Certificats S/MIME

Avantages et bonnes pratiques de la signature et du chiffrement des e-mails

LIVRE BLANC GLOBALSIGN

www.globalsign.fr

SOMMAIRE

INTRODUCTION

Dans un contexte d'intensification des cybermenaces, aucune organisation – quelle que soit sa taille – ne peut se permettre de traiter à la légère l'intégrité ou la confidentialité de ses données. Chaque jour, des données sensibles transitent, sans protection, par une multitude de réseaux relais et de services tiers.

Alors que les menaces en ligne gagnent du terrain avec l'essor du stockage de données dans le Cloud et à distance, la lutte contre un nouveau spectre de vulnérabilités de sécurité s'intensifie. Il existe plusieurs solutions pour contrer les risques potentiels d'interception et d'altération des données : les certificats numériques X.509 basés sur le protocole de sécurité S/MIME représentent, à ce titre, la solution la plus complète et la plus simple. Standard de référence pour la sécurisation des e-mails, S/MIME garantit la confidentialité, l'intégrité et la non-répudiation des messages, et offre ainsi une protection contre les attaques.

Ce livre blanc aborde les signatures numériques et le chiffrement des e-mails sous l'angle de la nécessité, et compare dans cette perspective les atouts des certificats électroniques par rapport à d'autres solutions. Ce document présente également les avantages pour les organisations ainsi que les bonnes pratiques d'implémentation.

E-MAILS NON SÉCURISÉS : QUELS RISQUES ?

Si l'importance du chiffrement des e-mails était jusqu'ici largement sous-estimée, la médiatisation autour des dernières attaques commises contre des fournisseurs de services de messagerie a contribué à l'émergence d'une prise de conscience. Particuliers et entreprises doivent être informés des risques liés à l'utilisation d'Internet comme mécanisme de transport pour les e-mails – risques, pour la plupart, hors de leur contrôle. L'actualité regorge d'exemples de violations de bases de données d'identifiants utilisateur par des hackers malveillants, avec pour conséquence, une exposition des données hautement sensibles. Mais en exigeant une clé privée spécifique pour décrypter et lire les messages, le chiffrement des e-mails permet de résoudre ce problème.

LE PROTOCOLE S/MIME

La technologie S/MIME (*Secure/Multipurpose Internet Mail Extensions*) constitue la norme sectorielle pour le chiffrement par clé publique des données MIME. Si le chiffrement S/MIME assure l'intégrité et la confidentialité du message, l'ajout de signatures numériques permet d'attester de l'origine du message et de garantir sa non-répudiation. Suivie par l'Internet Engineering Task Force (IETF), la norme S/MIME est aujourd'hui définie par plusieurs RFC (*Requests for Comments*) dont les RFC 3851, 3850, 3370 et 3369. L'entité MIME à sécuriser est placée dans un message PKCS7 lors du chiffrement. En clair : les certificats numériques utilisent le protocole S/MIME.

POURQUOI LES CERTIFICATS NUMÉRIQUES ?

L'utilisation de certificats numériques pour sécuriser les e-mails garantit non seulement la confidentialité des données grâce au chiffrement, mais permet également de certifier l'origine et l'intégrité du message grâce à l'ajout de signatures numériques.

PREUVE DE L'ORIGINE DU MESSAGE ET NON-RÉPUDIATION

Un certificat numérique est un petit fichier de données qui associe numériquement une clé cryptographique à l'identité d'un utilisateur. Utilisés pour signer numériquement les messages électroniques, ces certificats offrent aux destinataires un gage de sécurité en attestant de l'origine des e-mails – une étape essentielle dans la prévention des attaques par hameçonnage (*phishing*).

INTÉGRITÉ

Les signatures numériques protègent également l'intégrité du contenu des e-mails à l'aide d'algorithmes de hachage uni-directionnel qui condensent et masquent les données. Le hachage d'un fichier consiste à

calculer une empreinte de taille limitée à partir des données de base (comme une chaîne de caractères, par exemple) ; cette empreinte fait alors partie de la signature numérique. Tant que les données originales du fichier ne sont pas modifiées, la valeur alphanumérique de l'empreinte (*hash*) reste la même et le destinataire peut vérifier que le fichier n'a pas été modifié au cours de l'envoi.

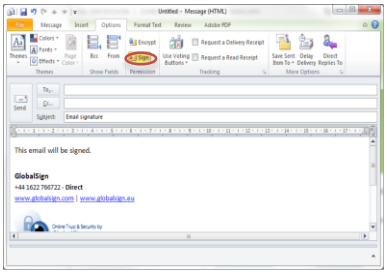
CONFIDENTIALITÉ

En dissimulant le contenu d'un message à l'aide d'un texte crypté, un message chiffré assure une défense proactive contre les violations de confidentialité. Dans l'infrastructure à clés publiques (PKI) d'une organisation, le chiffrement d'un message s'effectue à l'aide de la clé publique du destinataire. En clair, seul le détenteur de la clé privée correspondante (c'est-à-dire, le destinataire) est en mesure de déchiffrer le texte crypté pour en lire le contenu. Par conséquent, aucun utilisateur non autorisé ne peut accéder aux informations.

TRANSPARENCE POUR L'UTILISATEUR FINAL

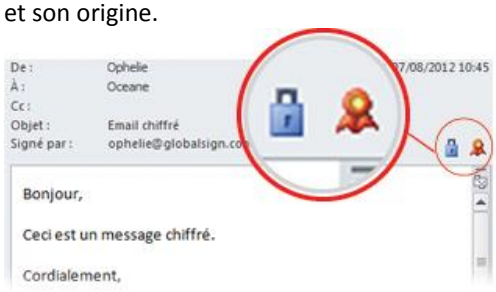
Les certificats numériques de signature /chiffrement d'e-mails émis par une autorité de certification indépendante et de confiance comme GlobalSign sont généralement simples à utiliser et transparents pour l'utilisateur final qui n'a pas besoin de maîtriser PKI dans toutes ses subtilités.

Une fois le certificat installé, l'utilisateur peut signer ou chiffrer ses e-mails en un seul clic. Cette option peut être paramétrée par défaut pour permettre la signature systématique des e-mails par le biais du certificat numérique, sans autre intervention de l'utilisateur.

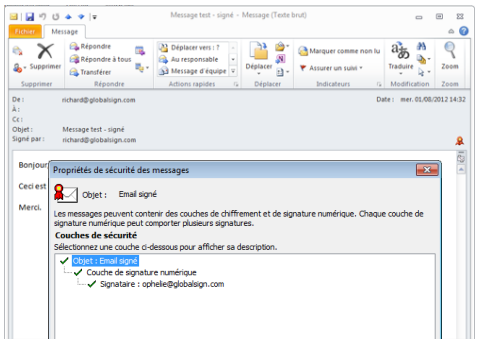


Signature d'un e-mail dans Microsoft Outlook 2010

Grâce aux pictogrammes intuitifs, le destinataire d'un e-mail peut facilement confirmer l'intégrité d'une signature d'e-mail et son origine.



E-mail signé et chiffré



Vérification de l'origine de l'e-mail

ALTERNATIVES À S/MIME

OpenPGP, l'implémentation la plus courante de PGP (*Pretty Good Privacy*), représente le principal rival de S/MIME. Contrairement à S/MIME, PGP n'utilise pas de certificats X.509 pour distribuer les clés publiques, mais une paire de clés générées par un plug-in ou une implémentation logicielle PGP stockée à l'aide d'un « porte-clés » PGP. Principal inconvénient de ce modèle : l'absence de vérification de la paire de clés PGP par une entité externe comme une autorité de certification. La distribution des clés ne peut donc pas s'appuyer sur le modèle de la « Toile de confiance » et les clés doivent être échangées manuellement avec d'autres utilisateurs. Pour des raisons évidentes, cela augmente les risques de compromission des clés. De plus, avec PGP, l'ajout de plug-ins ou de logiciels au client de messagerie peut, au final, faire grimper la note pour les déploiements en entreprise.

BONNES PRATIQUES

L'utilisation de certificats numériques implique le respect de quelques bonnes pratiques. Face à l'évolution permanente et la sophistication

croissante des méthodes de contournement employées, les certificats numériques et les méthodes de chiffrement à clés publiques doivent s'adapter. Aussi, pour soutenir la complexification des suites de cryptage et des algorithmes de chiffrement, les exigences minimums et les bonnes pratiques sont régulièrement réactualisées.

CHOISIR DES ALGORITHMES FORTS

L'évolution des algorithmes de hachage et de chiffrement s'est récemment accélérée, comme en atteste l'abandon du chiffrement Triple DES (3DES) et du hachage Message Digest (MD5), aujourd'hui supplantés par des algorithmes plus évolués : AES (*Advanced Encryption Standard*) 256 bits pour le chiffrement symétrique de données, RSA pour le chiffrement asymétrique et SHA1 (*Secure Hashing Algorithme*). La migration vers la version plus avancée SHA2 de ce dernier algorithme de hachage sécurisé est en cours, alors que la version SHA3 est en cours de ratification.

Lors du choix d'un algorithme de signature, on recherchera le meilleur compromis entre compatibilité universelle et hachage fort, sans oublier de consulter son AC afin de prendre connaissance des dernières recommandations (document en anglais).

Lors de l'utilisation d'un certificat numérique et d'une clé publique, il est également vivement recommandé d'effectuer une sauvegarde du certificat et de la clé publique. Les utilisateurs sous Windows pourront créer un fichier de sauvegarde protégé par mot de passe PKCS#12 (.pfx). Cette fonction est accessible dans le magasin de certificats Microsoft par le biais d'Internet Explorer ou de la Console MMC. La clé privée doit également pouvoir être exportée. Une fois la sauvegarde du certificat terminée, elle devra être enregistrée sur un périphérique amovible et conservée en lieu sûr.

CONCLUSION

Pour remplir leur mission de protection des organisations, de leurs données et de leurs clients, les directions des services informatiques doivent s'attaquer à de nombreux chantiers et se conformer, en prime, à une multitude de réglementations. Avec l'explosion du nombre de données transmises par voie électronique et transférées dans le Cloud, la sécurité des informations confidentielles est devenue un enjeu prioritaire.

Si l'ajout de signatures numériques aux e-mails renforce le niveau de confiance pour les parties concernées, le chiffrement assure quant à lui une protection nécessaire contre les menaces actuelles. Faciles à déployer, les certificats numériques S/MIME jouent un rôle clé dans le cadre d'une stratégie globale de sécurité des informations.

L'APPORT DE GLOBALSIGN ?

GlobalSign, l'un des leaders mondiaux des solutions de sécurité des informations, propose les outils et les compétences requises pour la mise en place de ces solutions. La plate-forme de gestion Web EPKI (Enterprise PKI) de GlobalSign simplifie la gestion des nombreux certificats numériques dans l'entreprise, tout au long de leur cycle de vie.

POURQUOI CHOISIR GLOBALSIGN ?

- Un historique d'innovations dans la sécurité et une réputation de confiance : Plus de 20 millions de certificats dans le monde s'appuient sur la confiance publique du certificat racine GlobalSign. L'entreprise exploite une infrastructure PKI de confiance depuis 1996 et est accréditée WebTrust depuis plus de 12 ans.
- L'engagement d'excellence de son support client : lorsque vous appelez GlobalSign, vous avez affaire à des interlocuteurs bien réels.
- Une présence mondiale : avec des services d'assistance technique aux quatre coins du globe, vous bénéficiez d'une réactivité supérieure et de solutions localisées en fonction de votre langue, de votre région et de votre pays.

INTERROGEZ-NOUS SUR NOS SOLUTIONS DE SÉCURISATION DES E-MAILS

Contactez vite GlobalSign, par téléphone ou par e-mail, pour discuter avec l'un de nos spécialistes de la mise en place d'une stratégie basée sur les bonnes pratiques et des outils nécessaires. Vous pouvez également consulter notre site : www.globalsign.fr/securisation-email/

À PROPOS DE GLOBALSIGN

GlobalSign est l'une des plus anciennes autorités de certification ; elle propose en effet des services d'accréditation numérique depuis 1996. Les équipes basées à Londres, Bruxelles, Boston, Tokyo et Shanghai assurent les services d'assistance commerciale et technique en plusieurs langues.

GlobalSign est soutenu depuis longtemps par de nombreux investisseurs comme ING Bank et Vodafone. L'entreprise est désormais intégrée à GMO Internet Inc., un groupe ouvert coté à la prestigieuse bourse de Tokyo (TSSE : 9449) qui compte parmi ses actionnaires les sociétés Yahoo! Japon, Morgan Stanley et Crédit Suisse First Boston.

Leader dans le domaine des services de confiance publics, les certificats GlobalSign ont la confiance des principaux navigateurs, systèmes d'exploitation, terminaux et applications. Ils incluent les services suivants : SSL, signature de code et de documents, sécurisation des e-mails et authentification, solutions numériques pour entreprises, gestion PKI interne et signature racine des services de certificats Microsoft. Les certificats racines de confiance de GlobalSign sont reconnus par tous les systèmes d'exploitation, par les principaux navigateurs, serveurs Web, clients de messagerie et applications Internet, ainsi que par tous les terminaux mobiles.

Niveau d'accréditation maximum

Accrédités WebTrust en qualité d'autorité de certification publique, nous proposons à des milliers d'entreprises des solutions pour mener en toute sécurité leurs transactions et transferts de données en ligne. Nos solutions leur permettent de diffuser du code inviolable et d'associer les identités à des certificats numériques pour le chiffrement S/MIME des e-mails et l'authentification à deux facteurs à distance, comme avec les VPN SSL.

GlobalSign France Tél. : +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	**GlobalSign Allemagne** Tél. : +49 800 7237980 www.globalsign.de verkauf@globalsign.com	**GlobalSign Pays-Bas** Tél. : +31 85 8882424 www.globalsign.nl verkoop@globalsign.com
GlobalSign Royaume-Uni Tél. : +44 1622 766766 www.globalsign.co.uk sales@globalsign.com	**GlobalSign Russie** Tél. : +7 (495) 972 46 33 www.globalsign.ru sales@globalsign.com	**GlobalSign Europe** Tél. : +32 16 89 19 00 www.globalsign.eu sales@globalsign.com