Communiqué de presse
Février 2013

tbs internet
fait de SHA2 une priorité pour 2013

SHA et le SSL
SHA – Secure Hash Algorithm – est un algorithme de hashage utilisé par les autorités de certification pour signer certificats et CRL (liste de révocation de certificats). SHA1 est aujourd'hui l'algorithme de hashage le plus couramment utilisé. Pour amorcer le passage vers un algorithme de hashage plus performant, TBS INTERNET lance une toute nouvelle gamme de certificats SSL signés en SHA2.

SHA2, une priorité qui ne date pas d'hier
En 2008 TBS INTERNET était la première autorité de certification à proposer des certificat SSL signés en SHA256. Il s'agissait alors de produits mono-sites issus de notre propre gamme TBS X509. Début 2013, nous élargissons cette gamme à d'autres marques et types de certificats.

Du certificat wildcard au certificat client en passant par des produits multi-site ou Extended Validation, notre gamme est aujourd'hui à même de répondre à tous les types de besoins. Mi-2013 cette dernière sera encore élargie pour accueillir de nouvelles marques et inciter, nous l'espérons, les utilisateurs à se tourner définitivement vers les produits actuellement les plus sûrs du marché.

Fonctionnement
Chaque certificat embarque un certain nombre d'informations : durée de validité, clé publique, propriétaire...

L'ensemble de ces informations est hashé. Le produit de ce hash est appelé condensat. Ce dernier assure l'intégrité des informations contenues dans le certificat. En clair, si ces informations sont modifiées le condensat résultant sera différent.

Dans l'exemple ci-dessous, deux variantes d'un même message hashé d'abord en SHA1 puis en SHA2 :

Contact : J.P. DONNIO – tbs internet – +33 2 7630 5900

Voici un message hashé (SHA1)
b6877fdc70dea41c4bbd733e2048c4dde8ec6d28

voici un message hashé (SHA1)
15076536074c02db9bb07300f1bab3bc316824a5
On enlève la majuscule au mot « voici » et le hash produit est complètement différent

Voici un message hashé (SHA256)
aeb36d756d7f8340ce9178575aa7f665c5c899384da0d35533a75067db6d1cec

Voici un message hashé (SHA256)
ae05f090ed14ae2bc262723fdb743fc0db17517cf322110dd9397ac9341fee68

La force de SHA

- Chaque condensat est unique : ajoutez une virgule au message initial, le condensat produit sera différent.
- La fonction n'est pas réversible. Il n'est pas possible de déterminer le contenu d'un message à partir de son condensat.

Des origines de SHA

SHA est créé en 1993 par la NSA avec SHA0. Il est rapidement suivi par SHA1 puis par SHA2 en 2002 et enfin SHA3 en 2012. SHA0, SHA1 et SHA2 sont relativement similaires et même si leurs structures divergent ils sont conçus sur le même modèle de base. SHA3 est lui, complètement différent et utilise un algorithme complètement nouveau. Il est issu d'un concours lancé par la NSA et invitant les cryptographes du monde entier à proposer leur version de SHA.

À propos de la NSA : La National Security Agency est une agence gouvernementale américaine dont l'une des mission est, entre autres, d'assurer la sécurité des communications de son gouvernement.

Quelles sont les menaces auxquelles s'expose SHA et pourquoi migrer vers SHA2 ?

Comme toute technologie en lien avec la sécurisation de données sensible, SHA est la proie des hackeurs, toujours plus performants, cherchant à s'approprier des informations confidentielles. Il existe 2 types d'attaques spécifiques à SHA :

- La collision : une collision se produit lorsque 2 fichiers différents produisent le même condensat. Dans ce cas il est alors possible de substituer un fichier par un autre. Dans notre secteur on pourrait dès lors imaginer remplacer un certificat officiel par un autre produisant les même valeurs de hash. SHA0 est vulnérable à la collision, c'est la raison pour laquelle il n'est plus utilisé aujourd'hui.

- La pré-image : Il faut distinguer la pré-image et la pré-image secondaire. La première consiste à déterminer la valeur d'un fichier à partir de son condensat. La seconde à utiliser un condensat pour produire une valeur différente de celle à l'origine du hash.

Bien qu'aucune collision complète n'ai abouti avec SHA1, l'évolution des capacités de calculs rendra bientôt la chose possible. SHA2 est quant à lui totalement hermétique à la collision et le restera au moins une dizaine d'années.

À noter : Le référentiel général de sécurité (RGS), qui pose les principes régissant la sécurisation des systèmes d'information des autorités administratives françaises, impose SHA256 aux certificats RGS. Cette norme deviendra obligatoire à partir de mai 2013.

La compatibilité des certificats SHA256

Les certificats SHA256 sont chainés aux même racines que leurs homologues signés en SHA1. Leur reconnaissance par les navigateurs dépend de la capacité de ces derniers à supporter un tel niveau de hashage. Lancé en 2002, SHA2 a, depuis, largement été déployé. Il existe néanmoins encore quelques vieux navigateurs ou machines non compatibles.

TBS INTERNET propose des outils de test en ligne permettant de vérifier la compatibilité de votre navigateur avec ce type de produits. Nous éditons également une liste des produits compatibles et une liste de correctifs pour les systèmes non nativement compatibles.

Enfin, plusieurs certificats de test (valide 30 jours) sont disponibles. Ils permettent de mieux préparer un passage vers une version SHA2 des produits de sécurité qu'il s'agisse de certificat serveur ou client.

Les certificats SHA256 proposés par TBS INTERNET

TBS INTERNET est le premier courtier en certificats SSL à proposer des certificats SSL SHA256 de tout type. Découvrez une gamme complète et inédite de certificats serveur et client !

Certificats SSL serveur :

- X509 SHA256 TBS
- X509 Omnidomaine SHA256 TBS
- X509 Multi-Sites SHA256 TBS
- Comodo EV SHA256
- Certigna SSL RGS*

Certificats client :

- X509 Sign & Login SHA256 TBS
- X509 Email Professionnel SHA256 TBS
- Chambersign Audacio RGS**

Certificats de test :

- X509 Test SHA256 TBS
- X509 Test Sign & Login SHA256 TBS

Créer la confiance en ligne

La confiance est essentielle en ligne, c'est pour cette raison que la sécurité est au cœur des préoccupations des éditeurs de sites web. La technologie SSL est un sujet largement abordé notamment dans les nombreux salons spécialisés (Forum Cybercriminalité, TechDays, Salon des Entrepreneurs...).

http://www.tbs-internet.com
http://www.tbs-certificats.com

A propos du courtier tbs internet

TBS INTERNET est une SSII spécialisée pour les Fournisseurs de Services Internet depuis 1996 basée à Caen. Avec une forte compétence en sécurisation des transactions électroniques par certificats, TBS INTERNET est le premier courtier en certificats en France. Depuis plus de 15 ans, nous apportons aux entrepreneurs de l'Internet notre savoir faire en matière de SSL.
Partenaire de Symantec – Thawte – Geotrust – Comodo – ChamberSign – GlobalSign et Certigna, TBS INTERNET propose également sa marque dédiée : TBS X509.
TBS INTERNET est membre du Pôle de compétitivité TES – Transactions Électroniques Sécurisées.