Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: "Swiss Secure Messaging Trust Center" : la sécurité des courriels astucieusement améliorée
Autor: Hauser, Ralph
DOI: https://doi.org/10.5169/seals-823461

Cyber

« Swiss Secure Messaging Trust Center » - La sécurité des courriels astucieusement améliorée

Ralph Hauser
CEO Privasphere

Les communications électroniques par courriel ressortissent aux applications informatiques les plus utilisées mais aussi les plus risquées ; elles restent toutefois trop souvent négligées, relativement aux politiques de sécurité des entreprises et administrations.

Plusieurs études constatent que plus des deux-tiers des flux d'informations commerciales ou de sécurité transitent, d'une manière ou d'une autre, par la messagerie électronique, que cela soit sous forme de texte, ou de pièces jointes présentant un intérêt sécuritaire.

Afin que les communications par messagerie électronique puissent aspirer à être utilisées de manière sûre, confidentielle et efficiente, les standards de sécurité y-afférents se doivent d'être vérifiés et améliorés de manière continue.

Considérant d'une part que la confiance en une multitude d'émetteurs de certificats de sécurité est écornée et que la « Certificate Transparency Initiative » de Google n'est essentiellement utile qu'après un sinistre, un projet commun de plusieurs cantons, inspirés par ailleurs de plusieurs organisations « feu-bleu » et d'organismes financiers, essentiellement des banques cantonales, a porté sur les fonts baptismaux le « Swiss Security Messaging Trust Center » ou « SSMTC ». https://ssmtc.ch

L'idée originelle, afin d'augmenter sensiblement le niveau de sécurisation des échanges, consiste en ce que les principales organisations puissent confirmer directement leurs certificats, se prémunissant ainsi des « moutons noirs » de la communauté des émetteurs de certificats.

L'utilisation du SSMTC permet un chiffrement systématique de toutes les communications par le biais de certificats, à destination des domaines de réception accrédités. Pour l'utilisateur final, cela signifie qu'il n'a plus à se préoccuper de la confidentialité de ses transmissions. Celle-ci est donnée, pour autant que :

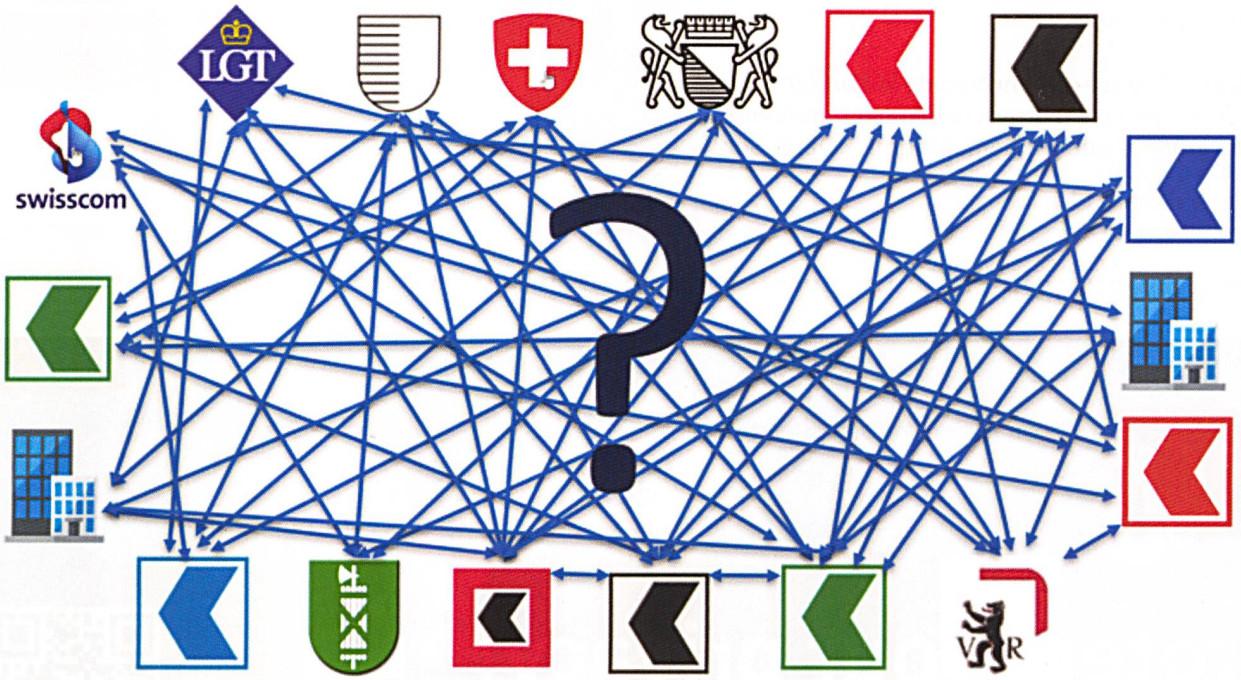
- La sécurité au sein des domaines soit garantie, ce qui libère d'assurer la sécurité des messages proprement-dits jusqu'à l'ordinateur du destinataire
- Les processus au sein du domaine de réception, relativement aux erreurs d'acheminement soient, sous l'angle des processus, suffisamment sécurisés et que le secret de fonction ou d'autres obligations légales similaires, relatives à la préservation du secret où à l'effacement des données soient respectés.

Protection contre les attaques de type « Man-in-the-Middle » - Elévation de la sécurisation grâce au « Pinned TLS » obligatoire

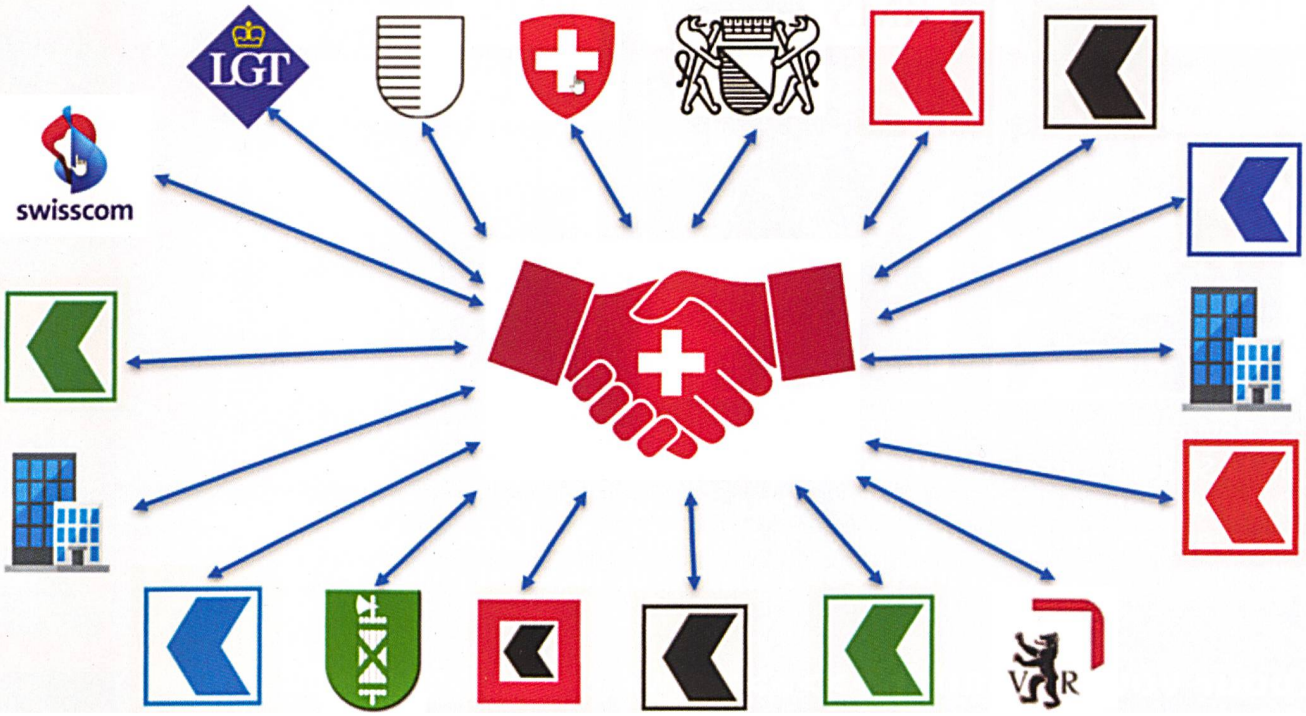
Dans cette configuration, le « NIP », sorte d'épingle-à-nourrice, relie l'émetteur du message au certificat du réseau destinataire de manière non-falsifiable. Pour ce faire, l'expéditeur reçoit des informations supplémentaires relativement au certificat. En pratique, le « pinning » est la résultante d'un « Hash » obtenu d'une clef publique, par exemple par un algorithme SHA256 sur un certificat conforme au standard X.509. Du fait que la valeur issue de l'emploi de l'algorithme SHA256 ne peut se reposer que sur la paire de clefs publiques/privées du domaine destinataire pré-enregistré, et sous réserve de l'intégrité de l'algorithme de cryptage choisi, une interception malveillante d'un tiers est exclue.

A supposer, par extraordinaire, qu'un assaillant se situerait effectivement dans la position du « Man-in-the-Middle » et ferait état d'un certificat apparemment valable au dire des instituts de certification, cette fraude serait détectée et le courriel ne pourrait pas être décrypté à sa destination, faute d'accréditation du certificat malveillant par la plateforme SSMTC.

Man in the middle Attack?



Swiss Secure Messaging Trust Center (SSMTC



Quid du SSMTC?

Pour l'heure, le SSMTC est une initiative suisse, mais les premières étapes d'une expansion internationale sont en voie d'élaboration.

Par ailleurs, et grâce au concours de la *Fondation My-D*, le SSMTC est en voie d'être sensiblement amélioré:
En effet, grâce à une implémentation « Open Source » sous « smimeJS », l'on peut désormais également transmettre jusqu'à un Go de données à tout destinataires de manière cryptée, en mode point-à-point.

Pour plus d'informations sur le SSMTC r:
https://ssmtc.ch

R. H.