# Des éléments sécurisés matériels préconfigurés en usine pour des réseaux IoT protégés

Grâce aux derniers développements en matière d'outils en ligne et de composants matériels pour la sécurité, les entreprises avec un projet, de quelque taille que ce soit, peuvent dorénavant mettre en œuvre un élément sécurisé avec leurs appareils IoT. Les obstacles qui existaient ont été levés et il existe une chaîne d'approvisionnement de la sécurité facile d'accès, qui permet d'étendre les bonnes pratiques des modèles de sécurité à l'ensemble de l'écosystème de l'Internet des objets.

AUTEUR

Xavier Bignalet, responsable du marketing produit au sein du département Secure Product Group chez Microchip Technology.

Les menaces de cybersécurité ont pris beaucoup d'ampleur sur tous les segments de marché depuis l'avènement de l'Internet des objets (IoT). Chaque appareil connecté au réseau y introduit un nouveau point d'attaque, non seulement sur les appareils eux-mêmes, mais également sur les systèmes, à la fois localement et dans le nuage, utilisés pour leur gestion.

Les attaques peuvent avoir de graves conséquences. En effet, toute intrusion réussie dans un objet connecté donne la possibilité d'y télécharger un nouveau firmware à des fins malveillantes. Bien que certaines attaques se contentent d'interrompre le fonctionnement de l'appareil pour pouvoir l'utiliser autrement, par exemple comme nœud dans un réseau de machines (botnet) utilisé pour réaliser une attaque par déni de service, d'autres attaques peuvent utiliser les systèmes visés pour pénétrer le réseau d'un opérateur.

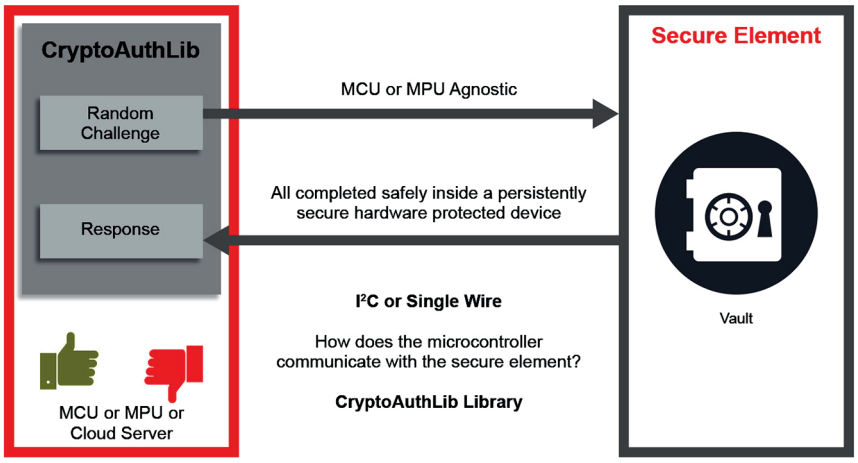
L'intrusion est facilitée par l'utilisation d'autorisations logicielles telles que des mots de passe. A l'aide de ces autorisations, un hacker qui réussit à pénétrer un appareil sera à même d'utiliser ces informations pour accéder à des services distants et, peut-être, mener plus facilement des attaques contre ces derniers. La sécurité appliquée par le matériel, associée à des identifiants sécurisés, offre un mécanisme qui permet de prévenir l'exploitation des appareils et de rendre le succès des premières attaques beaucoup moins probable. Grâce à la sécurité appliquée par le matériel, les codes d'accès et l'identité valide ne peuvent être créés qu'en usine en utilisant les mécanismes d'une infrastructure de gestion de clés publiques PKI (Public Key Infrastructure). Grâce à la PKI, chaque appareil possède une clé privée unique reliée mathématiquement à un certificat numérique connu comme valide, qui est conservé en sécurité par le fabricant. Cette clé privée est utilisée pour signer un certificat afin d'identifier l'appareil de façon unique sur n'importe quel serveur ayant accès à la clé publique correspondante. La clé publique est un ensemble d'informations visible publiquement et ne représente donc pas de risque si ladite clé est divulguée à des utilisateurs non autorisés. Dans le contexte d'un objet connecté, l'identité de l'appareil est prouvée grâce à son utilisation d'une clé privée. La clé publique associée est utilisée dans les protocoles qui déterminent si l'identité revendiquée est valide. Cette identité peut être utilisée pendant tout le cycle de vie de l'appareil pour authentifier les éventuelles mises à jour de firmware ainsi que l'identité de l'appareil quand il accède à des services distants.

## Protéger les clés de chiffrement privées

Etant donné leur rôle central dans les systèmes de chiffrement, les clés privées des appareils ne doivent être vulnérables ni aux attaques physiques ni à toute tentative d'extraction à distance. Dans l'idéal, les clés de chiffrement sont conservées dans un élément sécurisé qui impose une frontière sécurisée et isolée de sorte

**1 PRINCIPE DE FONCTIONNEMENT DE L'ÉLÉMENT SÉCURISÉ**

L'élément sécurisé sur la plateforme Trust de Microchip enregistre les données secrètes, y compris les clés et certificats qui sont générés pendant la fabrication au sein des usines sécurisées de la société et qui ne sont absolument jamais exposés au cours du processus entièrement sécurisé d'octroi de clé.



que les clés ne sont jamais exposées. Il ne s'agit pas là d'une mince affaire. Le système doit être inviolable et nécessite une protection contre les tentatives d'espionnage telles que l'analyse de canal latéral. Pour protéger efficacement la clé de cette manière, il convient de posséder une très grande expertise de la sécurité. Cela allonge également le temps de développement de la solution IoT.


• Etant donné leur rôle central dans les systèmes de chiffrement, les clés privées des appareils IoT ne doivent être vulnérables ni aux attaques physiques ni à toute tentative d'extraction à distance. il existe des éléments sécurisés, tels que le ATECC608A de Microchip Technology, qui disposent du niveau de protection requis.

Cependant, il ne s'agit pas d'une responsabilité à laquelle on peut renoncer, car la protection de la clé est une pratique de sécurité extrêmement importante à mettre en place. Heureusement pour les fabricants, il existe des éléments sécurisés, tels que le ATECC608 de Microchip Technology, qui disposent du niveau de protection requis (figure 1).

Malgré l'existence de tels composants, l'utilisation de la gestion de l'identité appliquée par le matériel reste problématique. La plupart des fabricants, intégrateurs système et fournisseurs de services ont rencontré des difficultés à appliquer l'identité sécurisée de manière à ce qu'elle ne puisse être compromise par un hacker particulièrement doué. L'approche conventionnelle consiste à configurer avec les clés privées adéquates un élément sécurisé matériel au cours de la fabrication. Cependant, des considérations relatives à la chaîne logistique ont généralement limité l'utilisation de cette approche aux déploiements à grande échelle. Octroyer une clé à chaque appareil avec une identité sécurisée unique revient souvent à personnaliser le processus de fabrication : un effort coûteux à moins que la personnalisation ne soit amortie par un large volume d'unités de sorte que le coût par appareil n'en soit que peu affecté. Cependant, il est dorénavant possible de fournir la configuration requise de l'élément sécurisé à un prix abordable pour une quantité minimum de commande (MOQ, pour Minimum Order Quantity) très faible, soit 10 unités, en préconfigurant les appareils IoT et en procédant à l'octroi de clé en usine. Grâce à cette formule, qui est compatible avec la plateforme Trust de Microchip, même une caméra de surveillance connectée basique, une passerelle, un climatiseur ou toute autre application similaire, peut être protégé par des certificats génériques pré-générés pour les appareils, verrouillés dans un élément sécurisé, pour une authentification autonome sur le cloud. Le coût total par appareil pour fournir ce stockage matériel des clés sécurisées avec un certificat générique est inférieur à toutes les solutions que peuvent offrir tous les fournisseurs de services PKI tiers et autres autorités de certification, et c'est une approche qui réduit significativement la complexité système ainsi que les délais de commercialisation.

## Comment déployer une solution

Les productions en petit à moyen volume ayant désormais accès à une façon économique d'intégrer la gestion de l'identité sécurisée dans leurs appareils, l'étape suivante consiste à configurer l'élément sécurisé de la façon la plus appropriée pour les cas d'utilisation. En effet, avec l'octroi de clé de l'appareil, sont associés des autorisations et d'autres éléments chiffrés qui sont utilisés pour le modèle d'authentification donné. À côté de l'identité principale de l'appareil, il est possible qu'il y ait d'autres clés privées et données secrètes à injecter dans l'élément matériel. Il peut s'agir par exemple, de données secrètes non issues de la clé principale mais qui peuvent être nécessaires pour authentifier des accessoires, périphériques, contenus tiers et hôtes distants, afin que leurs autorisations soient générées séparément.

Le principe derrière l'élément sécurisé est qu'il contrôle l'accès aux ressources vitales et agit comme une vérification contre les activités non autorisées, telles que les tentatives pour remplacer le firmware approuvé par le fabricant par un code malveillant qui pourrait essayer d'utiliser les informations secrètes contenues dans l'appareil afin de mener à bien de futures attaques.

L'une des exigences essentielles pour s'assurer que les hackers ne puissent pénétrer les appareils et les reprogrammer consiste à utiliser une stratégie de démarrage sécurisé, qui soit donc également protégé par un élément sécurisé. Le démarrage sécurisé garantit que l'appareil IoT peut uniquement faire tourner le code autorisé. En condition de démarrage sécurisé, l'appareil peut uniquement charger des blocs de code qui sont hachés et signés avec une clé privée détenue par le fabricant.

Quand le microcontrôleur a besoin de charger le code depuis la ROM de démarrage, le microcontrôleur demande une vérification à l'aide de la clé publique totalement immuable, conservée par l'élément sécurisé. Le microcontrôleur essaie de charger le code uniquement si la vérification réussit. Si l'appareil rencontre un bloc de code qui est signé de façon incorrecte, il s'arrête de charger le logiciel compromis et essaie de revenir à un état de sortie d'usine ou, à défaut, de se désactiver. Tant que le bootloader du microcontrôleur ne peut être modifié (c'est le cas s'il est stocké sur une ROM ou une mémoire flash protégée), la fonction de vérification ne peut être contournée.

## Ajouter d'autres cas d'usage de la sécurité

Une fois la sécurité mise en place, d'autres cas d'utilisation peuvent être facilement ajoutés, comme la prise en charge de l'authentification sur les serveurs distants basée sur un certificat, l'un des ingrédients clés des objets connectés. Cette authentification à distance utilise des protocoles standards tels que TLS (Transport Layer Security) pour les communica-

tions chiffrées et X.509, qui est utilisé pour gérer les certificats numériques servant à prouver l'authenticité d'un appareil ou d'un service.
Avec le standard X.509, tous les certificats numériques renvoient à un certificat OEM principal, au sommet de la chaîne de confiance, utilisant une hiérarchie de certificats subordonnés. Les informations que contient le certificat permettent d'identifier le propriétaire légitime de chaque certificat et, à partir de cela, d'obtenir la clé du certificat au niveau supérieur dans la hiérarchie, afin que la signature du certificat en dépendant puisse être validée.
Lorsqu'un appareil IoT correctement sécurisé communique avec un serveur distant, il utilise les informations qui se trouvent dans le certificat qu'il contient pour prouver qu'il est un utilisateur autorisé du service. De l'autre côté, le serveur utilise son propre ensemble de certificats pour confirmer à l'appareil qu'il est lui-même authentique. Tant que l'appareil conserve les certificats nécessaires, l'authentification bidirectionnelle peut être assurée.
Dans le contexte des objets connectés, des certificats numériques peuvent être utilisés pour simplifier le processus d'intégration des appareils lorsqu'ils sont mis sous tension pour la première fois et qu'ils essaient de se connecter à leur fournisseur de service sur Internet. Pour ce faire, les certificats nécessaires sont transmis aux serveurs quand l'élément sécurisé est programmé pour la première fois ; sont également stockés dans l'élément les certificats que l'appareil va utiliser pour authentifier ces mêmes serveurs, tout comme la clé privée principale de l'appareil.

En guise d'exemple de cette approche, Microchip a travaillé avec les fonctionnalités Amazon Web Services (AWS) pour permettre à tout produit créé à l'aide de la plateforme Trust d'être intégré de cette façon dans les services IoT de AWS. Comme les protocoles standard et les systèmes de certification sont pris en charge, les mêmes techniques peuvent être utilisées facilement avec tout autre service de clouding, tel que Microsoft Azure, ainsi qu'avec toute infrastructure de clouding privée ou hybride.

## Sécuriser les mises à jour à distance

Les mises à jour à distance (OTA) des firmwares des objets connectés sont un autre cas d'utilisation typique de l'Internet des objets. Ces mises à jour offrent la possibilité de corriger les failles de sécurité sans risquer que les appareils soient mis en danger par le processus de mise à jour en lui-même. Les mises à jour numériquement signées envoyées par le biais de la liaison OTA peuvent être vérifiées, de la même manière que l'authenticité du code est vérifiée pendant le démarrage sécurisé, avant que la mise à jour ne soit appliquée. Une fois en place, le code stocké devra également passer les tests du démarrage sécurisé quand l'appareil redémarrera.
On peut encore citer d'autres cas d'utilisation comme la protection des données d'IP (pour vérifier la validité des consommables et accessoires en option), ainsi que la protection des données de l'utilisateur, la rotation de clés et l'authentification LoRaWAN. Certains fabricants peuvent avoir besoin d'options de personnalisation qui dépassent le cadre de ces services principaux. D'autres peuvent avoir besoin d'une approche de la sécurité moins gourmande en ressources s'ils fournissent des appareils aux ressources limitées. L'autorisation de Google Cloud IoT Core, par exemple, ne nécessite pas de créer de certificat numérique entier. Le service emploie des clés de type JWT (JSON Web Token), qui sont dérivées de la clé privée principale contenue dans l'élément sécurisé ATECC608B, qui remplace une connexion conventionnelle avec identifiant et mot de passe.
Grâce à la plateforme Trust de Microchip et à sa prise en charge d'un grand nombre de formules différentes, il est très facile de gérer ces différents cas d'utilisation avec de faibles coûts de paramétrage. La première formule offre aux clients un moyen facile d'obtenir des appareils avec des autorisations sécurisées, utilisant un flux par défaut. Dans cette formule, la clé privée de l'élément sécurisé et les certificats génériques sont générés pendant le processus de fabrication, dans une usine sécurisée de Microchip. La clé et les certificats restent à l'abri des regards pendant tout le processus d'octroi de clé sécurisé, verrouillés dans l'élément sécurisé, où ils restent en sécurité pendant la livraison. Les autorisations publiques liées peuvent être envoyées aux services d'intégration via le cloud ou un Join Server LoRaWAN.
Comme de nombreux fabricants veulent bénéficier de davantage de flexibilité dans l'authentification et avoir la possibilité de créer et d'injecter des certificats basés sur leur propre chaîne d'authentification, une deuxième formule fournit un ensemble de cas d'utilisation préconfigurés qui offrent la possibilité de réaliser ces actions automatiquement. Des changements plus poussés sont possibles dans la troisième formule. Dans cette approche, que l'on peut voir sur la figure 2, le client commence par commander un composant avec élément sécurisé vierge, puis utilise les outils prévus à cet effet par Microchip pour suivre les étapes de l'octroi de clé, y compris le XML, qui est utilisé pour contrôler la livraison des clés privées et des certificats pour l'élément sécurisé dans les usines sécurisées de Microchip. ■

**2 PROCESSUS DE DÉFINITION DE L'OCTROI D'UNE CLÉ PERSONNALISÉE**

Après le processus de prototypage et de codage, l'octroi de clé commence par la cérémonie des clés PKI et la création des données secrètes. Après les tests de prototypage, les données secrètes sont verrouillées dans l'élément sécurisé.