

Les 10 recommandations de CertEurope pour établir l'e-Confiance en 2011

Alors que les échanges Internet se développent de manière exponentielle, la sécurité de ces échanges est chaque jour mise à mal. Pour rétablir la confiance et favoriser les échanges entre entreprises, particuliers et organisations, CertEurope liste les 10 recommandations pour établir l'e-Confiance en 2011.

Paris, le 24 janvier 2010 - CertEurope, 1er opérateur de Services de e-Confiance™, a fêté en fin d'année 2010 ses 10 ans, et s'est livré à cette occasion à une réflexion sur les 10 recommandations à faire aux entreprises et aux institutions pour développer l'e-Confiance dans les années à venir, participant ainsi à la dématérialisation des échanges administratifs, commerciaux, citoyens, etc.

1. Protéger son identité numérique

Chaque année en France, plus de 210 000 personnes sont victimes d'une usurpation d'identité (source Credoc). L'usurpation d'identité est une menace pour les individus mais également pour les entreprises, dont la maîtrise de l'image et de la réputation est essentielle à leur survie, alors que les usages croissants des réseaux sociaux ont démultiplié ce risque.

Les solutions pour se prémunir existent: l'authentification forte constitue l'une des parades. Le secteur bancaire par exemple propose d'ores et déjà ce service aux clients entreprises, et sont aujourd'hui en réflexion, poussées par les recommandations de l'Etat, pour déployer ce même service vers les particuliers.

2. Sécuriser les échanges électroniques

76% des internautes opèrent leurs démarches administratives en ligne (TNS 2008), l'eCommerce est toujours en croissance, soit +26% selon la fédération du e-commerce et de la vente à distance (Fevad) cette année.

Pour favoriser le développement des échanges électroniques, avec tous les avantages que cela apporte, il faut pouvoir assurer la même fiabilité que les échanges traditionnels, en validant de façon certaine l'identité d'une personne ou d'une société et en garantissant l'intégrité des données échangées. Les technologies de signatures et de certificats électroniques répondent à cette problématique de manière fiable depuis maintenant 10 ans (loi du 13 mars 2000).

En outre, dans cette même logique, le gouvernement a récemment lancé le label IDéNum, qui vise à favoriser le déploiement pour le plus grand nombre, de solutions déjà éprouvées : les certificats électroniques, afin d'offrir aux internautes des accès plus sûrs aux différents services Internet.

3. Garantir la valeur probante des échanges

La signature électronique a la même valeur que la signature manuscrite. Un email signé électroniquement a valeur de preuve, ce qui peut s'avérer essentiel dans les échanges inter entreprises mais également entre les citoyens et l'administration par exemple.

La 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. Cette loi a modifié les règles de preuves du Code civil. Dorénavant, l'article 1316-1 du Code civil reconnaît que "l'écrit sur support électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont l'écrit émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité". D'autre part, l'article 1316-4 du Code civil reconnaît que la signature électronique a la même valeur juridique que la signature manuscrite, sous réserve que le procédé de signature

électronique soit fiable. L'article 1316-4 du Code civil prévoit également le principe d'une présomption légale de fiabilité du procédé de signature électronique; les conditions permettant de bénéficier de cette présomption étant détaillées dans le Décret n°2001-272 du 30 mars 2001.

4. Sécuriser l'accès aux applications en mode SAAS

De plus en plus nombreuses à adopter le mode « Service à la demande », les entreprises sont parvenues à optimiser les coûts, à accélérer les déploiements, à réaliser une meilleure répartition budgétaire et à renforcer la mobilité et le nomadisme, via des accès distants, à partir d'un simple navigateur ou de terminaux mobiles.

Mais les aspects de géo-localisation, de sécurité des échanges (authentification des accès ou archivage en regard des législations en vigueur), d'authentification unique (SSO), sont au cœur de l'informatique à la demande et constituent les facteurs clés de la dématérialisation des échanges dans des environnements applicatifs en Cloud.

5. En finir avec les Login et mots de passe

On ne compte plus le nombre de mots de passe et code d'accès qu'un individu doit retenir, tant pour ses usages privés que professionnels. Les entreprises ont ouvert leur périmètre et leur système d'information à de nombreux acteurs externes (partenaires, clients, fournisseurs), qui peuvent accéder aux systèmes via des login et mot de passe. Outre le fait qu'il devient difficile de mémoriser une moyenne de 10 mots de passe, la sécurité basée sur le login / mot de passe n'est plus adaptée aujourd'hui. En effet, nos ordinateurs ne sont pas à l'abri des programmes malveillants de type Keyloggers (enregistreur de frappe) capables de capter ce qu'un utilisateur saisi sur son clavier. Leur usage s'est largement multiplié et il n'est pas nécessaire d'être informaticien pour utiliser ce type de programme. On les trouve en effet prêt à l'emploi sur Internet !

La parade, une nouvelle fois, c'est le certificat électronique. Logiciel ou sur un support cryptographique, le certificat électronique garantit la sécurité des connections.

6. S'appuyer sur le certificat électronique

Le certificat électronique peut être adopté par tous aujourd'hui comme garantie d'une sécurité fiable des différents échanges Internet et email, et ce afin de se prémunir contre les risques d'usurpation, de détournement et de malversation.

Plusieurs niveaux de sécurité peuvent être opérés avec le certificat, en fonction des exigences de sécurité :

- classe 1 : adresse électronique du demandeur requise
- classe 2 : preuve de l'identité requise (photocopie de carte d'identité par exemple)
- classe 3 : présentation physique du demandeur obligatoire
- classe 3+ : identique à la classe 3, mais le certificat est stocké sur un support physique cryptographique (clé USB à puce, ou carte à puce et remis en main propre)

7. Favoriser l'horodatage des échanges

Tout comme il est possible de se fier au cachet de la poste pour dater un courrier, le cachet faisant foi, il est possible d'attester la date d'un document électronique. Les technologies d'horodatage permettent d'émettre un jeton, une sorte de tampon électronique, qui certifie la date du document, et garantit son intégrité. L'horodatage est une garantie supplémentaire de non altérité d'un document.

La réponse aux appels d'offres publics en ligne est l'un des exemples illustrant les bénéfices de l'horodatage : il permettra ici d'attester qu'une entreprise a répondu à une date précise et les documents ainsi horodatés seront inaltérables.

8. Archiver, sécurité et conformité des échanges

Les entreprises dématérialisent de plus en plus, aussi ce sont de nombreux documents qu'il s'agit de conserver, d'archiver, parfois de manière probante. Pour cela, il est recommandé de s'appuyer sur un Tiers Archiveur, également Tiers de Confiance, et disposant des infrastructures sécurisées qui permettent de garantir l'intégrité des données déposées ainsi que leur haute disponibilité et leur restitution dans le temps.

9. Vers plus de simplification avec la dématérialisation des échanges

La dématérialisation favorise la croissance en simplifiant les échanges et en accélérant les processus. C'est un fait acquis pour les entreprises, qui la placent d'ailleurs dans le top 3 de leurs priorités. Elle permet des réductions de coûts notable, l'exemple de la facture électronique parle de lui-même : une facture papier coute jusqu'à dix fois plus cher qu'une facture électronique.

En tant qu'individu, la dématérialisation est également un vecteur de gain de temps, de simplification de processus. En effet, elle est de plus en plus présente dans nos relations avec l'administration (impôts, amende, cantine, etc), avec les banques, et les e-services aux citoyens sont en fort développement.

10. S'appuyer sur un tiers de confiance

Un tiers de confiance est un organisme habilité à mettre en œuvre - notamment - des signatures électroniques reposant sur des architectures d'infrastructure à clés publiques ou PKI (Public Key Infrastructure).

Depuis 10 ans, CertEurope est Tiers de Confiance qualifié et a délivré plus de 500 000 certificats.

| Contacts presse

CertEurope

Nathalie Schlang

Tél. : 01 45 26 72 00

nschlang@certeurope.fr

Agence Just Say It

Isabelle Jahn

Tél. : 01 44 61 81 81

isabelle@just-say-it.com