



Avantages de la Sécurisation des Echanges Electroniques

Avantages de la Sécurisation des Echanges Electroniques

L'essor de la dématérialisation est désormais une réalité. Le plan France Numérique 2012 devrait par ailleurs dynamiser cette tendance de fond. En parallèle, la croissance soutenue des revenus issus du commerce électronique démontre aussi l'essor des échanges électroniques dans notre économie. Fort de ce contexte, les organisations prennent conscience que la mise en place de solutions leur permettant de garantir la sécurité, la confidentialité, l'intégrité et l'authenticité des contenus échangés électroniquement avec leurs clients et partenaires devient désormais incontournable.

Ce document délivre quelques-uns des résultats d'une étude approfondie menée auprès de décideurs afin de mieux déterminer les apports des solutions de sécurisation et certification des transactions électroniques au développement commercial et à la valorisation de la relation client, d'identifier les flux concernés et solutions privilégiées.

Maîtrises d'ouvrage, chefs de projet, responsables informatiques, ..., prestataires, ce Référentiel de Pratiques vous apporte un premier niveau d'information.

Catalyseurs des projets de sécurisation des échanges électroniques

La « Charte de l'authentification sur Internet », signée par 14 acteurs du secteur à pour objectif de lutter contre la cybercriminalité et notamment le vol d'identité dans le cadre d'achats en ligne. Les signataires s'engagent ainsi à informer sur les bonnes pratiques en matière d'authentification et de protection des données personnelles.

Pour 69% des organisations interrogées, le développement de la dématérialisation est le principal facteur déclencheur qui les pousse à conduire des projets de sécurisation de leurs échanges électroniques. Alors que les documents dématérialisés ne représentaient, il y a quelques années encore, qu'un faible volume de l'ensemble des documents échangés avec les clients, ceux-ci prennent désormais une proportion significative qui impose de mettre en oeuvre des actions adaptées pour s'assurer des mêmes garanties que dans le monde physique.

Les organisations prennent conscience que la mise en place de solutions leur permettant de garantir la sécurité, la confidentialité, l'intégrité et l'authenticité de leurs contenus ainsi échangés électroniquement devient inévitable. Elles souhaitent notamment pouvoir mieux tracer les échanges électroniques avec leurs clients, les justifier à titre de preuve, améliorer leur fiabilité et assurer l'intégrité des contenus numériques ainsi échangés.

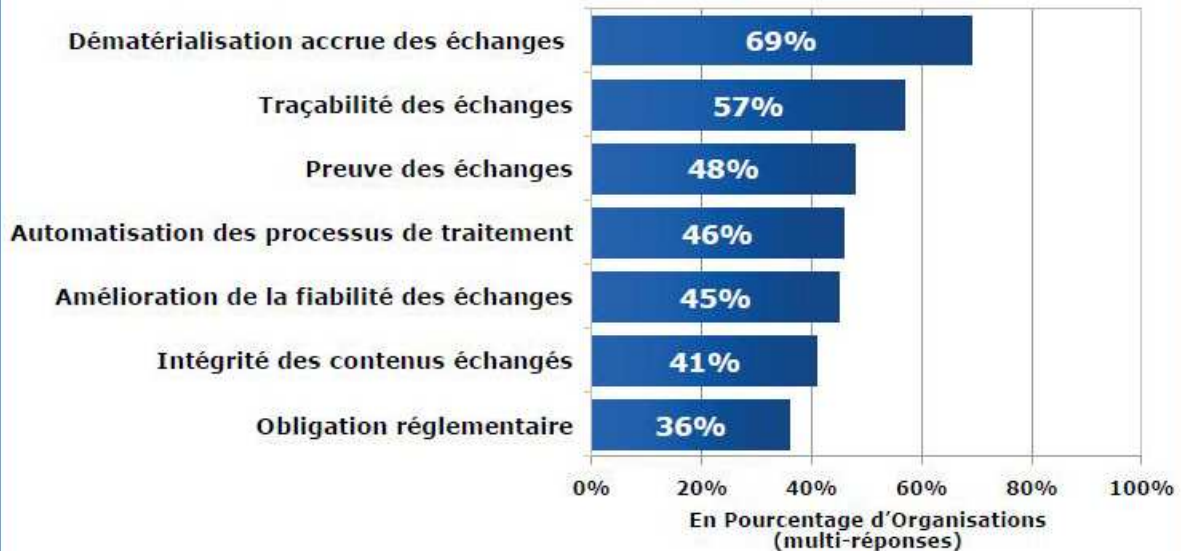
Ces projets sont aussi l'occasion pour elles d'automatiser certains processus de traitement jusqu'ici effectués manuellement, de gagner en efficacité et productivité, et financièrement.

La réglementation constitue aussi un formidable levier dans ce domaine (cf. la dématérialisation des marchés publics par exemple). Au-delà des garanties souhaitées, les organisations constatent que les solutions sécurisant les échanges électroniques sont aussi gage de valeur ajoutée car, en mettant en confiance les clients, elles peuvent contribuer au développement des ventes et à l'optimisation de la relation client.

Parmi les autres catalyseurs évoqués par au moins 30% des entreprises interrogées, il faut noter par ordre décroissant d'importance : la protection des données des clients, la mise en confiance des clients, le développement du e-commerce, l'engagement dans le développement durable, et la garantie de réception, non répudiation, bon routage...

Principaux Catalyseurs des Projets de Sécurisation des Echanges Electroniques avec les Clients – France 2009

(liste suggérée – 18 items)



Echantillon : 160 organisations – Intervalle de confiance +/- 7%

Contenus concernés et modes d'échanges électroniques privilégiés

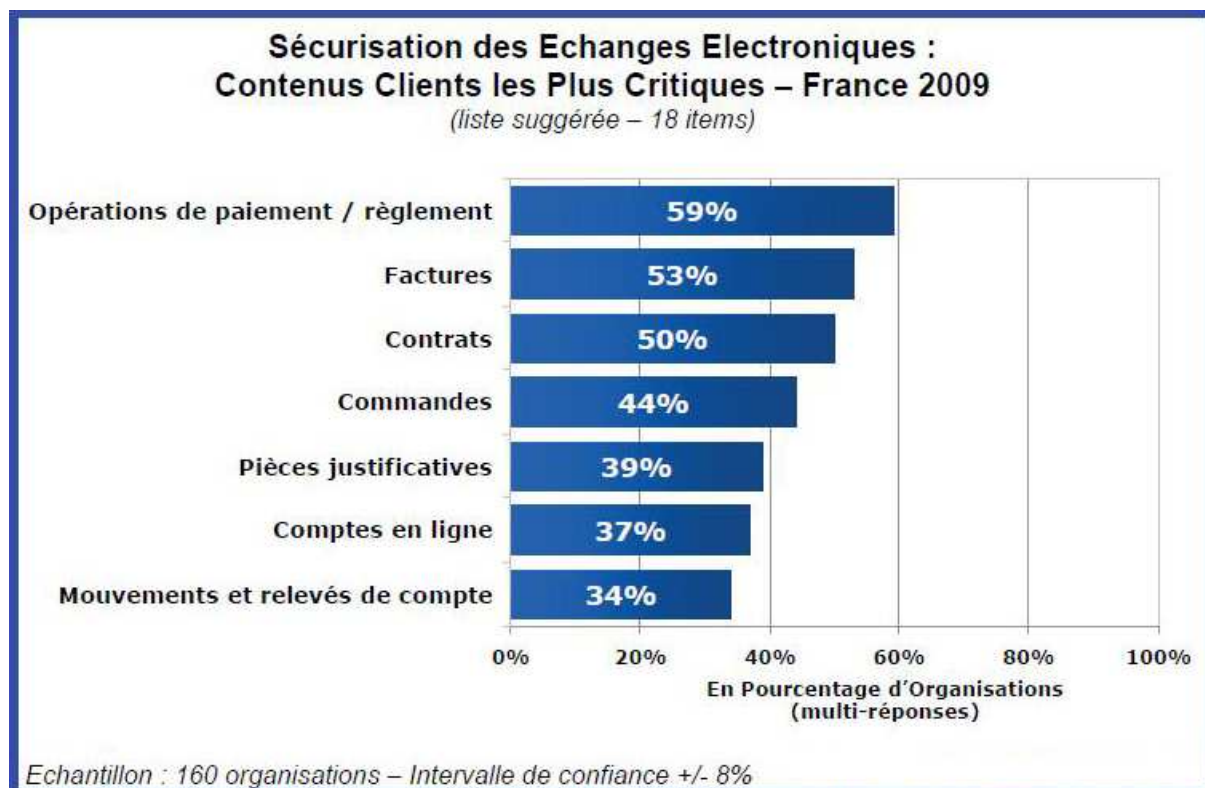
Les contenus associés à la relation contractuelle avec les clients, particuliers (B2C) ou professionnels (B2B), et échangés par voie électronique (via e-mails, sites web, sites de e-commerce, extranets...) vont de la prise de commande à la livraison d'un produit et/ou service en passant par l'émission de devis, la signature de contrat, la facturation, le paiement, le support après-vente et les réclamations, la gestion de comptes en ligne, etc.

En 2009, les documents les plus critiques selon les entreprises interrogées sont ceux qui touchent à l'acte de vente et, plus particulièrement, au règlement financier entre les parties. La majorité d'entre elles considèrent en effet la chaîne « commande-contrat-facture-paiement » comme la plus critique : elle nécessite des actions adéquates pour en assurer la sécurisation dès lors que les contenus associés sont échangés électroniquement.

Ces contenus ont une « propriété originelle » et, pour la plupart, peuvent être utilisés à titre de preuve (valeur probante). Il est important de connaître l'origine de ces documents à partir du moment où ils sont validés et figés dans le temps.

Ces contenus à vocation commerciale sont majoritairement échangés aujourd'hui par messagerie électronique pour 69% des organisations interrogées mais aussi via des extranets (41%), des plates-formes d'échanges collaboratifs (cf. écosystèmes clients-fournisseurs) (35%), des sites de e-commerce (33%), des intermédiaires spécialistes des échanges électroniques (places de marché...) (28%), chez les clients eux-mêmes (relation commerciale en face-à-face, agents de livraison...) grâce à des équipements spécifiques (cf. portables, terminaux de

type smartphones ou autres) (21%) ou même, mais dans une moindre mesure, en agences commerciales ou dans des points de vente grâce à des équipements spécifiques (cf. tablettes graphiques ou autres) (12%).



Solutions de sécurisation des échanges électroniques plébiscitées

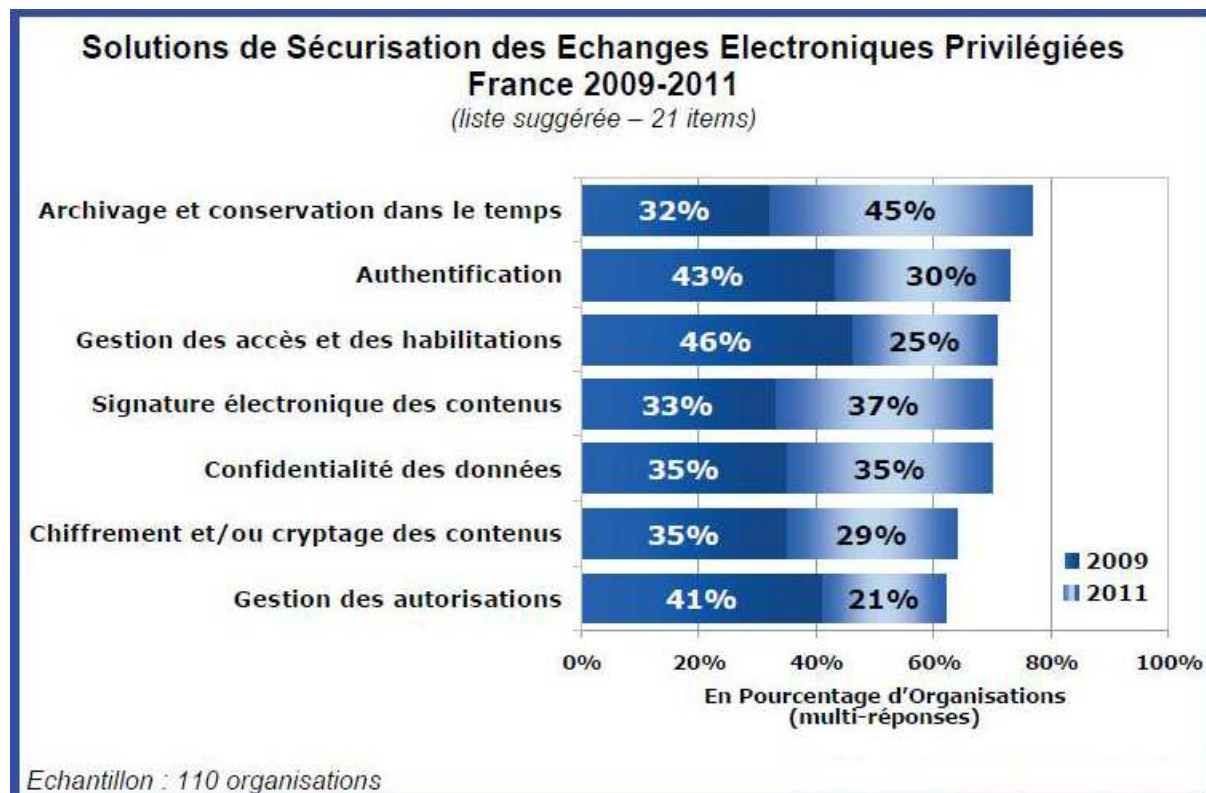
Parmi les autres domaines qui devraient connaître une forte demande d'ici 2011 de la part des entreprises, il faut noter les solutions permettant de gérer la preuve de l'échange, d'historiser chronologiquement les contenus, de garantir l'authenticité et la conformité des contenus.

En 2009, les entreprises interrogées semblent plus tournées vers des solutions permettant de gérer les accès et habilitations, davantage donc du ressort de la sécurité que de la confiance, dénotant une demande encore peu mature dans ce domaine. Il faut en effet bien distinguer les projets du ressort de la sécurité de ceux relevant de la confiance. Les usages associés ne sont pas les mêmes. La notion de « sécurité » résulte le plus souvent d'une approche défensive et technique. La notion de « confiance » relève plus de l'assurance et du contrôle.

D'ici 2011, les solutions de sécurisation les plus demandées par les entreprises interrogées pour leurs contenus associés aux échanges électroniques avec leurs clients portent en revanche sur l'archivage (notamment probatoire), la signature, la confidentialité et la protection (via chiffrement et/ou cryptage), et l'authentification.

En se rapprochant de ce qui est fait au quotidien et en transposant l'existant (papier) au monde numérique (cf. la signature et sa valeur par exemple), il est possible de dérouler les principales contraintes auxquelles font face chaque entreprise dans ses échanges commerciaux avec ses clients et partenaires.

Même si les contraintes du monde physique ne sont pas toutes transposables au monde numérique, la majorité des processus peuvent être repris : protection des contenus, assurance de bon routage, accusé de réception, horodatage, archivage, etc.



Technologies retenues pour la sécurisation des échanges électroniques

Parmi les nouveaux axes de développement envisageables autour de la carte à puce figure la signature électronique avancée (certificat électronique intégré dans la puce).

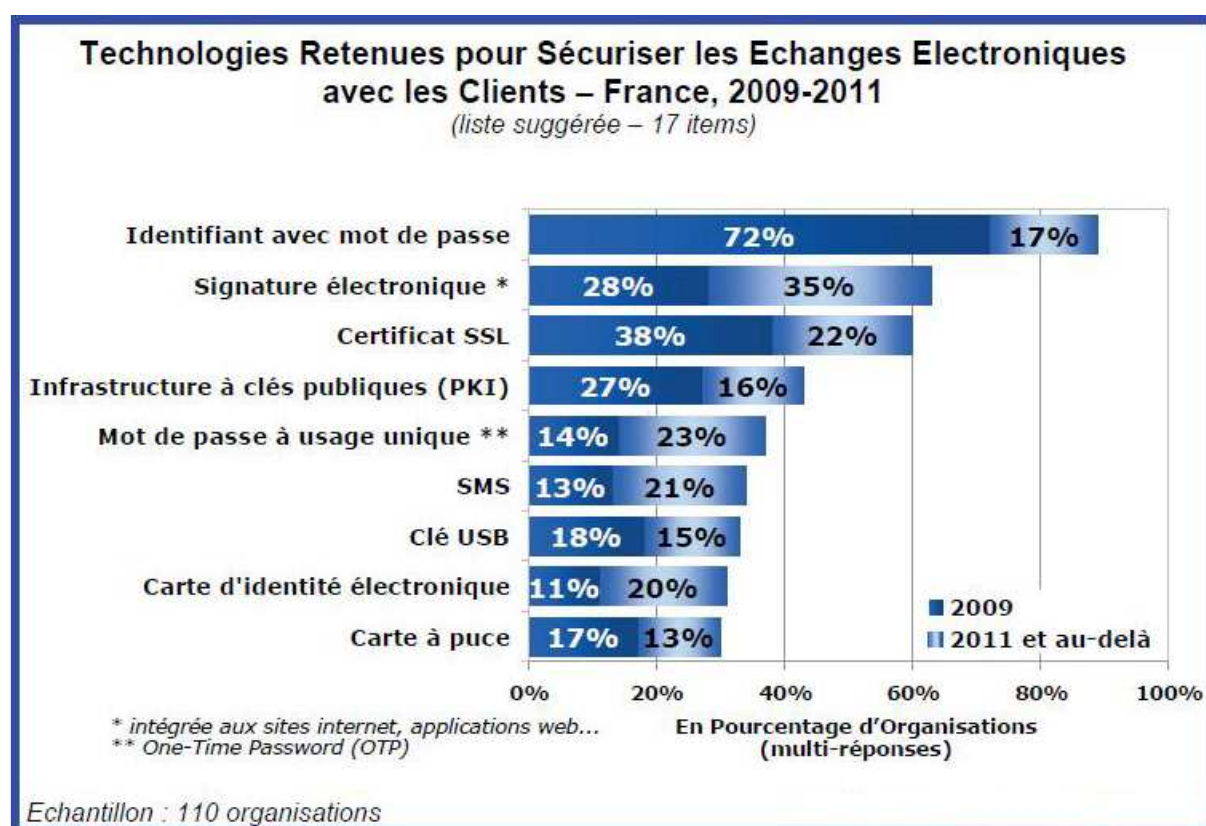
Même si les entreprises montrent un intérêt non négligeable vis-à-vis de la carte d'identité électronique, son usage reste étroitement lié à sa vitesse de déploiement d'ici 2011.

Les solutions de sécurisation retenues par les entreprises reposent sur différentes technologies pouvant être utilisées par ailleurs conjointement pour couvrir tout ou partie des besoins. Celle la plus largement déployée en 2009, par 72% des entreprises interrogées, reste l'identification avec mot de passe. Cependant, cette technologie ne répond que partiellement aujourd'hui à certaines des préoccupations des entreprises telles que vues précédemment et n'offre pas toutes les garanties souhaitées face aux enjeux croissants associés à la dématérialisation des échanges.

D'ici 2011, les entreprises devraient aussi recourir à d'autres technologies plus adaptées à leur contexte et reposant notamment sur : La signature électronique

qui consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

Celle-ci peut par ailleurs être directement intégrée aux sites Internet et autres applications web. Les entreprises semblent s'y intéresser pour signer directement en ligne des contrats (dans l'assurance, la banque, les services d'utilité publique, chez les opérateurs de services...) ; L'authentification utilisant des mots de passe à usage unique ou OTP (One Time Password). C'est le cas de certaines nouvelles cartes bancaires qui intègrent un petit écran produisant un code aléatoire unique à chaque utilisation ; Les certificats SSL pour sécuriser les échanges commerciaux et confidentiels réalisés sur des sites web, des intranets ou extranets ; Le SMS pour transmettre par exemple un code temporaire à saisir dans une fenêtre d'authentification afin de valider un achat ou une transaction sur Internet, et ainsi lutter contre l'utilisation frauduleuse de cartes bancaires.



Niveau de recours à des services de certification et à la signature électronique

Le certificat de signature électronique est le plus souvent délivré par une autorité de confiance. Il garantit de manière forte l'identité du signataire et l'intégrité d'un contenu, document ou message et confère une valeur juridique à l'échange. Il apporte la même valeur juridique aux contenus numériques que la signature manuscrite.

En 2009, 47% des 110 organisations interrogées mentionnent recourir déjà à des services de certification électronique afin d'authentifier, valider, dater, archiver, protéger, signer..., un contenu électronique et/ou le flux d'échange associé dans

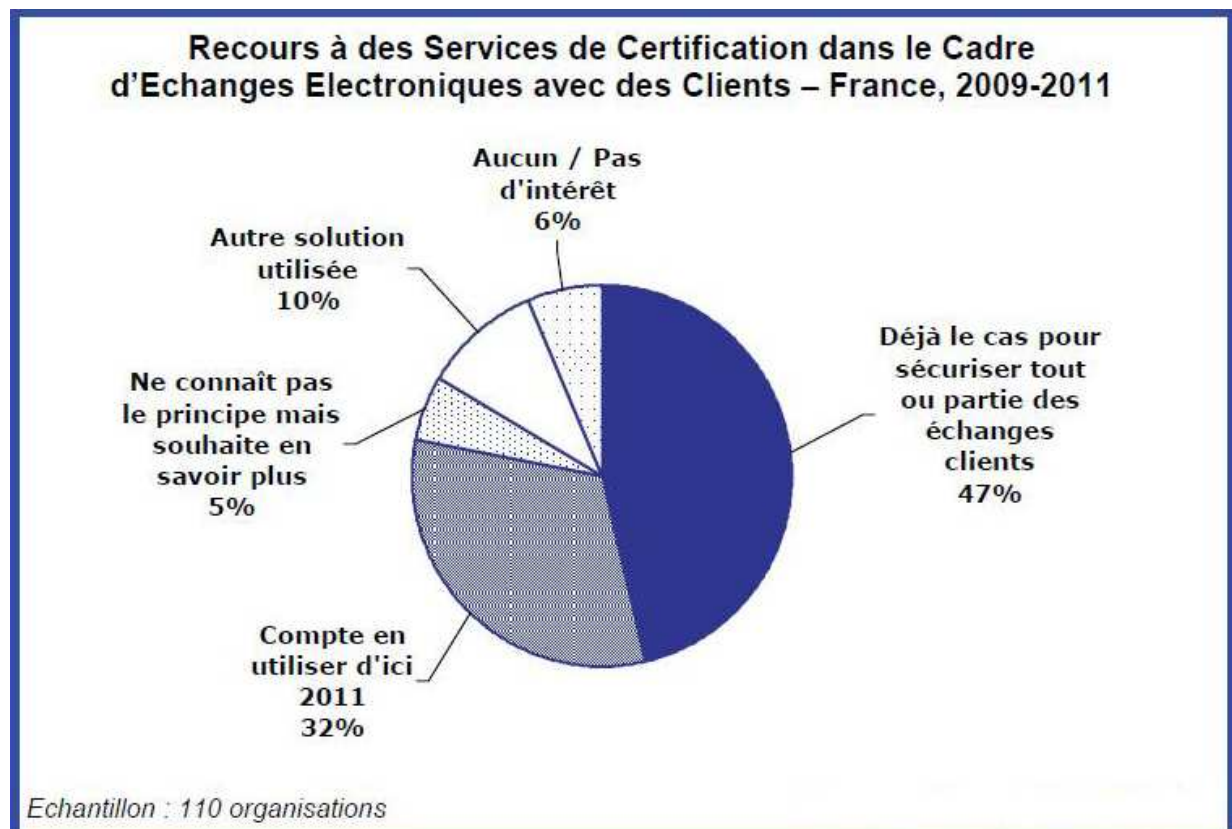
le cadre de transactions effectuées avec des clients. D'ici 2011, elles devraient être 79% à recourir à ces services ce qui présage une forte demande dans ce domaine !

En outre, 60% de ces organisations privilégient ou privilégieront le certificat électronique multi-usages qui peut être utilisé pour différent type de procédures et pas uniquement celles à vocations commerciales (téléprocédures administratives, financières, etc.). Elles ne sont que 20% à recourir ou souhaiter recourir à des certificats mono-usage.

Ces certificats électroniques ont ou auront pour vocation principale de :

- Garantir l'intégrité des contenus échangés et les protéger ;
- Signer électroniquement en ligne (via des extranets ou sites Internet) des contenus qui ont une valeur probante (contrats notamment) et garantir l'authenticité de ces contenus ainsi échangés ;
- Authentifier les personnes accédant aux contenus ;
- Garantir la date de l'échange des contenus (horodatage) ;
- Identifier formellement les parties.

Parmi les autres usages, il faut noter la conservation et l'archivage des contenus en lieu sûr sans possibilité de les modifier, la garantie de la preuve de l'échange et l'attestation du moment d'un consentement.



Bénéfices clients et commerciaux des solutions de sécurisation des échanges électroniques

Les solutions sécurisant les transactions électroniques peuvent contribuer sans conteste au développement des ventes et à l'optimisation de la relation client. C'est notamment le cas de la signature électronique qui voit son usage s'amplifier car, au-delà de son caractère probant, elle instaure la confiance, et permet d'augmenter le nombre de transactions effectuées en ligne (signatures de contrats, souscriptions, actes de vente, échanges de données confidentielles de consentement, etc.) et donc de favoriser le développement des affaires.

En période de crise, les projets de sécurisation des échanges électroniques peuvent donc être de formidables leviers pour accélérer les processus commerciaux, diminuer les coûts, accroître l'efficacité, améliorer la relation client.



Le recours à des solutions de confiance génère des gains et bénéfices qu'il est relativement aisé de quantifier. Nous distinguons deux types de bénéfices : ceux associés à la dématérialisation des échanges et des documents et ceux inhérents aux services de confiance. Les organisations interrogées sont généralement plus à l'aise pour avancer des indicateurs de ROI sur les apports de la dématérialisation :

Diminution des coûts d'affranchissement, d'impression (printing), associés à l'émission de courriers papier avec accusé de réception ou encore à l'archivage :

ainsi, grâce à la dématérialisation de factures, qu'elles soient entrantes ou sortantes, le coût de traitement peut être divisé par 2 ou 3 selon les entreprises interrogées. Le recours à la dématérialisation fiscale de factures permet, sous certaines contraintes imposées par la législation, de s'affranchir des factures au format papier. Le coût de traitement d'une telle facture peut ainsi être réduit, de même que les frais d'impression et d'affranchissement ;

Gain de temps : la dématérialisation de documents spécifiques (tels que des plans, par exemple) réduit considérablement les délais d'envoi ; la dématérialisation des factures permet de réduire le délai de clôture des comptes, de raccourcir le temps de validation avant paiement, etc.

Du côté des échanges sécurisés, les organisations mettent en avant :

- La diminution de la fraude à la souscription ;
- L'accélération du business et l'augmentation des ventes en ligne : pour une compagnie d'assurance, le recours à la signature électronique pour signer des contrats en ligne a permis d'augmenter le nombre de contrats signés et mis en gestion. Avant, la société obtenait 36% de retours sur des contrats VAD (vente à distance). Avec la mise en place de la signature électronique, 100% des contrats signés en ligne sont validés sur une base de 200 contrats mensuels ;
- L'automatisation des processus de traitement : le chiffrement et la signature de documents confidentiels permettent de réduire les délais de leur prise en compte par les clients pour un opérateur de télécommunications. Ces délais se comptent désormais en jours à la place de semaines auparavant ;
- L'augmentation de la productivité : une banque avance améliorer sa productivité en ayant recours à la norme de cryptographie X509¹ et à des cartes OTP (One Time Password) dans le cadre de transactions sur son site de « e-banking »

1 X.509 est une norme de cryptographie de l'Union Internationale des Télécommunications (IUT) pour les infrastructures à clés publiques (PKI) qui établit entre autres les formats standard de certificats électroniques et un algorithme pour la validation de chemin de certification (source : Wikipedia).

Freins à la mise en place des solutions de sécurisation des échanges électroniques

Malgré ces bénéfices clients et commerciaux, les projets de sécurisation des échanges électroniques associés aux relations contractuelles avec les clients font face à divers points de blocage qui peuvent en retarder ou avorter leur mise en oeuvre.

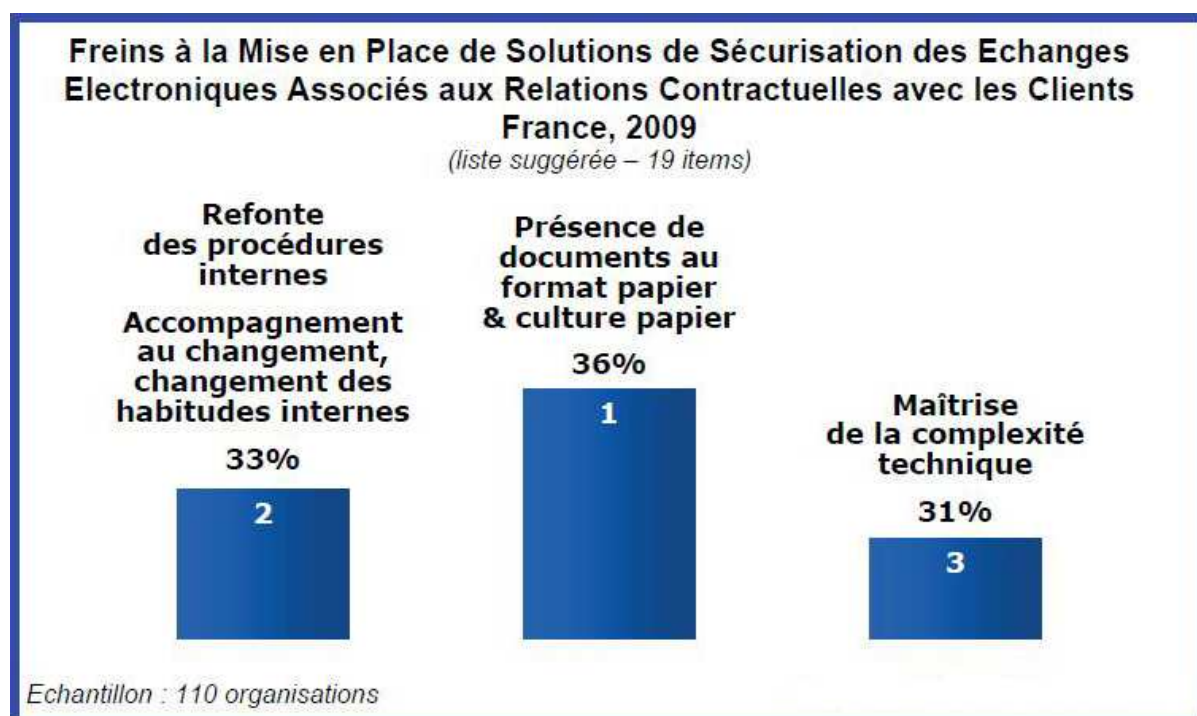
La présence de documents au format papier, encore nombreux, et la culture du papier tant en interne que chez les clients figurent au premier rang des freins majeurs mis en avant par les organisations interrogées. Il s'agit plus d'un frein inhérent à l'essor de la dématérialisation et des échanges numériques que liés aux projets de sécurisation associés.

Le corollaire est que les organisations ont besoin d'accompagner le changement et d'encourager la mutation des habitudes. De tels projets induisent aussi parfois de refondre certaines procédures internes et donc peuvent soulever des réticences.

Enfin, les projets de sécurisation des échanges électroniques sont vus comme des projets techniques complexes car ils portent sur des technologies le plus souvent nouvelles ou récentes dont la maîtrise n'est pas ouverte à tous.

Les organisations citent par ailleurs comme autres freins : la maîtrise des impacts sur les systèmes existants (intégration, interopérabilité, etc.), les investissements à consentir, le manque de ROI associé, la sensibilisation et la formation des clients au sujet, la maîtrise de la complexité juridique et/ou fiscale ainsi que la compréhension de la réglementation, la complexité des procédures associées, l'absence de standards/normes...

Un facteur « risque » est aussi mis en avant pour ce sujet complexe : risques associés à ces projets aussi bien au niveau des impacts humains et sociaux (gains en équivalent temps plein par exemple) que sur la responsabilité humaine et légale.



Nature des prestataires sollicités et importance des conseils externes

Les freins, plus spécifiquement organisationnels et techniques, associés aux projets de sécurisation des échanges électroniques liés aux relations contractuelles avec les clients, incitent les organisations à faire appel à des experts pointus.

En 2009, 71% des organisations interrogées précisent recourir à des conseils externes pour choisir notamment leurs solutions de sécurisation. Il est intéressant de constater, qu'au-delà des conseils classiques, les organisations se tournent aussi vers des associations spécialisées sur ces thématiques (fédérations, communautés, instances métier...), d'autres organisations ayant déjà une expérience sur le sujet et pouvant la transmettre à des tiers, l'administration ou encore des juristes (cabinets d'avocats par exemple).

De manière générale, les organisations font plus spécifiquement appel à des éditeurs de logiciels (pour 48% d'entre elles) et à des sociétés de services informatiques et/ou des intégrateurs (42%).

Les prestataires de certification sont mis en avant par 40% des organisations interrogées. Ils devraient continuer leur progression, poussés par les besoins en services de certification précédemment évoqués. Il en est de même pour les tiers archiveurs, privilégiés par 30% des organisations.

Les fabricants de support matériel (cartes à puce, clés USB...) sont mentionnés par 28% des organisations. Ces acteurs sont peut-être moins visibles car ils sont le plus souvent partenaires des catégories d'offres précédentes, plus en contact direct avec les organisations clientes.

Parmi les autres catégories de prestataires indiquées, mais dans une moindre proportion, figurent les hébergeurs (24%), les tiers horodateurs (23%), les opérateurs EDI (18%), les opérateurs de télécommunications (14%), les banques (11%), et les experts comptables (4%).

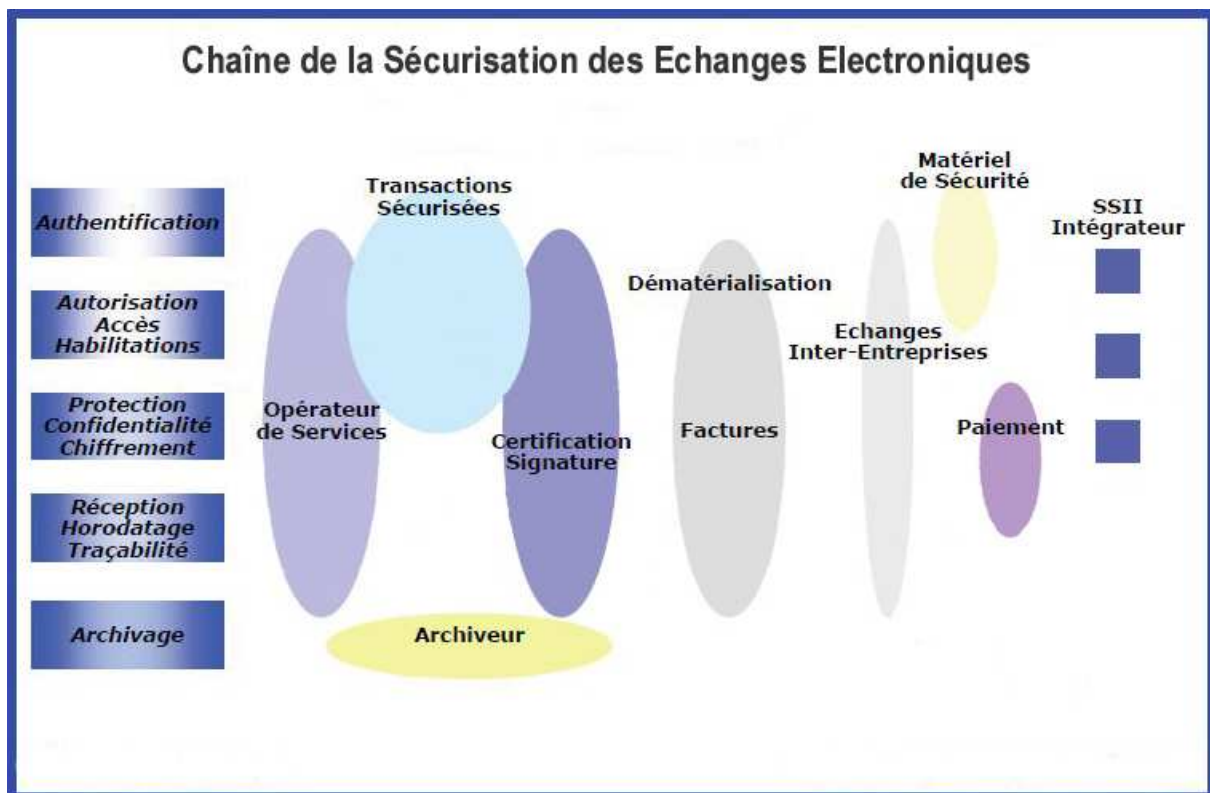


Positionnement d'acteurs sur la chaîne de la sécurisation des échanges électroniques

Marché particulièrement complexe, la sécurisation des échanges électroniques fait intervenir un écosystème d'acteurs, de domaines et de cultures parfois différents mais le plus souvent complémentaires.

La sécurisation des échanges électroniques voit intervenir aussi bien des acteurs très spécialisés sur un domaine d'activité, comme les cartes à puce ou les solutions de paiement en ligne, que des acteurs plus globaux qui vont adresser plusieurs briques fonctionnelles en propre ou avec des partenaires (80% des prestataires interrogés dans le cadre de cette étude aussi indiquent avoir établi des partenariats pour compléter leurs offres dans ce domaine).

La complexité de la chaîne de valeur et la spécificité de chacun de ses maillons entraînent bien souvent les entreprises à devoir aborder leurs projets selon des briques distinctes. Cependant, dès lors qu'elles souhaitent garantir leur processus « contrat-commande-facture-paiement », ces briques doivent nécessairement être liées entre elles et assemblées en cohérence. La difficulté pour les entreprises est donc de faire co-exister et d'orchestrer les différentes solutions retenues dans ce domaine, ce qui peut expliquer aussi que plus de 40% d'entre elles s'adressent à des intégrateurs et/ou à des prestataires de certification.



Le marché de la sécurisation des échanges électroniques se décompose entre la vente de matériels, la vente de logiciels et de prestations de services (conseil,

intégration, maintenance, exploitation, hébergement, services en mode SaaS - Software as à Service, services d'externalisation...). En ce qui concerne le marché français des logiciels et services associés aux solutions de sécurisation des échanges électroniques, il est estimé à 740 millions d'euros à fin 2009. Il devrait atteindre 990 millions d'euros en 2011 (soit +15,7% de croissance moyenne annuelle).

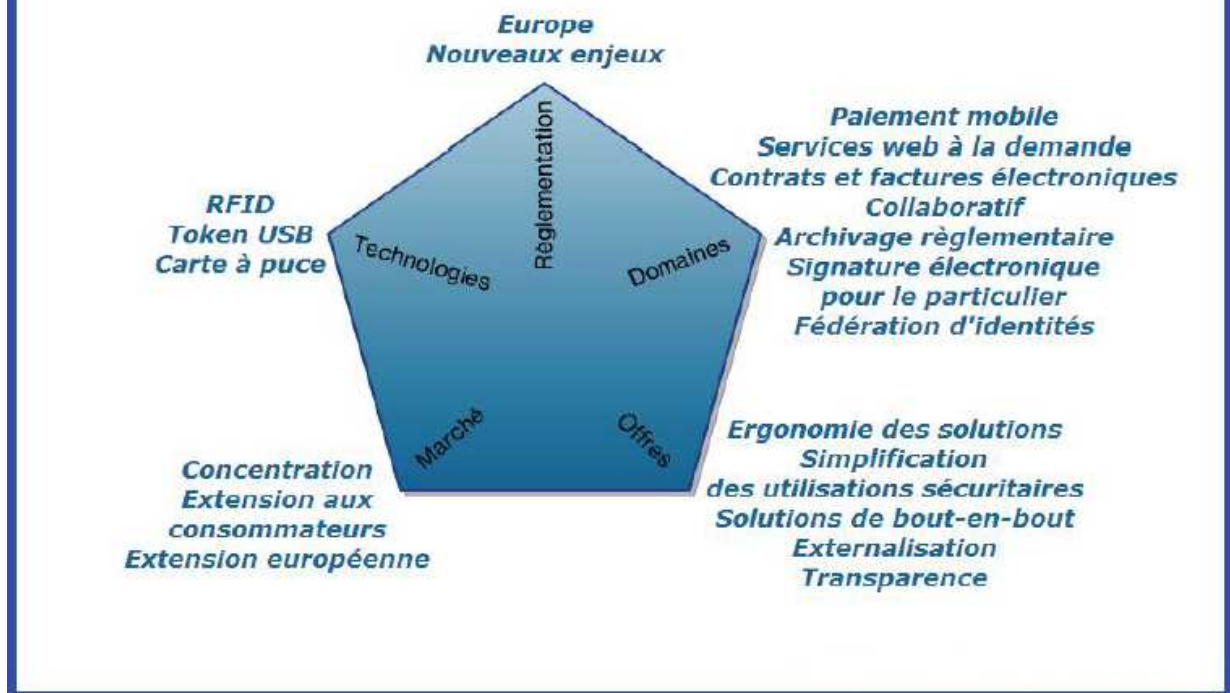
Tendances majeures d'ici 2011

D'ici 2011, nous anticipons plusieurs tendances de fond poussées par la progression de la dématérialisation et des échanges électroniques commerciaux. Ces tendances impacteront plus ou moins directement les projets de sécurisation des échanges électroniques associés à la relation contractuelle avec les clients et génèreront de nouveaux besoins et approches dans ce domaine.

Ces tendances sont principalement de cinq ordres et concerneront :

- Les domaines applicatifs suivants : le paiement via le mobile, les services web à la demande, la dématérialisation de contrats et de factures, les espaces collaboratifs (internes/externes) avec notamment la diffusion des applications de type web 2.0, les besoins associés en archivage probatoire, la signature électronique pour les particuliers, la fédération d'identités... ;
- Les technologies avec l'essor de la RFID (Radio Frequency Identification), le token USB et la carte à puce ;
- Les offres du marché qui devront se simplifier au niveau de leur utilisation et de leur ergonomie, couvrir un spectre fonctionnel plus étendu et en phase avec les besoins évolutifs des organisations, proposer des alternatives se rapprochant de l'externalisation ;
- Le marché lui-même qui devrait à la fois voir des concentrations d'acteurs mais aussi s'étendre à d'autres domaines ;
- L'évolution de la réglementation qui devra s'adapter aux nouveaux enjeux que la dématérialisation et au développement du numérique tant au niveau français qu'international (surtout européen).

Sécurisation des Echanges Electroniques Associés à la Relation Contractuelle avec les Clients : Principales Tendances d'ici 2011



Conclusion

Les principaux points à retenir en conclusion de cette analyse consacrée à la sécurisation des échanges électroniques associés à la relation contractuelle avec les clients sont les suivants :

- La dématérialisation, la traçabilité et la preuve des échanges constituent les catalyseurs clés des besoins en solutions de sécurisation sachant que les organisations souhaitent garantir avant tout le processus « contrat-commande-facture-paiement » ;
- La messagerie, les espaces collaboratifs et les sites de e-commerce sont les modes d'échanges avec les clients les plus concernés par la sécurisation ;
- Les besoins d'ici 2011 porteront sur des solutions d'archivage, authentification, signature électronique, gestion de preuve, historisation, authenticité et conformité. Ils engendreront une demande en services de certification électronique associés ;
- Les bénéfices escomptés des solutions de sécurisation mises en oeuvre sont plus spécifiquement les suivants : accélération et automatisation des processus dont ceux liés à l'acte de vente en ligne, accroissement de l'efficacité, baisse des coûts, amélioration de la relation client, développement de nouveaux services ;
- Parmi les éléments freinant les projets de sécurisation, les organisations notent le fort ancrage dans la culture du papier, les changements des processus internes que ces projets induisent ainsi que leur complexité technique ;

- Les responsables interrogés indiquent avoir besoin de conseils et favorisent le recours à des experts en sécurisation des échanges électronique ;

- La dématérialisation de factures et de contrats, l'essor des espaces collaboratifs avec le web 2.0 ainsi que le m-paiement figurent parmi les tendances clés à considérer d'ici 2011 qui devraient impacter les projets de sécurisation des échanges électroniques.

Solutions de Sécurisation des Echanges

Le besoin de garantie et de sécurité est dicté par les enjeux de la dématérialisation dont l'essor est sans commune mesure depuis quelques années. Les solutions proposées permettent de mettre en place les dispositifs nécessaires pour bénéficier des avantages de la dématérialisation sur les documents à valeur probante, ne pas perdre la sécurité qui existe dans le monde « matériel », et être en conformité avec la loi. Elles reposent sur l'utilisation de certificats numériques de tout niveau, la signature électronique, l'horodatage, la traçabilité, l'archivage des échanges ou encore l'utilisation d'espaces sécurisés.

Elles permettent de :

- **Certifier l'identité d'une personne physique ou morale connectée** (identification des signataires d'un contrat électronique, une facture, un bon à tirer, d'utilisateurs de téléprocédures ou d'applications diverses...).

- **Signer un document électronique.** Permettant aux clients et partenaires de signer via le web des documents à valeur probante (contrat, vente d'abonnement, bon de commande, facture, bon à tirer, demande en injonction de payer, services en ligne nécessitant une signature...) ;

- **Dater et horodater des documents échangés en ligne** (signature d'un contrat, archivage, envoi et réception de documents...). Service intégré à une application web qui permet de dater un document électronique à la seconde et ainsi de garantir son existence et son intégrité grâce à un jeton d'horodatage ;

- **Archiver électroniquement des documents à valeur probante** (contrat, rapport d'analyse, preuve électronique...). Au-delà de l'archivage, tracer les documents, faire des recherches a posteriori et valider la disponibilité des données.

En savoir plus sur nos offres...

MERCI DE NOUS CONTACTER POUR PLUS D'INFORMATIONS...

<http://digitaltrustscience.com>

Digital Trust Science a Division of Three Forest Company OMN LLC
220 East Delaware Avenue, Newark, Delaware DE 19711 USA - EIN 98-0490055
E-Mail : admin@digitaltrustscience.com - Phone : +1 302 261 53 30

Nuage de Tags

Digital Trust Science, conseille, entreprises, dématérialiser, développement durable, réduire, coûts, administratifs, risques, opérationnels, outils, productivité, sécurité, formations, suivi, conduite du projet, intégration, environnement, légales, plateforme, échanger, informations, stratégiques, non-répudiable, électronique, recommandé postal, dématérialisation, flux métiers, valeur probatoire, temps, argent, optimisation, documents, factures, fiches de paie, les contrats, documents administratifs, solution, impression, papier, communication électronique, scanning, réception, factures électroniques, factures papier, factures électroniques, archivage, légal, documents électroniques, canal, fournisseur, marché,