LoRa security strengthened by Microchip secure authentication

Steve Taranovich - February 05, 2019

Microchip is no stranger to security solutions. They began with a Crypto ASIC collaborating with IBM in 1998 and implemented a number of other security solutions over the years culminating in a most impressive Advanced IoT Secure Element solution with their ATECC608A.

At the 2018 MEMS Executive Congress, Cynthia Wright, Principal Cyber Security Engineer, MITRE Corporation presented a call-to-action keynote on cybersecurity. Also, my visit to Vancouver, Canada last summer alerted me to LoRa security needs. We heard Antony Passemard, head of product management for Google Cloud IoT, say that the LoRa Alliance's vision around interoperability and openness aligns with the Google Cloud IoT mission to build the world's most open cloud and enable faster innovation and tighter security.

Connected devices are under accelerated software attack by hackers in this age of the IoT. Trust/authentication is critical on all networks because hackers are talented and want to disrupt systems because they can, or for the glorification they will get from their peers, or even for international or corporate espionage and disruption.

Current LoRa security

LoRa is based on a pre-shared key (PSK) architecture right now, but that is not good enough to address network security basics (**Figure 1**).

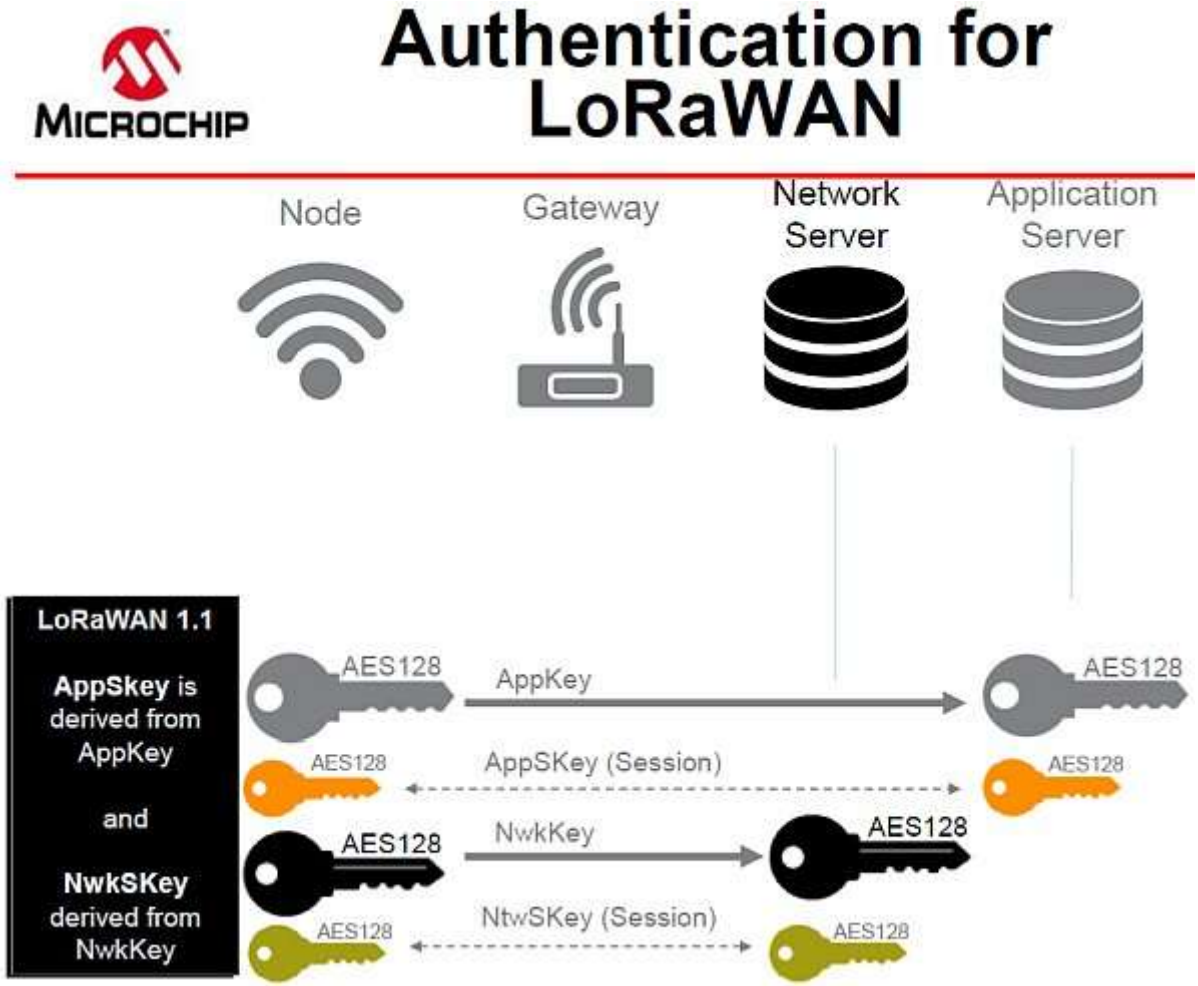

Figure 1 LoRaWAN 1.1 authentication right now (Image courtesy of Microchip)

Device vulnerability

In the existing LoRaWAN system, authentication keys are typically stored in flash memory. These keys are accessible to hackers and subject to counterfeiting, enabling a device identity theft possibility.

Backend vulnerability

In LoRaWAN 1.0x an AppSKey can be derived by a network server provider owing the AppKey and thus associated customer data can be decrypted. Also, an application server provider can use an AppKey to derive the NwKSKey and clone LoRaWAN end nodes.

LoRaWAN 1.1 improved backend security so that when in the possession of an AppKey only the AppSKey is derived. Also, with the NwKKey, only the NwkSKey can be derived.

However, the AppKey and NwKKey are still accessible and exposed to software and people. More security is needed.

Re-keying vulnerability

We need to look at how to transfer a key from network to network servers as well as application to application servers at a global scale. The challenge is we first need to copy the key to move it and then we need to trust the old network.

In the server solution we need a new root key (re-keyed). This can be generated in the application or the network servers, but is still exposed to software attacks.

In the node solution we also need a new root key (re-keying). Today, the new key is pushed over the air between/from servers, but this is still exposed in the microcontroller and is created from the untrusted, unvalidated root key.

Supply chain vulnerabilities from humans to servers

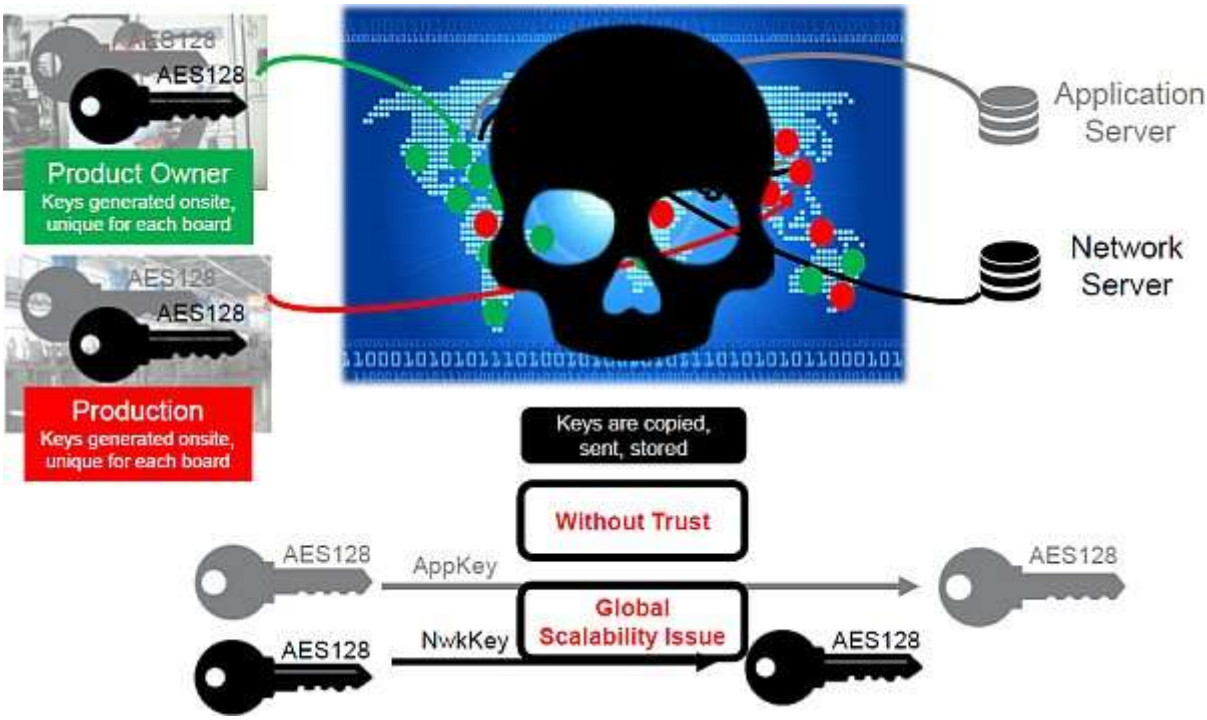

Figure 2 The supply chain has vulnerabilities from humans to servers (Image courtesy of Microchip)

Figure 3 shows a summary of vulnerabilities in secure authentication in LoRaWAN.

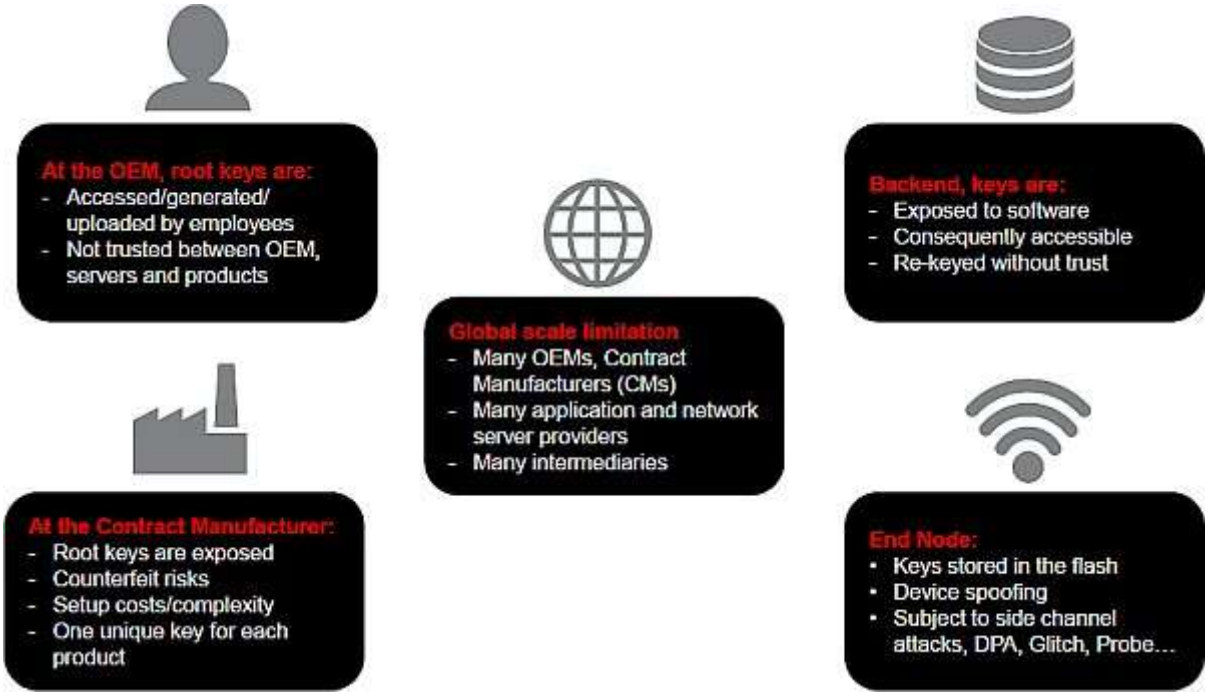

Figure 3 A summary of vulnerabilities in secure authentication in LoRaWAN today (Image courtesy of Microchip)

Secure distribution of shared keys

Secure distribution of shared keys

The Things Industries (TTI), a LoRaWAN network, application, and join server provider, is an all-i--one backend service for the LoRaWAN industry.

LoRaWAN secure authentication can be achieved via the Microchip ATECC608A-MAHTN secure element coupled with The Things Industry Join Server service. These two companies will provide a bundled offering:

- Pre-provisioned secure key storage
- Secure provisioning via Microchip service
- One year of bundled TTI Join Server service
- TTI Join Server re-keying

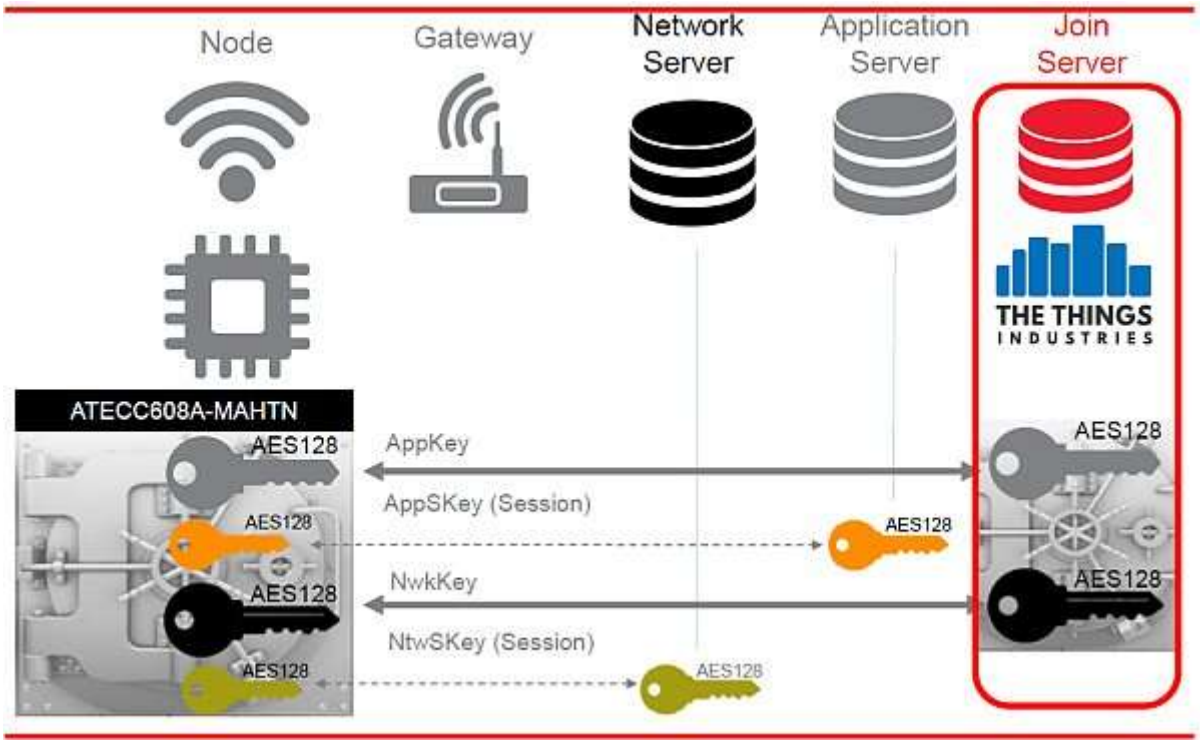

Figure 4 Authentication for LoRaWAN 1.0.x (Image courtesy of Microchip)

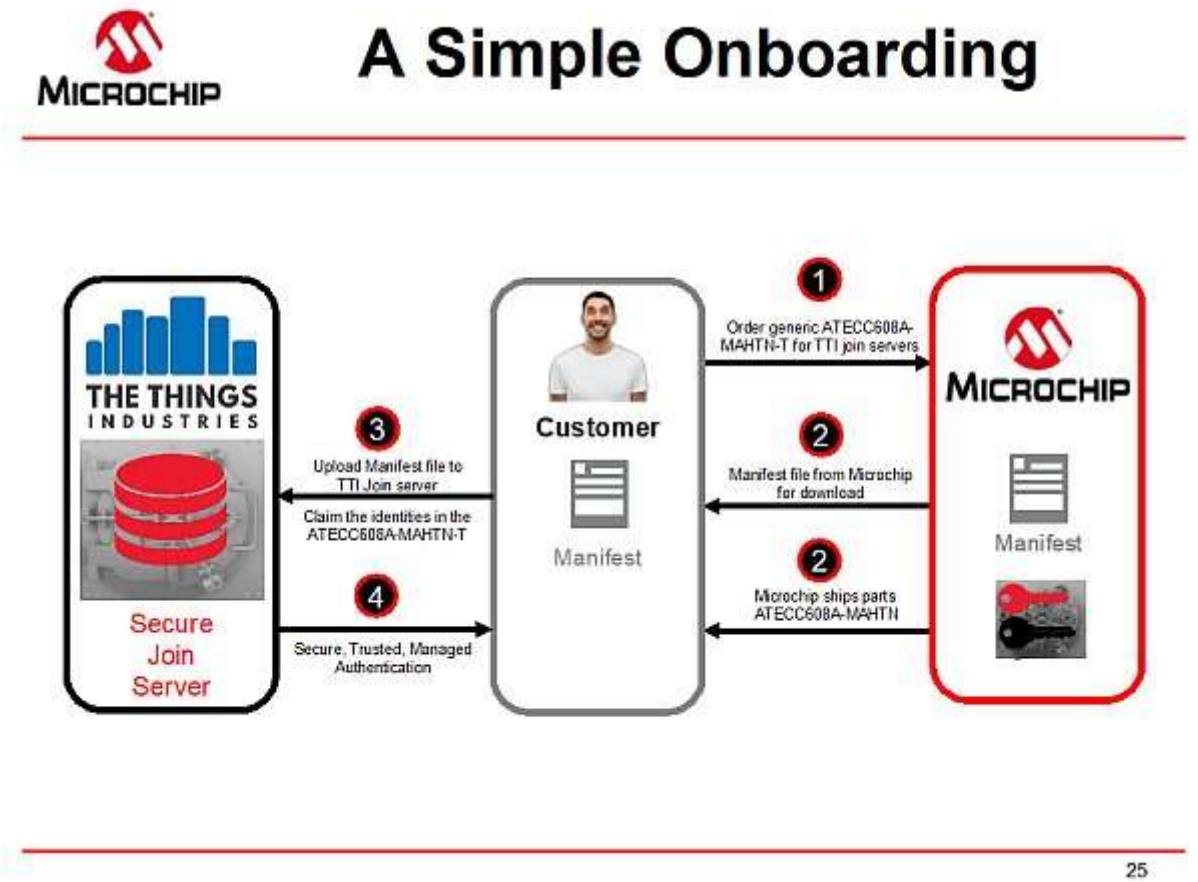

Figure 5 Simple onboarding (Image courtesy of Microchip)

Ultimately, the best solution for security practices for handling keys is:

- To isolate private keys from users because people are the most unpredictable security risk
- Isolate keys from software and firmware since an unprotected microcontroller can be hacked and their secrets embedded in code is vulnerable to attackers
- Isolate key manipulation from the manufacturing phase, and not only from supply chain equipment, but operators in the supply chain as well.
- Keep the critical crypto-primitives where the keys are in, isolated securely together because backdoors appear with algorithms dealing if keys and crypto primitive are in a two separate containers

We isolate keys in a secure element. That secure element is a secure boundary that protects secrets which is a companion device to any microcontroller thanks to the CryptoAuthLib library that goes with it.

Secrets are generated during manufacturing inside Microchip factories and inside the secure boundary. Keys are never exposed since they are handled solely by Microchip’s secure provisioning process.

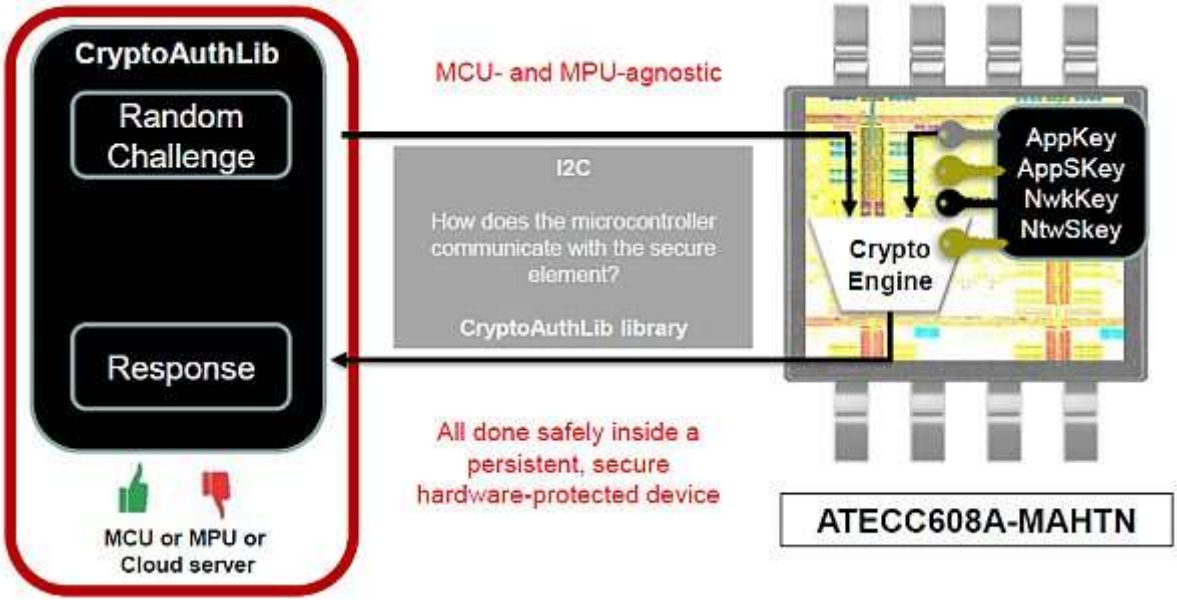

Figure 6 Keys are isolated in a secure element (Image courtesy of Microchip)

How are the keys protected in this environment?

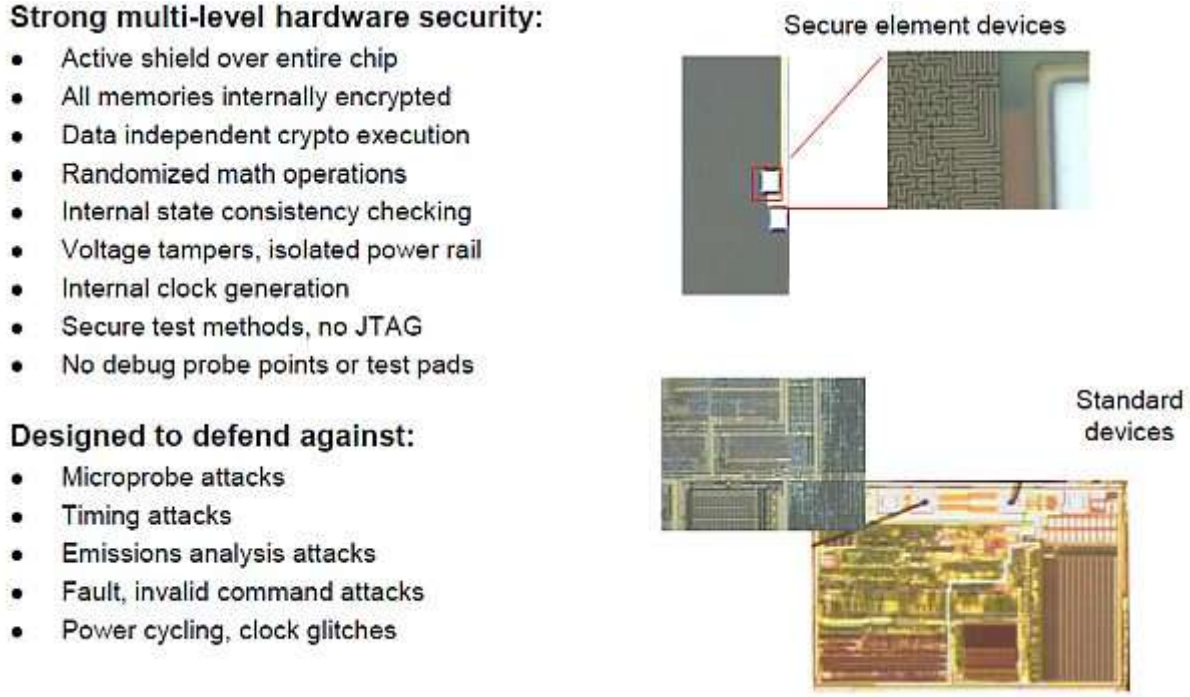

Figure 7 It matters how the keys are protected (Image courtesy of Microchip)

How Microchip measured safety

Too often, engineers think security is something obscure that can't be measured, which is a misconception. Common Criteria is a well known standard in the security industry with well defined specifications. It grants a level from EAL1 to EAL7 for military- or aeronautic-grade security. But this rating encompasses many requirements including a very specific section that relates to secure key storage. That section has its own rating call JIL for Joint Interpretation Library going from 1 to 31. To prove the level of security of the secure element, Microchip has submitted the ATECC608A to a third-party laboratory to have them try to extract the keys. A rule of thumb gives three man months to the lab to extract the key. The lab had not managed to extract the keys by using various

kinds of known attack methods.

The Microchip ATECC608A received a JIL ‘high” rating which is the highest JIL rating possible. A number is not assigned since no secrets were revealed in the period of time defined by the lab.

Now the logistic problem of shipping a LoRa authentication key all over the globe is solved with TTI Join Server service and Microchip pre-provisioned secure element. The keys are now shipping within a secure container without being exposed with a minimum orderable quantity of 1 unit (MOQ-1)!

Tools for designers

- AT88CKSCKTUDFN-XPRO CryptoAuthentication UDFN Socket kit
- SAM R34/R35 LoRa sub-GHz SiP with SAM R34 SiP, AT88CKSCKTUDFN-XPRO, and Microchip LoRaWAN stack
- SAM L21 Xplained Pro Evaluation Kit with Semtech Discrete Radio, AT88CKSCKTUDFN-XPRO, and Arm LoRaWAN stack

Steve Taranovich is a senior technical editor at EDN *with 45 years of experience in the electronics industry.*

Related articles:

- My journey with LoRaWAN begins at the LoRa Alliance
- Building the IoT: connectivity and security
- IoT & cloud security overview
- Connectivity options for the IoT
- Trust and then verify your IoT security
- Security: where the IoT meets the IT infrastructure
- IoT security: hardware vs software
- IoT module promises WiFi-LoRa-BLE triple play
- Technologies that make cities smarter and better to live in