

**Edi Wolfensberger**

étudiant HES FHNW,  
ediwolfensberger@  
googleMail.com

**Florian Reck**

étudiant HES FHNW,  
reckf@gmx.ch

**Michael Wiedemann**

étudie la communication  
d'entreprise et le journalisme  
à la ZHW,  
wiedemann@privasphere.com

# Transmission électronique d'information fiduciaire par eMail

Utilité, motivation est qualification de processus de communications électroniques sécurisées

Le trafic d'eMail fait partie intégrante de la communication d'aujourd'hui et le monde des affaires ne pourrait plus se concevoir sans lui. Un échange toujours plus important de données électroniques offre cependant un nombre accru de possibilités d'attaques et mène de ce fait à des abus de plus en plus fréquents. Pour combattre ces abus, des entreprises développent des technologies permettant de réaliser et de garantir une communication sécurisée et authentifiée par Internet. Dans des branches telles que les fiduciaires ou les cabinets d'avocats et de notaires, le potentiel d'amélioration de la sécurité et d'augmentation de l'utilisation du trafic d'eMail est particulièrement élevé.

## Possibilités d'un système d'eMail sécurisé

Bien que le Secure Messaging rend possible d'un trafic d'eMail protégé et sans danger, de nombreuses entreprises renoncent encore à une telle assurance ou ont encore quelques craintes face au moyen rapide et simple de la communication en ligne. En collaboration avec PrivaSphere, les étudiants en ingénierie économique Florian Reck et Edi Wolfensberger (Fachhochschule Nordwestschweiz) ont étudié dans le cadre de leur travail de semestre dans

quelle mesure Secure Messaging peut être appliqué et utile peuvent être utiles dans le secteur fiduciaire et comment le trafic électronique des données pourrait être amélioré spécifiquement pour les fiduciaires. Ils ont par ailleurs expliqué pour quelles raisons de nombreuses entreprises renoncent encore à un système d'eMail sécurisé bien que la demande d'une communication par eMail sécurisée soit importante et que les exigences posées à un système d'eMail soient très élevées.

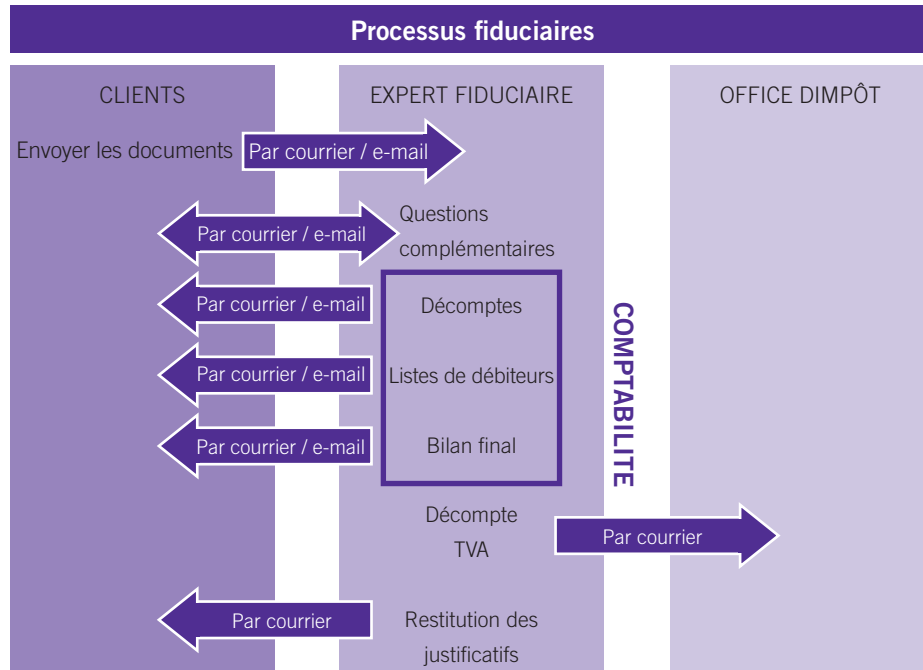
## Processus de fonctionnement de la communication d'entreprise

Après une première phase d'analyse, les étudiants se sont intéressés de plus près aux principaux processus de fonctionnement des fiduciaires et des cabinets d'avocats et de notaires en portant leur attention sur les échanges d'informations se faisant par écrit. Pour les fiduciaires, l'essentiel portait sur la comptabilité, les révisions et les déclarations d'impôt. Dans ces domaines, il existe un intense échange d'informations qui se fait encore majoritairement par courrier postal.

A l'exemple d'un processus de fonctionnement dans le secteur de la comptabilité (voir l'illustration), il est possible d'identifier et d'analyser

les moyens et les types de communication. Le graphique montre que dans le cadre d'un tel processus, le client reçoit plusieurs fois des informations et des documents par email ou par courrier postal. Dans le secteur fiduciaire, c'est avant tout la comptabilité qui enregistre une fréquence élevée d'échange d'informations qui nécessite un niveau de sécurité élevé. Pour tous les processus, la sensibilité dans le secteur des fiduciaires est moyenne. L'expert fiduciaire communique beaucoup avec son client, une grande partie de cette communication n'étant pas considérée comme sensible. Dès qu'il s'agit toutefois de transmettre divers documents, l'analyse débouche sur une sensibilité moyenne, voire élevée. Dans la comptabilité, les exigences posées à la sécurité et à la simplicité de la communication sont les plus élevées. C'est pourquoi le recours au Secure Messaging dans la comptabilité est particulièrement efficace.

Il ressort de divers entretiens menés avec des experts fiduciaires qu'il existe auprès des entreprises une forte motivation mais aussi certaines réticences qui favorisent ou gênent le recours à un système de Secure Messaging. Ces motivations et ces obstacles sont différents pour chaque fiduciaire mais ont souvent les mêmes motifs et se basent souvent sur les mêmes problèmes.



**Exigences de sécurité imposées par la loi**

De nombreuses entreprises ne voient encore aucun besoin de disposer d'un système d'eMail sécurisé. Elles pensent être en sécurité. Or, lors de l'envoi d'un simple courriel, diverses interventions de tiers peuvent survenir (voir figure ci-dessous). Par conséquent, aucune sécurité ne peut être donnée quant à l'authenticité du message transmis.

Pour l'expéditeur de données ou d'informations confidentielles, il existe diverses **bases légales**. Selon l'art. 321 CP, diverses catégories professionnelles, dont les contrôleurs, les avocats et les notaires, sont tenues de ne pas révéler des secrets dont ils ont eu connaissance dans l'exercice de leur activité. Par ailleurs, selon l'art. 398 CO, le mandataire est responsable de la «bonne et fidèle exécution du mandat». Cela signifie que les données sensibles doivent être transmises par voie électronique sécurisée. Si tel n'est pas le cas, il se pourrait qu'il y ait violation du secret professionnel et de l'obligation de diligence qui pourrait rendre l'expéditeur punissable. Mais il existe également des dispositions découlant de la protection des données qui doivent être prises en compte avec le trafic d'eMail. Les données personnelles doivent être protégées «contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées» (art. 7 de la Loi fédérale sur la protection des données). Un système d'eMail conventionnel ne peut en aucun cas garantir cette protection et ne devrait donc pas être utilisé pour des données confidentielles. En cas de dommage, il se pourrait ainsi que la

fiduciaire ou le cabinet d'avocat se voient obligés d'assumer leur responsabilité. Le **Secure Messaging réduit ce risque pratiquement à zéro**. La confirmation d'envoi reconnue en justice permet par ailleurs de disposer de toutes les preuves nécessaires. Par la vérification unique du partenaire de communication, il n'est possible d'envoyer un courriel qu'à ce dernier. D'éventuelles personnes avec des adresses de courriel similaires ne recevront pas l'eMail envoyé à une fausse adresse.

**Avantages du trafic d'eMail**

Pour des raisons de tradition, certaines entreprises restent attachées à d'anciennes valeurs telles que le courrier postal. A cela vient s'ajouter un certain scepticisme face à de nouvelles

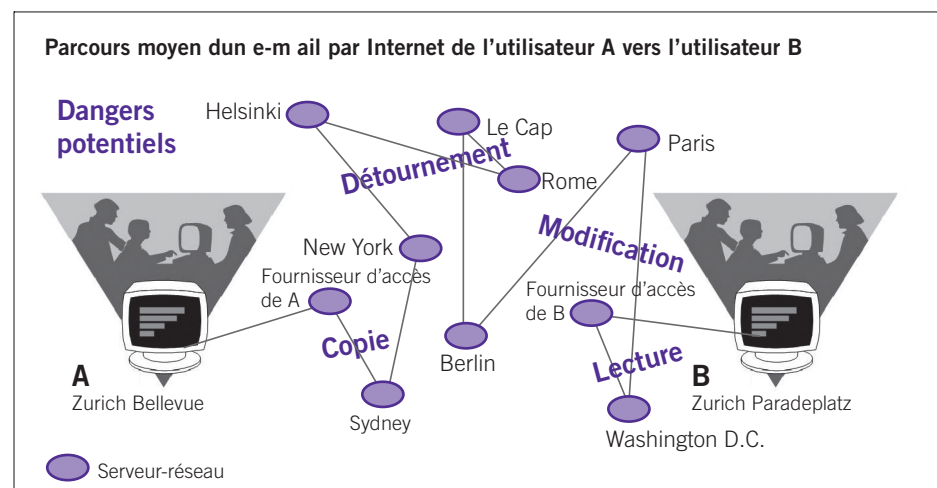
technologies et une certaine attitude négative et un état d'esprit conservateur face aux email. Or certaines entreprises ne savent pas quels dangers sont liés au courriel traditionnel. Souvent, c'est tout simplement l'ignorance de l'existence et de l'utilité du Secure Messaging qui empêche les entreprises d'adopter et d'utiliser un tel système.

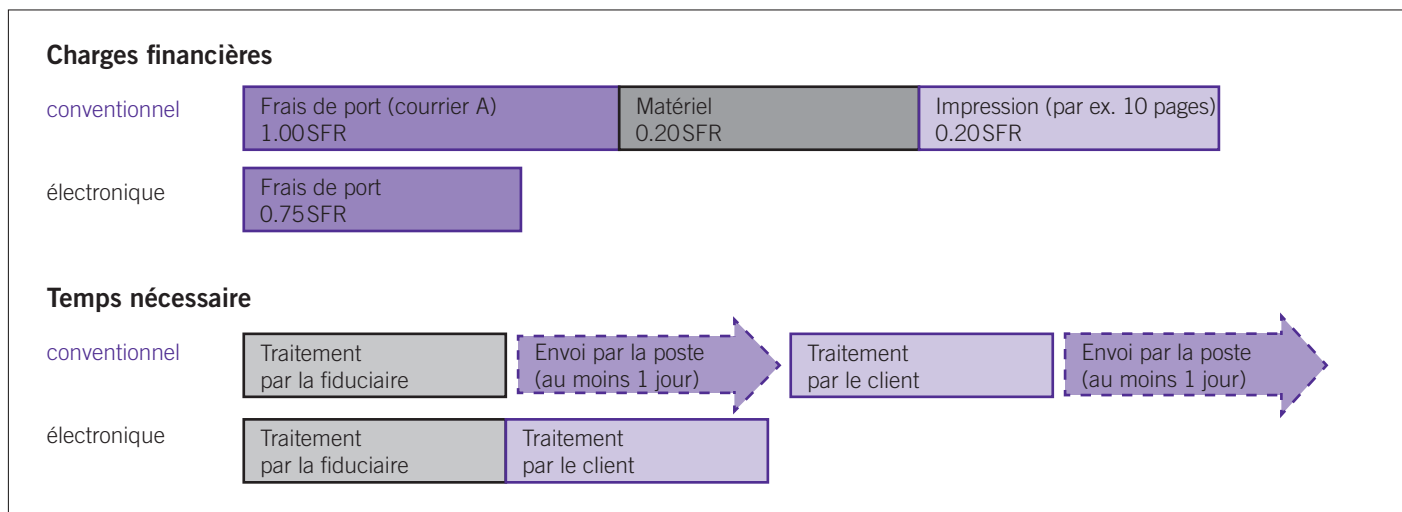
Ainsi, de nombreuses personnes interrogées pensent que la présence professionnelle assurée par le Secure Messaging et l'avance technique qui y est liée permettent justement d'améliorer l'image d'une entreprise. De cette façon, la sécurité et la fiabilité que préconisent de nombreux plans directeurs d'entreprises peuvent également être réalisées dans le domaine de la communication.

Le fait que les entreprises pensent qu'elles ont besoin d'une infrastructure spéciale pour recevoir des email sécurisés, respectivement qu'elles ne disposent pas de l'infrastructure nécessaire à cet effet, constitue parfois un autre obstacle. Pourtant, les possibilités permettant de communiquer par email de manière simple et sécurisée sans installations supplémentaires existent déjà. Par conséquent, un tel système répond non seulement aux exigences d'une entreprise mais il est très rapidement adopté par les utilisateurs en raison de son maniement très simple. En recourant au Secure Messaging, l'entreprise montre à ses clients qu'elle tire profit des possibilités permettant de réduire les risques et gagne ainsi leur confiance.

**Economies de temps et d'argent**

Pour les entreprises, les coûts liés à un tel système en raison des frais d'abonnement et des charges supplémentaires qui en découlent constituent souvent un obstacle. Or, grâce à une transmission plus rapide de données sen-





sibles, il est possible de rendre la communication avec les clients plus efficace, ce qui permet de réaliser des économies de temps et d'argent. De ce fait, les avantages et l'efficacité du courriel priment finalement. On peut démontrer ceci de manière très simple au moyen d'une comparaison entre un envoi électroniquement sécurisé et un envoi conventionnel. L'exemple pris en compte portait sur l'envoi d'une liste de débiteurs. Selon cette comparaison de coûts (voir graphique), l'exécution électronique de ce processus permet de réaliser diverses économies.

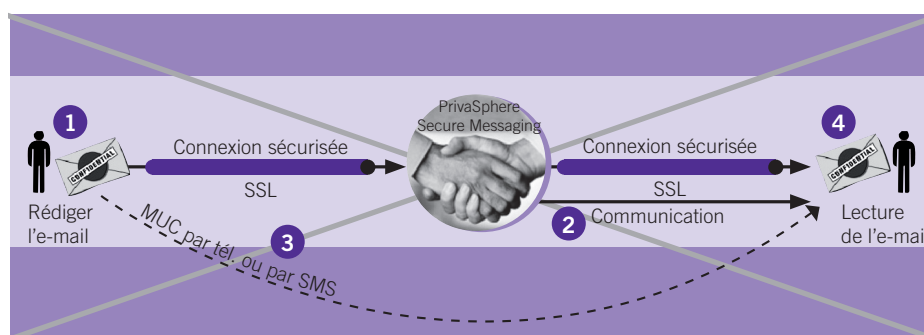
Les économies financières portent sur l'envoi. Les processus préliminaires sont identiques pour les deux types d'envoi et occasionnent les mêmes coûts. L'économie porte sur un envoi particulier qui est réalisé par le biais d'une plate-forme de courriel sécurisée en raison de son caractère hautement sensible. De manière conventionnelle, l'envoi se ferait par courrier postal – l'envoi en recommandé provoquerait des frais d'inscription supplémentaires. Si l'on pense que l'envoi d'une seule lettre (courrier A) provoque un coût supplémentaire d'env. 0.65 SFR par rapport à un courriel, on comprend aisément que le passage à l'envoi électronique permette de réduire considérablement les frais d'administration.

La transmission plus rapide permet de traiter les cas de manière plus rapide et plus efficace et donc de les conclure plus rapidement. Ceci constitue un important gain de productivité. En effet, le traitement électronique permet d'accélérer l'ensemble des processus de fonctionnement. Cela signifie que l'intervalle de temps séparant le début et la fin d'un mandat se réduit de manière importante. Le passage à un système de Secure Messaging empêche les longues «périodes de vide» nécessaires à l'envoi par courrier postal et permet de réduire le temps de travail.

### Davantage de sécurité et moins de frais

Secure Messaging est une prestation de services qui améliore considérablement aussi bien la sécurité que l'efficacité du trafic d'eMail. C'est tout spécialement aux branches dont la communication est très sensible, par exemple le secteur fiduciaire, qu'un tel système offre de nombreux avantages. Les entretiens menés avec des experts fiduciaires, des avocats et des notaires montrent qu'il reste encore à faire un

intense travail de persuasion quant aux dangers et aux possibilités de la communication en ligne. Des entreprises de service telles que PrivaSphere proposent déjà un système permettant de simplifier les processus de communication d'entreprise et d'augmenter très fortement la sécurité d'un courriel. Ainsi, l'objectif d'une entreprise doit être de faire des exigences posées à un système d'eMail un véritable standard, non seulement en raison de son utilité évidente mais également en raison des nombreux dangers liés au trafic d'eMail. ■



#### Secure Messaging

L'expéditeur rédige un eMail dans son progiciel de d'eMail ou en ligne par le biais d'une liaison sécurisée sur la plate-forme Secure-eMail. Le récepteur d'un tel eMail sécurisé est informé par eMail usuel qu'un message confidentiel a été déposé pour lui sur la plate-forme. Le récepteur reçoit de l'expéditeur un code d'accès unique. (Pour des raisons de sécurité, cette communication se fait personnellement ou par téléphone/SMS). Ce code permet au récepteur d'aller chercher le message confidentiel, y compris les documents annexes. Pour d'autres contacts avec un client déjà enregistré sur la plate-forme Secure-eMail, le recours à un tel code n'est plus nécessaire. Pour l'emploi du Secure Messaging, aucun logiciel et aucune installation supplémentaire n'est nécessaire. Les prestations de services de PrivaSphere s'intègrent très aisément au programme d'eMail standard du client. Il est ainsi possible d'expédier et de recevoir des eMail sécurisés depuis le progiciel d'eMail habituel (par exemple Outlook, Outlook Express, Lotus, etc.). Etant donné qu'il s'agit d'une plate-forme Internet et non pas d'un logiciel à installer, l'utilisateur a également la possibilité d'avoir accès à une plate-forme pour eMail sécurisée depuis n'importe quel ordinateur disposant d'un accès à Internet, c'est-à-dire également lorsqu'il est en déplacement.