



Courriels sécurisés

Recommandation de norme

Version 1.1

16 novembre 2011

Sebastian Penalosa
Directeur, TI et relations-clients
CEPA/CSIO
Centre d'étude de la pratique d'assurance
110, rue Yonge, bureau 500
Toronto (ON) M5C 1T4

Table des matières

1	Sommaire	3
1.1	Objectif du document et public cible.....	3
1.2	La problématique	3
1.3	L'histoire	3
1.4	La solution	4
1.5	Pourquoi cette solution TLS est-elle importante?	4
2	Courriels sécurisés	5
2.1	La problématique	5
2.2	Les solutions envisageables	5
2.3	La solution recommandée – le cryptage TLS	6
2.3.1	Qu'est-ce que le cryptage TLS?.....	6
2.3.2	Comment fonctionne le cryptage TLS?	6
2.3.3	Avantages et inconvénients du cryptage TLS	7
3	Mise en œuvre	7
3.1	Exigences générales.....	7
3.2	Comment confirme-t-on le fonctionnement?.....	7
4	Que faire si mon système n'est pas compatible avec le protocole TLS?	8
4.1	Acheter un serveur.....	8
4.2	Trouver un hôte indépendant	8
4.3	<i>Microsoft Exchange</i> en ligne	8

1 Sommaire

1.1 Objectif du document et public cible

Le présent document de référence s'adresse aux sociétés d'assurance et aux cabinets de courtage œuvrant dans le secteur des sociétés d'assurance multirisques au Canada. Il présente un aperçu de la norme sur les courriels sécurisés qui permet l'échange de renseignements en toute sécurité entre les cabinets de courtage et les assureurs. Le document renseigne le personnel technique au sujet de la préparation et de l'administration de la mise en œuvre. Il est à noter qu'il s'agit d'une solution qui permet d'atténuer, et non d'éliminer, les risques associés aux courriels.

1.2 La problématique

De nos jours, les sociétés d'assurance et les cabinets de courtage s'exposent à divers risques en échangeant, dans le réseau Internet ouvert, des courriels contenant des renseignements privés au sujet des assurés, notamment :

- les renseignements figurant sur leur carte de crédit et d'autres renseignements bancaires;
- les renseignements figurant sur leur permis de conduire;
- leur adresse personnelle;
- des renseignements personnels sur leur état de santé.

L'envoi de courriels dans le réseau Internet ouvert enfreint les pratiques courantes en matière de sécurité et pourrait entraîner l'interception de renseignements personnels par une source extérieure.

1.3 L'histoire

En Amérique du Nord, le transfert de courriels contenant des renseignements personnels dans le réseau Internet ouvert existe depuis plusieurs années, et aucune inquiétude n'a jamais été soulevée à cet égard. En automne 2008, l'ACAC et son homologue américain ont commencé à étudier des solutions de rechange possibles.

Cet enjeu est devenu hautement prioritaire au fil du temps et constitue aujourd'hui l'un des trois principaux enjeux auxquels le comité technologique de l'ACAC est confronté. Après avoir étudié les solutions envisageables, le comité a proposé au CEPA de collaborer à l'élaboration d'une norme applicable à l'ensemble du secteur.

Dans les mois qui ont suivi, nous avons rencontré à plusieurs reprises les représentants de l'ACAC et certains spécialistes en matière d'architecture de sécurité provenant de diverses sociétés d'assurance afin de discuter des possibilités. Une validation de principe a été élaborée en compagnie de deux cabinets de courtage et de plusieurs sociétés d'assurance dans le but de confirmer que la solution recommandée conviendrait au secteur.

La recommandation finale fut présentée au comité technologique de l'ACAC le 20 juin 2011. Nous souhaiterions maintenant implanter cette solution à l'échelle du secteur.

1.4 La solution

Le CEPA a collaboré avec l'Association des courtiers d'assurances du Canada (ACAC) et plusieurs spécialistes en matière d'architecture de sécurité provenant de diverses sociétés d'assurance dans le but d'étudier les différentes options possibles et de formuler une recommandation. Nous avons pris la décision de formuler une recommandation de norme faisant appel au protocole TLS pour le cryptage de sécurité, car il s'agit d'une norme ouverte et compatible avec toutes les solutions de courriels d'entreprise. Diverses solutions de série ont été examinées, mais aucune d'entre elles ne répondait aux critères de transparence et de convivialité requis pour que cette solution soit acceptée comme étant la norme à l'échelle du secteur. La solution et sa mise en œuvre seront expliquées en profondeur dans le document principal.

Il faut mentionner que même si le protocole de sécurité TLS crypte le message en cours d'envoi, il n'est pas garanti que l'expéditeur soit bel et bien la personne qu'il prétend être. Il faut également souligner que le message est sécurisé lors de son acheminement d'un serveur de courriels à un autre, mais ne l'est plus après avoir atteint le réseau local des organisations. Cela dit, le protocole ne répond pas entièrement aux exigences de conformité à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), mais il augmente considérablement le niveau de sécurité actuel.

1.5 Pourquoi cette solution TLS est-elle importante?

Cette recommandation constitue une solution uniforme et peu coûteuse à mettre en œuvre pour l'échange sécurisé de courriels entre les sociétés d'assurance et les cabinets de courtage. Elle permet de résoudre un grave problème dans les plus brefs délais.

2 Courriels sécurisés

2.1 La problématique

Il n'existe actuellement aucune norme au sein du secteur qui puisse assurer l'échange sécurisé de courriels entre plusieurs utilisateurs provenant d'organisations distinctes. Le diagramme qui suit illustre la configuration typiquement employée pour l'échange de courriels entre un cabinet de courtage et une société d'assurance :

Email Server = Serveur de courriel

Firewall = Pare-feu

User = Utilisateur

Email Client = Client de courriel (de messagerie)

Public Internet = Internet public

Insurance Broker = Courtier d'assurance

Insurance Company = Société d'assurance

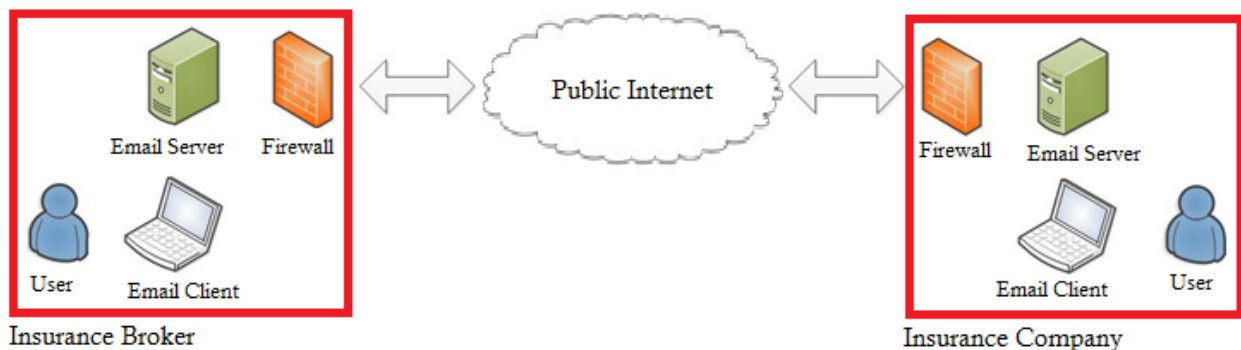


Figure 2.1-1 : Échange de courriels typique

Cette image indique que le courriel, après avoir quitté le serveur de l'expéditeur, aboutit dans le réseau Internet public sans être crypté ni protégé par aucune source externe pour ensuite se retrouver dans le serveur du destinataire. Les renseignements envoyés risquent ainsi d'être interceptés et utilisés à des fins malveillantes.

2.2 Les solutions envisageables

Au cours de notre examen, nous avons étudié diverses solutions qui s'offraient à nous :

1. Cryptage TLS – solution offerte à titre de norme ouverte créée par l'*Internet Engineering Task Force* (IETF) et compatible avec tous les serveurs de courriel d'entreprise (p. ex., Microsoft Exchange et Lotus Notes). Pour s'en servir, l'utilisateur devrait se procurer un certificat SSL auprès d'un détaillant en ligne et se le faire installer dans son système de courriels, celui-ci étant facile à implanter et peu coûteux.

2. Logiciels de série – offerts dans un grand choix de marques. Ces produits logiciels sont aussi compatibles avec les principaux serveurs de courriel d'entreprise; cependant, leur achat exigerait l'obtention d'une licence pour chaque adresse de courriel utilisée, ce qui occasionne des coûts augmentant de manière exponentielle. Voltage, IronPort, Comodo et ePost, pour ne nommer que ceux-là, font partie de ces produits.
3. Serveur de courriel privé – il permettrait aux cabinets de courtage d'envoyer des courriels aux sociétés d'assurance par l'entremise d'un environnement s'apparentant à un portail. L'élaboration d'un tel serveur serait toutefois assez coûteuse et entraînerait de très longues interruptions des activités du courtier. De plus, chaque société d'assurance aurait besoin d'un « serveur portail » de ce genre, ce qui non seulement ne résoudrait pas le problème, mais en occasionnerait également un autre.

2.3 La solution recommandée – le cryptage TLS

2.3.1 Qu'est-ce que le cryptage TLS?

Le protocole de sécurité de la couche transport (TLS) est un protocole de cryptage qui assure la sécurité des communications par Internet. En termes simples, il s'agit d'un protocole qui sécurise les données pendant qu'elles sont acheminées sous forme de courriel, vers un site Web ou pour toute autre raison de sécurité jugée nécessaire.

2.3.2 Comment fonctionne le cryptage TLS?

L'établissement d'une connexion TLS nécessite une « poignée de main », c'est-à-dire une certaine liaison entre les deux serveurs de courriel, afin de permettre l'envoi du message. Le diagramme suivant explique comment cette liaison s'établit :

Email Server = Serveur de courriel

Public Internet = Internet public

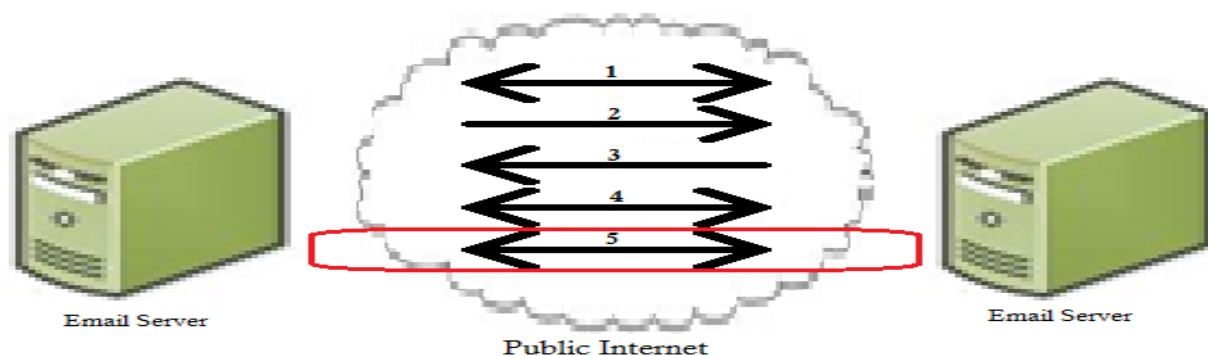


Figure 2.3-1 Négociation typique d'une clé cryptographique TLS

1. Une connexion est établie entre les serveurs de courriel de l'expéditeur et du destinataire.
2. L'hôte expéditeur demande le cryptage TLS pour l'envoi du message.

3. L'hôte destinataire accepte le cryptage TLS.
4. Les serveurs de courriel s'échangent les clés cryptographiques pour permettre le transfert du message.
5. Le message crypté (avec la clé cryptographique mentionnée à l'étape précédente) est transféré.

2.3.3 Avantages et inconvénients du cryptage TLS

Tout changement survenant dans l'univers des technologies de l'information entraîne des effets positifs et négatifs. Il est toutefois primordial que les effets positifs l'emportent sur les effets négatifs. Heureusement, l'utilisation du protocole TLS visant à sécuriser les messages électroniques comporte de nombreux avantages et très peu d'inconvénients.

AVANTAGES	INCONVÉNIENTS
- Faible coût de mise en œuvre	- Cryptage du message, mais aucune vérification de l'expéditeur
- Utilisation d'une norme ouverte	- Délai d'envoi du courriel prolongé de quelques millisecondes en raison des négociations de clés cryptographiques
- Implantation facile dans tous les systèmes de courriel d'entreprise	- Cryptage du message uniquement dans Internet, et non dans le réseau de l'organisation
- Invisible à l'utilisateur final	
- Cryptage des fichiers de texte ainsi que les pièces jointes	
- Solution éprouvée par plusieurs assureurs et cabinets de courtage	

3 Mise en œuvre

3.1 Exigences générales

Toute société qui désire recourir au protocole de cryptage TLS doit se procurer un certificat SSL pour que le protocole fonctionne. Ces certificats sont vendus auprès de divers détaillants en ligne, et leur prix varie de 45 à 100 \$ par année.

3.2 Comment confirme-t-on le fonctionnement?

Afin de vérifier si votre serveur de courriel est bien configuré pour l'envoi de courriels sécurisés au moyen du protocole de cryptage TLS, vous devez trouver un autre partenaire dont le système est configuré pour ce protocole puis échanger des courriels avec lui. Vous devez ensuite rechercher les données suivantes dans les en-têtes Internet :

Microsoft Mail Internet Headers Version 2.0

Received: from *ssmtl104.axa-canada.com* ([10.1.2.5]) by *ssmtl102.axa.ca* with Microsoft SMTPSVC(5.0.2195.7381);

Wed, 25 May 2011 15:08:02 -0400

X-AuditID: 0a010204-b7cc6ae0000071e1-59-4ddd539116ea

Received: from *mail189.messagelabs.com* (*mail189.messagelabs.com* [85.158.139.179])

(using TLS with cipher AES256-SHA (AES256-SHA/256 bits))

(Client did not present a certificate)

by *ssmtl104.axa-canada.com* (Symantec Brightmail Gateway) with SMTP id 98.CD.29153.2935DDD4; Wed, 25 May 2011 15:08:02 -0400 (EDT)

Veillez prendre note que les en-têtes Internet varient selon le système; toutefois, si votre message en cours d'envoi a été sécurisé au moyen du cryptage TLS, l'en-tête l'indiquera.

4 Que faire si mon système n'est pas compatible avec le protocole TLS?

Malheureusement, certains systèmes ne sont pas compatibles avec le protocole TLS. Voici quelques suggestions que vous pouvez suivre si vous désirez profiter du cryptage TLS au bureau.

4.1 Acheter un serveur

Il s'agirait d'une décision dispendieuse, car il vous faudrait d'abord acheter le matériel et les logiciels. Ensuite, vous auriez à configurer vous-même le serveur et, en même temps, vous pourriez configurer le cryptage TLS. Vous prendriez ainsi le plein pouvoir en étant hôte de votre propre serveur; par contre, vous auriez à assumer les coûts d'entretien de votre serveur.

4.2 Trouver un hôte indépendant

Au Canada, de nombreux fournisseurs de TI offrent l'hébergement d'adresses de courriel à un prix abordable. Nous vous suggérons de vous renseigner auprès de diverses entreprises et de demander des devis distincts afin de vous assurer de payer un prix raisonnable. Il s'agirait là d'un bon compromis vous permettant d'avoir le plein pouvoir de votre serveur courriel sans vous préoccuper des aspects techniques, que vous confieriez à une entreprise de TI moyennant un certain coût.

4.3 Microsoft Exchange en ligne

Microsoft propose désormais une version en ligne de sa solution Microsoft Exchange pour seulement 5 \$ par mois par utilisateur. Vous pouvez ainsi profiter du protocole TLS tout en conservant votre domaine et vos adresses de courriel actuels.