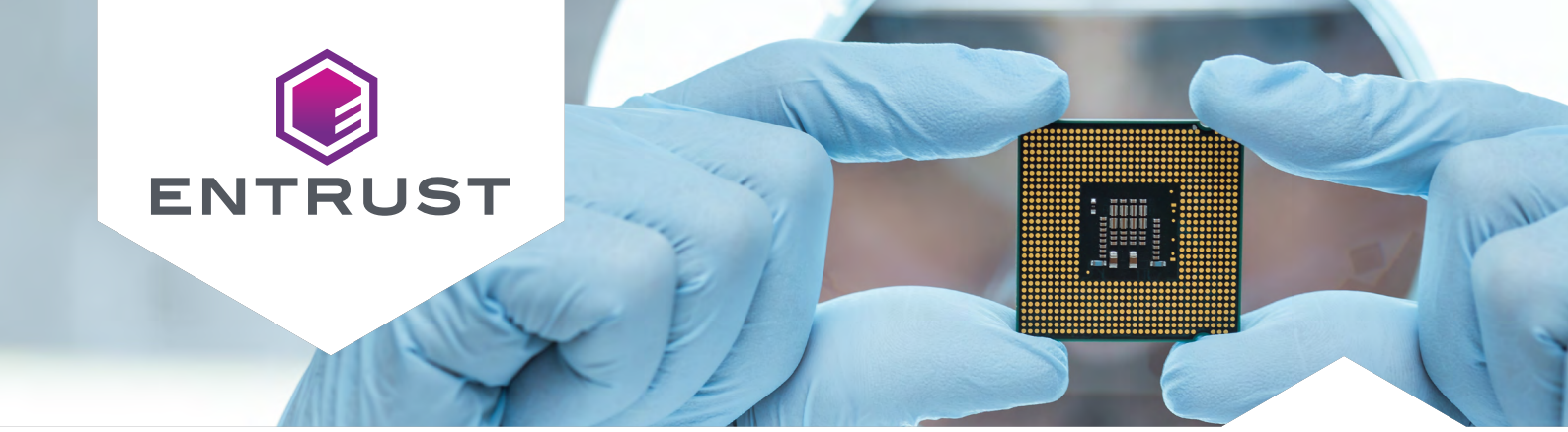

Entrust établit la racine de confiance des micrcontroleurs SAM L11 de Microchip, conçus pour l´IoT.

L'Internet des objets (IoT) est un phénomène désormais incontournable. Alors que beaucoup considèrent cela comme une estimation très prudente, IDC prévoit que le nombre total d'appareils IoT connectés dépassera les 40 milliards d'ici 2025.

Pourtant, la prolifération galopante du nombre de terminaux liés à l'IoT, allant des véhicules autonomes aux appareils électroménagers intelligents en passant par les équipements de santé et les machines agricoles, n'est pas sans poser de problèmes. La question de la sécurité est essentielle car il faut s'assurer que chaque appareil soit protégé de toute menace.

BESOIN OPÉRATIONNEL

Anand Rangarajan, responsable marketing produit chez Microchip Technology, précise : « Le monde de l'IoT ne dispose actuellement d'aucune norme de sécurité universelle. La complexité intrinsèque de l'intégration de mesures de sécurité appropriées au sein de leurs produits décourage de nombreux fabricants. »

> **« L'intégration d'une sécurité de qualité industrielle dans un système embarqué constitue une véritable révolution pour l'ensemble du marché de l'IoT. »**
>
> – Anand Rangarajan, responsable marketing produit chez Microchip Technology

DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

Microchip

Réputée pour sa capacité d'innovation permanente et ses produits novateurs, Microchip Technology Inc. est l'un des principaux fournisseurs au monde de solutions de microcontrôleurs, de circuits intégrés à signaux mixtes, de circuits analogiques et de circuits flash IP. L'un des tout derniers microcontrôleurs de la société, le SAM L11, a reçu le prix de l'innovation 2018 pour la meilleure contribution à la sécurité de l'IoT lors du salon ARM Techcon. Ce microcontrôleur a été conçu précisément pour répondre aux besoins en matière de caractéristiques, de fonctionnalités et de sécurité des nœuds IoT et des terminaux intelligents, tels que les appareils médicaux, les capteurs, les caméras et les voitures.

Basée à Chandler en Arizona, Microchip est cotée à la bourse du Nasdaq. La société a déjà fourni des milliards de microcontrôleurs et de microprocesseurs à des centaines de milliers de clients à travers le monde.

BESOIN TECHNOLOGIQUE

« Du point de vue technique, nous prévoyons que le SAM L11 sera utilisé dans des cas très particuliers, par exemple lorsqu'il s'agit d'obtenir des performances élevées pour une faible consommation d'énergie, » explique Rangarajan.

SOLUTION

Au cœur de l'architecture de sécurité du SAM L11 se trouve une fonction de racine de confiance créée par Microchip pour rendre possible l'insertion d'une clé unique dans l'appareil lors de sa fabrication. Le choix de la technologie pour gérer et exécuter cette tâche essentielle s'est avéré très simple. « Le choix des modules matériel de sécurité (HSM) pour générer les clés individuelles a été facile à faire puisque nous utilisions déjà depuis longtemps les produits de Entrust (auparavant nCipher), » indique Rangarajan.

Les HSM nShield® de Entrust sont des appareils de sécurité certifiés permettant de réaliser des opérations essentielles de chiffrement, de signature numérique et de génération de clés. Ces appareils renforcés en réseau sont très évolutifs et reposent sur une architecture flexible unique en son genre qui peut traiter des volumes considérables d'opérations de chiffrement.

RÉSULTATS

« L'insertion d'une clé unique à partir d'un HSM nShield dans chaque microcontrôleur SAM L11 permet de pouvoir identifier, vérifier et gérer les appareils à distance de façon individuelle. Cela se révèle particulièrement important lorsque la fiabilité doit être rétablie entre les dispositifs IoT et les autres terminaux connectés, » remarque Rangarajan. « Les fabricants peuvent désormais tirer pleinement parti du cloud pour établir une connectivité sécurisée et complète entre chaque nœud. C'est particulièrement utile lorsque l'on veut sécuriser des capteurs sans fil, chiffrer des données provenant d'appareils médicaux portables ou même authentifier à distance des systèmes connectés au cloud. »

Une partie du microcontrôleur SAM L11 de Microchip est le fruit de son partenariat avec Trustonic, leader sur le marché de la sécurité des appareils avec plus de 1,5 milliard d'unités protégées déployées dans le monde.

La création par Trustonic d'une bibliothèque de fonctions de sécurité comprenant l'authentification, le démarrage sécurisé, la détection des modifications, le chiffrement AES et SHA, et le stockage sécurisé des clés, lesquelles sont intégrées dans un kit de développement logiciel, constitue l'une de ses principales innovations.

Microchip

> **Le choix d'utiliser les HSM nShield de Entrust pour générer les clés individuelles était évident pour nous.**
>
> – Anand Rangarajan, responsable marketing produit chez Microchip Technology

« Les développeurs peuvent désormais utiliser cette structure de sécurité modulaire pour effectuer des appels d'API simples afin d'accéder à l'ensemble très élaboré de fonctionnalités de sécurité que nous avons mis au point, » commente Rangarajan. « Il n'est plus nécessaire de disposer d'une expertise approfondie des protocoles utilisés au niveau des puces. Cela permet de raccourcir considérablement le temps de développement et de réduire de façon significative les dépenses relatives à la sécurisation d'un appareil IoT. »

La bibliothèque de fonctions de sécurité est construite au-dessus de Kinibi-M, un environnement d'exploitation modulaire et sécurisé conçu par Trustonic pour les puces IoT de taille réduite. Une couche d'abstraction matérielle sous Kinibi-M facilite la communication directe avec le SAM L11, et permet notamment de gérer l'utilisation des clés de chiffrement générées par les HSM nShield de Entrust.

« Les développeurs du SAM L11 chez Microchip avait déjà déterminés que les HSM nShield de Entrust était le choix idéal pour nous, mais de manière tout à fait autonome, Trustonic a aussi recommandé l'utilisation des HSM de Entrust. C'était très gratifiant de voir notre choix validé de manière totalement indépendante, » se rappelle Rangarajan.

UNE PUCE INNOVANTE QUI SIMPLIFIE LA SÉCURITÉ

Le SAM L11 est le premier microcontrôleur du marché à utiliser le processeur Arm Cortex-M23 et la technologie de sécurité intégrée Arm TrustZone qui assure une isolation matérielle renforcée entre les ressources fiables et non fiables. Rangarajan précise : « Malgré la complexité et les nombreuses fonctionnalités de l'architecture de sécurité, l'utilisation de Kinibi-M simplifie encore le développement d'applications sécurisées grâce à un microprogramme entièrement intégré aux fonctions de sécurité de SAM L11, et constitue ainsi un précédent dont l'exemple d'un appareil tel que le SAM L11 pourrait s'avérer utile. »

La capacité de fournir aux développeurs d'appareils IoT une racine de confiance de classe mondiale grâce à l'utilisation de clés générées par un HSM nShield® de Entrust a un impact international significatif. Rangarajan conclut « L'approche que nous avons adoptée nous permet désormais d'intégrer des fonctions de sécurité à un ensemble performant qui consomme très peu d'énergie. L'intégration d'une sécurité de qualité industrielle dans un système embarqué constitue une véritable révolution pour l'ensemble du marché de l'IoT. »

Microchip

RENFORCER LA SÉCURITÉ DE L'IoT

Besoin opérationnel

- Mettre au point une solution permettant de sécuriser les nœuds et les terminaux de l'IoT
- Diminuer la complexité et le coût de l'intégration de systèmes de sécurité au sein des appareils IoT
- Éviter le recours à des techniques de programmation pointues au niveau de la puce

Besoin technologique

- Intégrer des fonctions de sécurité performantes au sein d'un microcontrôleur rapide et à faible consommation d'énergie
- Concevoir une petite empreinte permettant une utilisation avec des applications qui utilisent beaucoup de mémoire
- Établir la racine de confiance

Solution

- Les HSM nShield de Entrust

Résultat

- Lancement du microcontrôleur SAM L11 avec des caractéristiques et des performances de pointe
- Le kit de développement logiciel permet un accès simple aux API pour des fonctions de sécurité sophistiquées
- Réduction des délais de mise sur le marché pour les fabricants de appareils IoT
- Établit la racine de confiance pour les appareils IoT et les données qu'ils génèrent

À PROPOS DE ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre gamme unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com