life.augmented

Press release

P3833S

STMicroelectronics simplifie l'intégration de la sécurité pour l'Internet des objets

- *Le nouvel élément de sécurité optimisé STSAFE-A100 intègre des fonctions d'authentification, de communications sécurisées et de gestion de clés de chiffrement tout en étant conforme aux standards de sécurité les plus élevés pour les objets connectés (Critères communs EAL5+)*

- *Cet élément de sécurité aide les concepteurs d'équipements à relever les défis d'intégration en mettant à leur disposition un écosystème complet*

Genève, le 14 juin 2016 - STMicroelectronics (NYSE: STM), un leader mondial dont les clients couvrent toute la gamme des applications électroniques, annonce un élément de sécurité à la fois robuste et d'utilisation aisée. Conçu pour protéger les appareils connectés à l'Internet des objets (IoT) aux niveaux industriel et grand public, le STSAFE-A100 empêche également le clonage et la copie de produits en garantissant leur authenticité.

Certifié conforme aux normes de sécurité les plus strictes, l'élément de sécurité STSAFE-A100 peut être utilisé par des développeurs qui ne disposent pas d'une expertise particulière en matière de sécurité, grâce à un écosystème de support complet.

De nombreux produits grand public, appareils domestiques, actifs industriels et capteurs sont déjà connectés à l'Internet, ou le seront bientôt. La plupart d'entre eux sont conçus pour fonctionner de façon autonome et sans surveillance et à ce titre, doivent bénéficier d'une sécurité électronique de pointe afin d'empêcher les *hackers* de procéder à toute tentative de contrefaçon, de clonage, de vol d'informations ou d'utilisation abusive. Le STSAFE-A100 de ST est une solution clé en main sécurisée qui met à la disposition de l'Internet des objets l'expertise éprouvée acquise par la Société dans les domaines de la sécurité électronique pour des applications telles que les services bancaires, le commerce électronique ou la protection des identités. En tant qu'élément de sécurité fournissant des services d'authentification et pouvant être associé à un microcontrôleur classique, le STSAFE-A100 intègre son propre système d'exploitation sécurisé et est certifié conforme aux Critères Communs EAL5+[1], la norme de sécurité appliquée par l'industrie bancaire.

« *Le STSAFE-A100 est une solution hautement sécurisée, économique et certifiée pour protéger les objets de marque et l'Internet des objets. Par rapport aux approches existantes telles que la sécurité à base de logiciels déployée sur des microcontrôleurs polyvalents ou dans des éléments de sécurité non-certifiés, cette alternative présente des avantages évidents* », a déclaré Laurent Degauque, directeur du marketing, Division Secure Microcontrollers, Groupe MDG, STMicroelectronics. « *L'intégration aisée facilite la mise en*

[1] CC EAL5+: évaluation selon les Critères Communs Niveau 5+.

place de la sécurité au cœur du produit, et permet aux développeurs de se concentrer pleinement sur la valeur ajoutée qu'ils apportent à l'application. »

Pour faciliter l'intégration de son nouvel élément de sécurité, ST met à la disposition de ses clients un écosystème complet composé d'une carte d'extension avec un brochage Arduino, d'une librairie logicielle pour microcontrôleurs et de codes d'implémentation de référence. Ces outils simplifient la connexion de l'élément de sécurité STSAFE-A100 à des microcontrôleurs appartenant, par exemple, à la famille STM32.

L'élément de sécurité STSAFE-A100 est prévu pour être fabriqué en volume en juillet 2016 et disponible en boîtiers SO8N (4 x 5 mm) et UFDFPN8 (2x 3 mm). Veuillez contacter le bureau de vente de ST pour toute demande de tarifs et d'échantillons.

Informations complémentaires techniques :
L'élément de sécurité STSAFE-A100 dispose de fonctions d'authentification forte grâce auxquelles, seuls les appareils IoT autorisés peuvent accéder à des services en ligne et, seuls les accessoires ou consommables autorisés sont reconnus et acceptés par une application. Il est compatible avec le protocole d'authentification de périphériques USB Type C™ et sécurise les communications avec un hôte distant utilisant le protocole d'établissement de connexions TLS (Transport Layer Security).

Plusieurs fonctions supplémentaires permettent de réduire les risques de faille de sécurité, parmi lesquelles la vérification de signature pour sécuriser le *boo*t et la mise à jour des *firmware*, des compteurs sécurisés qui contrôlent l'utilisation de consommables, l'appairage sécurisé au processeur d'application hôte, le chiffrement et le déchiffrement de données pour un hôte local ou distant, ainsi que la génération de paires de clés de chiffrement.

L'élément de sécurité STSAFE-A100 prend en charge les technologies de chiffrement asymétrique telles que le chiffrement par courbe elliptique (*Elliptic Curve Cryptography*-ECC) NIST[2] ou Brainpool sur 256 et 384 bits, ainsi que le chiffrement symétrique utilisant des clés AES-128/AES-256. Le STSAFE-A100 est livré avec un numéro de série propre à chaque circuit ; son système d'exploitation comprend un noyau pour l'authentification et la gestion des données, et assure une protection forte contre les attaques physiques, logiques, par faute ou par canal caché.

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] NIST: US National Institute for Standards and Technology

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