Cellular IoT: Security Beyond SIM

Connectivity standards for IoT have one thing in common: implementing them ensures device connectivity, but not data security.

Billions of devices are being connected to the Internet of Things (IoT) through many different connectivity standards. These standards utilize either the licensed cellular spectrum (NB-IoT/LTE-M/4G/5G) or the unlicensed spectrum (e.g. LoRa, Sigfox). One thing these standards have in common is that they were not developed with data security in mind. For example, cellular IoT, with SIM as its standard for network security, does not protect data during transmission. It authenticates devices to a network and connections are encrypted, but this protection ends as soon as the data arrives at the first cell tower. After that, unprotected IoT data still has a long way to go to its destination.

Problem

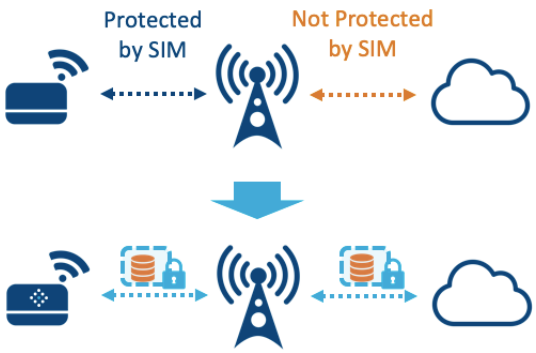
- Despite common misconception, while cellular networks use SIM to secure connections, SIM does not secure IoT data. SIM is used to authenticate devices to the network, not to provide end-to-end security for data
- Keys and certificates are needed on a device to set up a secure channel to cloud services
- Traditional ways of storing keys and certificates do not scale with volume of IoT

Solution

- Start security where the data is created, by deriving a unique and unclonable identity, based on SRAM PUF, for every connectivity module
- Use the identity to authenticate and encrypt all data to protect it from the moment it leaves the device, all the way to cloud services

Results

- Secure data from the moment it is created, delivering end-to-end protection
- An unclonable, immutable, invisible and unique identity to authenticate every device
- Low-cost solution for a scalable market
- Low resource requirements for IoT devices
- Flexible integration in hardware and software
- Security functionality provides a competitive advantage to connectivity chips and modules in a commoditizing market



The lack of focus on data security in IoT is an opportunity for chip and module makers to differentiate from other vendors.

The fact that having a SIM card in a device is not sufficient to protect IoT data is news to many, and an opportunity for chip and module makers to differentiate from other vendors. Adding the right security functionality will make the difference between success and failure for cellular connectivity chips in the IoT. But how can security be added in a market with significant price pressure?

To get data safely from an IoT device into cloud services, the device and the cloud service need to exchange keys and certificates. Standard methods exist for this, such as "zero touch provisioning." Once the appropriate credentials have been exchanged, the device and cloud service are able to set up a secure channel. The secure channel makes sure that data cannot be eavesdropped upon or altered when in transit.

But the biggest challenge when applying these methods is to get the required keys and certificates on the IoT device, especially since they are not part of a standard SIM implementation. Traditional methods for provisioning keys and certificates are either to inject them in manufacturing or to put them on an additional chip in the device, such as a secure element (SE). Both methods come with serious downsides.

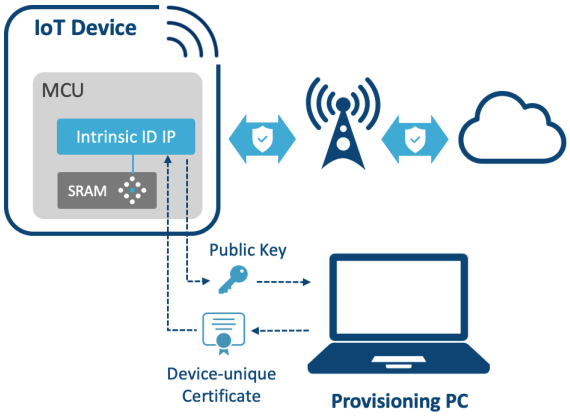
With key injection, there is:

- No secure storage for keys
- Potential key exposure in manufacturing
- Extra time and cost in production

Adding a secure element imposes:

- Higher BOM cost for an additional chip
- Dependency on SE vendor to handle keys
- Extra effort to onboard SE

So, getting keys onto IoT devices and storing them securely is a challenge. Adding an SE to a device will drive up costs, while injecting keys creates liabilities around provisioning and storing them.



Solution: Secure Connectivity

These problems are resolved by Intrinsic ID's secure connectivity solution. Using Intrinsic ID's patented SRAM PUF technology*, the IP internally creates a unique and unclonable identity for every connectivity chip, which is never stored in memory and cannot be copied from one device to the next. The identity is immutable, and invisible to adversaries, creating an unparalleled anchor of trust, which is even a suitable foundation for the future iSIM trend. Keys derived from the SRAM PUF are used to establish the secure channel.

Intrinsic ID supplies these solutions as either hardware or software IP. With this functionality in the chip hardware or module software, chip/module makers have a strong differentiator, and therefore value, in an increasingly commoditizing market. The solution also comes at a cost amenable to profitable scaling of the IoT and is future proof toward iSIM solutions.

Bottom Line Benefits

- Unclonable, immutable and invisible ID
- Authentication and encryption of data
- Flexible integration in HW or SW
- Competitive edge and future proof solution for connectivity platform at a low investment

** For details see our white paper "SRAM PUF The Secure Silicon Fingerprint" http://go.intrinsic-id.com/secure-silicon-fingerprint-lp*