

Les algorithmes ECC sont les plus rapides et les plus robustes.

Info

Posté par : JPilo

Publié le : 19/2/2013 11:00:00

Symantec a annoncé de nouvelles mises à jour de son portefeuille de solutions de sécurité pour les sites Web (WSS) avec des fonctionnalités innovantes et complètes répondant aux besoins croissants des entreprises connectées en matière de sécurité et de performance.

La stratégie WSS de Symantec met l'accent sur la protection des entreprises, le respect des réglementations, l'amélioration des performances et la réduction des coûts d'infrastructure. L'objectif est de garantir aux entreprises et à leurs clients la fiabilité des achats, de la publicité et des applications. Symantec a également annoncé la disponibilité des premiers certificats SSL utilisant plusieurs algorithmes avec les nouvelles options ECC et DSA.

Ces offres permettront aux entreprises de protéger leur écosystème Web et de renforcer la confiance en ligne.



Pour conserver une longueur d'avance sur les nouvelles menaces en ligne sophistiquées, le NIST (Institut national américain des normes et technologies) recommande à tous les sites Web de passer des clés RSA 1024 bits aux certificats RSA 2048 bits d'ici le 1er janvier 2014. Symantec a commencé à faire évoluer ses clients vers les certificats SSL RSA 2048 bits l'année dernière. Dans le cadre de l'annonce faite ce jour, la société enrichit son portefeuille de certificats SSL avec de nouveaux algorithmes de sécurité pour renforcer la protection et garantir de meilleures performances.

Algorithmes ECC plus rapides et plus robustes

Symantec est la première autorité de certification à commercialiser des certificats SSL utilisant les algorithmes ECC (Elliptic Curve Cryptography) et DSA (Digital Signature Algorithm).

Les algorithmes ECC sont les plus rapides et les plus robustes.

<https://www.info-utiles.fr/modules/news/article.php?storyid=18341>

L'algorithme ECC sera disponible au sein de la solution Symantec Managed PKI for SSL dans le courant du premier semestre 2013. Suite à des tests internes, l'algorithme ECC avancé offre les avantages suivants :

â€¢ **Sécurité renforcée**, Symantec ECC est 10 000 fois plus fiable qu'une clé RSA 2048 bits reposant sur des méthodes de calcul industrielles. Les certificats ECC 256 bits de Symantec offrent une sécurité équivalente à un certificat RSA 3072 bits ;

â€¢ **Amélioration des performances des serveurs** pendant les pics de charge et capacité à traiter un plus grand nombre de demandes par seconde en réduisant l'utilisation du processeur, ce qui est de plus en plus important, car l'adoption des terminaux mobiles et des tablettes alourdit la charge de travail de l'infrastructure Web ;

â€¢ **Amélioration des performances** et du temps de réponse du serveur vers le poste de travail. Des tests internes ont montré qu'un serveur équipé d'un certificat RSA traitait 450 demandes par seconde, avec un temps de réponse moyen de 150 millisecondes. Dans les mêmes conditions, le serveur équipé d'un certificat ECC offrait un temps de réponse moyen de seulement 75 millisecondes.

[Plus d'info.](#)