Communiqué de presse
16 janvier 2009

tbs internet

Lance le certificat SSL à signature forte SHA256

TBS X509 est la **première grande autorité de certification** à proposer des certificats SSL serveur nouvelle génération, utilisant l'algorithme de signature **SHA256**. Il remplacera les algorithmes existants tels MD5 et SHA1.

L'algorithme de condensé au coeur du certificat

Les procédés de signature électronique s'appuient sur une méthode mathématique pour condenser le message à signer. Ce condensé doit être inviolable et unique pour que l'on ne puisse substituer un message signé par un autre. Avec les progrès des CPU, il est nécessaire de remplacer périodiquement ces méthodes.
Dans les années 90, l'algorithme MD5 était utilisé pour ce faire (avant d'être remplacé par SHA1, le standard actuel). Le 30 décembre dernier, un groupe de chercheurs a démontré que dans des conditions très particulières, ils avaient réussi à falsifier un certificat en exploitant une faille de MD5.

SHA256 est le futur standard : il est plus sûr que les algorithmes précédents et permettra donc de maintenir les signatures inviolables pendant une quinzaine d'années au moins.

Le certificat TBS X509 SHA256 est le plus sûr du marché

Lancé quelques jours avant l'annonce relative au MD5, le certificat TBS X509 SHA256 innove en utilisant le niveau de signature le plus fort du marché ! Il fonctionne avec les navigateurs récents également compatibles tels Internet Explorer 7 (sous Vista ou XP SP3), Firefox 2 ou 3, Safari, etc.

Outre l'algorithme SHA256, le certificat TBS X509 SHA256 dispose également du forçage à 128-bit Microsoft SGC et d'un **audit de délivrance avancé** de type 3-facteur.

Afin de faciliter le déploiement, tbs internet propose un site de test pour évaluer les navigateurs (http://sha256.tbs-internet.com/) et un certificat de test valide 30 jours.

Depuis son lancement en janvier 2006, l'autorité de certification TBS X509 a trouvé son marché et dispose d'une gamme complète de certificats serveur (standard, SGC, wildcard, SAN) et utilisateur (email professionnel, authentification forte, signature).

A propos de 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.
Partenaire de VeriSign – Thawte – Geotrust – Comodo – Chambersign, tbs internet commercialise les certificats de ces marques, et est **autorité de certification** sous sa marque « TBS X509 ».
tbs internet est membre du Pôle de Compétitivité Transactions Electroniques Sécurisées.

Contact : Jean-Philippe DONNIO – tbs internet – 02 31 76 30 59 00