également désigné comme étant un processus asymétrique, car les deux parties utilisent des clés différentes. À l'aide de signatures, vous pourrez d'autant plus garantir l'authenticité de vos communications.



D'après « Comment assurer le chiffrement de vos emails avec PGP », www.ionos.fr, 9 octobre 2019.

> Voir lexique BTS SIO, p. 221

Missions professionnelles

Document 5 La solution du coffre-fort numérique de M@Banque

Le coffre-fort numérique proposé par M@Banque est une solution de stockage d'informations certifiée sans intrusion possible. Son objectif est de conserver les données intactes et de permettre leur restitution à l'identique à un utilisateur accrédité. Le coffre-fort numérique doit donc garantir, avant tout, l'intégrité des informations dans le temps.

Ce service est désormais proposé aux particuliers, sous la forme d'un espace de stockage sécurisé, qui nécessite une identification. Ses fonctionnalités permettent la récupération automatique des différents types de documents confiés par le client (relevés bancaires, fiches de paie, factures, diplômes, papiers d'identité, documents administratifs ou fiscaux, etc.). Une fois configuré, cet outil aspire donc automatiquement les nouveaux documents produits par M@Banque (par exemple, un relevé de compte bancaire).

M@Banque garantit, à l'utilisateur, un « accès exclusif » du service par la mise en œuvre des mesures suivantes :

- une identification par un identifiant et un mot de passe personnels ;
- un chiffrement par le service de coffre-fort numérique de l'ensemble des documents et données lors de leurs stockages, transferts vers ou depuis le service.

Fiche savoirs CEJM appliquée 4

Le droit de la preuve électronique

Le recours à la preuve électronique est indispensable pour faire valoir ses droits dans une relation commerciale, la défense d'une propriété intellectuelle ou encore la défense de sa e-réputation.

I Définition

Extrait de l'article 1316 du Code civil :
« 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. »

Cette définition large de la preuve permet d'adapter le droit à l'utilisation des nouvelles technologies de l'information.

II La force probante et les conditions de recevabilité de la preuve électronique

Extrait de l'article 1316 du Code civil :
« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit 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 garantir l'intégrité. »

1. La force probante de la preuve électronique

Depuis la loi n° 2000-230 du 13 mars 2000, l'écrit électronique est accepté comme preuve légale au même titre que l'écrit papier, ce qui lui confère sa force probante.

La force probante est la valeur juridique donnée à un mode de preuve même si le juge reste libre de forger son intime conviction, avec l'obligation de motiver sa décision.

2. Les conditions de recevabilité de la preuve électronique

Deux conditions doivent être respectées pour qu'une preuve électronique soit recevable :
- l'authentification de la personne à l'origine de la preuve doit être rendue possible ;
- l'intégrité de la preuve doit être garantie.

III Les moyens de la preuve électronique

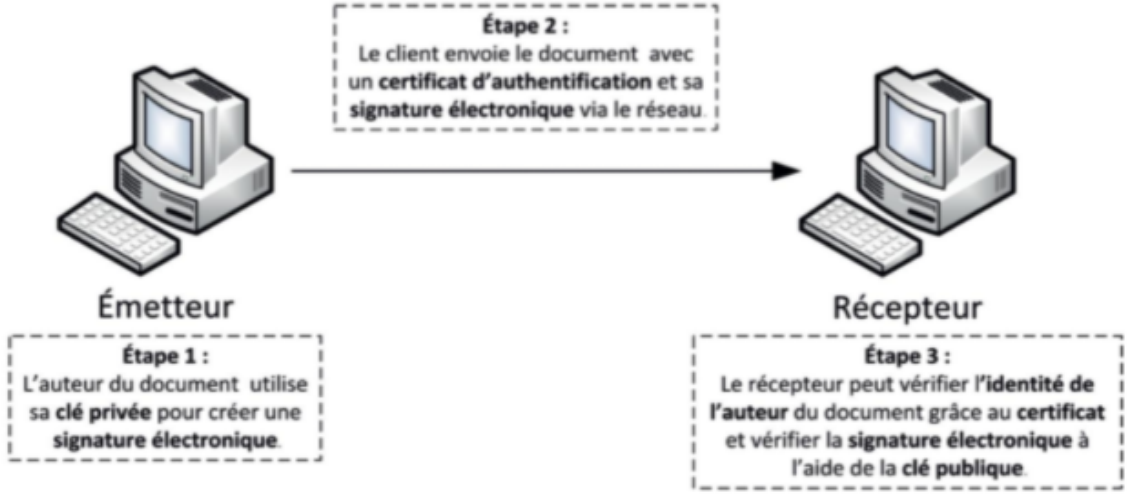
1. Les moyens/supports de l'authentification

L'article 1316-4 du Code civil stipule que la « signature identifie celui qui l'appose et manifeste le consentement des parties aux obligations qui découlent de 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 signature électronique est recevable à condition que le signataire soit identifié et que l'écrit soit indissociable de celle-ci. Elle permet de garantir la non-répudiation par le signataire du document signé, c'est-à-dire le fait que le signataire ne peut contester être l'auteur de l'écrit.

Une signature électronique est réalisée à partir de la cryptographie asymétrique (voir Fiche savoirs technologiques 9, p. 151). Elle repose sur un couple de clés, l'une privée, connue par son seul propriétaire, l'autre publique, connue de tous. La clé publique a pour fonction de crypter le message, et la clé privée de le décrypter.
La problématique est de pouvoir vérifier l'identité de l'auteur de la signature. L'utilisation d'un certificat électronique, délivré par une autorité de certification de confiance, permet de répondre à ce besoin.
Un certificat doit contenir :
- les informations d'identification (par exemple, le nom, la localisation) ;
- une clé publique ;
- une signature construite à partir de la clé publique.

Échange d'un document avec signature électronique et certificat d'authentification



2. La garantie de l'intégrité de la preuve électronique

L'intégrité attendue d'une preuve électronique est assurée par l'utilisation d'un algorithme de chiffrement qui permet de vérifier, à l'arrivée du message signé électroniquement, que celui-ci n'a pas été modifié.
Le procédé technique de calcul d'empreintes électroniques (par exemple, MD5 ou SHA) de l'information source et de l'information copiée est un moyen incontestable de respecter ce critère : il permet de démontrer que ces informations n'ont pas pu être altérées au moment de cette opération et que le contenu est resté strictement identique.

3. Les documents électroniques recevables comme preuves électroniques

Les documents signés certifiés par un organisme d'État	Les documents non signés	Les courriels, les SMS et les MMS
Ces documents signés garantissent l'identification de l'auteur (signature électronique) et l'intégrité du document par l'utilisation d'un certificat électronique délivré par l'État. Ils constituent des documents électroniques authentiques.	L'auteur du document est identifiable mais sans signature apparente. Cependant, l'intégrité est assurée par un procédé fiable. **Exemple :** l'échange de données informatisées. C'est un début de preuve si la loi exige un écrit « parfait ».	Les documents électroniques tels que les courriels, les SMS et les MMS ne permettent pas l'identification de l'auteur et ne garantissent pas l'intégrité du message. Ils ne peuvent pas être assimilés à des écrits, et encore moins à des écrits « parfaits ».