life.augmented

Press release

P3859S

ST renforce la sécurité informatique avec sa dernière génération de modules sécurisés

- *ST étend son offre STSAFE avec l'introduction de nouveaux modules Hardware TPM afin d'améliorer la sécurité on-line*
- *La plus importante mémoire embarquée du marché augmente la capacité disponible pour le stockage de données sensibles dans le TPM*
- *Les produits sont certifiés selon les normes de sécurité les plus élevées actuellement en vigueur et agréés par une autorité de certification indépendante*

Genève, le 23 novembre 2016 - STMicroelectronics (NYSE : STM), un leader mondial dont les clients couvrent toute la gamme des applications électroniques et membre actif du Trusted Computing Group (TCG) depuis plus d'une décennie, annonce la disponibilité de deux modules de sécurité de hautes performances qui assurent aux ordinateurs et aux périphériques connectés intelligents une protection agréée au niveau industriel contre les cyber-attaques.

Les nouveaux modules TPM (Trusted Platform Modules) de la famille STSAFE stockent des données d'authentification système — clés de chiffrement ou mesures logicielles — sur des supports matériels inaccessibles et inaltérables, offrant ainsi une solution standardisée au niveau industriel pour protéger les PC et les serveurs, mais également les équipements de bureau et à usage domestique (imprimantes, copieurs, passerelles domestiques, routeurs réseau et commutateurs). Cette protection du stockage empêche les agresseurs d'interférer avec l'intégrité des périphériques, de voler des données privées ou de prendre le contrôle du système afin d'y accéder de manière non autorisée ou d'obtenir des privilèges susceptibles de mettre le système, ses données ou son réseau en danger.

« *Un haut niveau de sécurité est essentiel pour faire pleinement confiance au nombre croissant de produits intelligents connectés qui accompagnent nos activités personnelles et professionnelles* », a déclaré Marie-France Florentin, Directrice générale de la division Microcontrôleurs Sécurisés de STMicroelectronics. « *Nos modules de sécurité de hautes performances allient la technologie informatique de confiance la plus récente à des fonctionnalités à valeur ajoutée qui assurent aux utilisateurs finaux un haut niveau de protection, de confidentialité et de sécurité*. »

La toute dernière spécification du Trusted Computing Group, TPM 2.0, ajoute des fonctionnalités supplémentaires à la version précédente (TPM 1.2[1]), parmi lesquelles des algorithmes cryptographiques et la prise en charge de la hiérarchie des utilisateurs. Annoncé sous la référence ST33TPHF2ESPI, le premier des deux nouveaux modules STSAFE-TPM

[1] Les spécifications TPM 1.2 et TPM 2.0 sont toutes deux agréées en tant que normes internationales par l'Organisation internationale de normalisation (ISO) et la Commission Électrotechnique Internationale CEI).

de ST prend en charge les deux spécifications et peut facilement basculer de l'une à l'autre, permettant aux équipementiers d'intégrer le niveau TPM 1.2 ou TPM 2.0 dans leurs produits. Le deuxième module, ST33TPHF20SPI, prend en charge la spécification TPM 2.0 et dispose de la plus importante mémoire non volatile du marché, à savoir jusqu'à 110 ko de stockage pour les données sensibles.

Les modules STSAFE-TPM s'appuient sur l'expertise développée par ST pour le processeur sécurisé ARM® SecurCore® SC300™ qui dispose de fonctions d'anti-falsification, de surveillance des données et de protection de la mémoire. Ces deux modules sont certifiés selon les Critères Communs (CC) et conformes aux protocoles du Trusted Computing Group (TCG) par rapport aux profils de protection TPM 1.2 et 2.0 ; leur certification FIPS[2] 140-2 est en cours. Les nouveaux modules sont livrés avec les clés Endorsement Keys[3] (EK) RSA et ECC[4] nécessaires pour exécuter les tâches d'authentification ; les certificats de clés correspondants sont fournis, et leur authenticité est garantie par la signature de l'autorité de certification indépendante Globalsign Ltd.

Les modules ST33HTPH2ESPI et ST33HTPH20SPI sont en production actuellement et disponibles en boîtier TSSOP28 ou QFN32. Pour toute demande de tarifs et d'échantillons, contactez votre bureau de vente ST.

STSAFE est une famille de produits d'authentification offrant des solutions clés en main. Tous les produits STSAFE sont architecturés autour de microcontrôleurs hautement sécurisés et certifiés par des laboratoires indépendants conformément aux Critères Communs EAL5+, la norme de sécurité actuellement la plus élevée. La famille de produits STSAFE est conçue pour offrir des solutions personnalisées qui répondent aux défis de sécurité croissants auxquels sont confrontés les secteurs de l'informatique de confiance, de la protection des marques et de l'Internet des objets.

À propos de STMicroelectronics
ST, un leader mondial sur le marché des semiconducteurs, fournit des produits et des solutions intelligents qui consomment peu d'énergie et sont au cœur de l'électronique que chacun utilise au quotidien. Les produits de ST sont présents partout, et avec nos clients, nous contribuons à rendre la conduite automobile, les usines, les villes et les habitations plus intelligentes et à développer les nouvelles générations d'appareils mobiles et de l'Internet des objets. Par l'utilisation croissante de la technologie qui permet de mieux profiter de la vie, ST est synonyme de « life.augmented ».

En 2015, ST a réalisé un chiffre d'affaires net de 6,90 milliards de dollars auprès de plus 100 000 clients à travers le monde. Des informations complémentaires sont disponibles sur le site : www.st.com.

---

[2] FIPS : Federal Information Processing Standard

[3] Endorsement Key : une paire de clés à codage cryptographique utilisée pour autoriser des transactions et identifier les écarts par rapport à une configuration d'équipement connue

[4] RSA et ECC : algorithmes cryptographiques pris en charge par les spécifications TPM 1.2 (RSA) et 2.0 (RSA et ECC)

Contacts presse :
Nelly Dimey
Tél : 01.58.07.77.85
Mobile : 06. 75.00.73.39
nelly.dimey@st.com

Alexis Breton
Tél : 01.58.07.78.62
Mobile : 06.59.16.79.08
alexis.breton@st.com