SW update for Long lived products

Jørgen Karkov,
May 2016

Existing measures to secure SW update is too resource demanding for the resource restricted devices and a further complication is that the product is very long lived.

Situation:
Very resource restricted devices with very long lifetime in the market, not always connected.
Restricted devices means: 100KB ROM, 6KB RAM. No HW accelerator and upto 2MB ROM, 128KB RAM.
Lifetime in the market is >15 years (always turned on).
Some products are not always connected to the cloud, some are connected momentarily (during maintenance/service visit).
The SW update needs to be possible even at low bandwidth e.g. 115,2kbps. Product down time must be kept to a minimum.
Critical SW updates due to security issues is needed but the HW might not be able to support e.g. an enhanced key length that is needed after e.g. 13 years.

Currently we are using pre-defined keys, AES128 encryption, and are using compression and investigating delta updates.

Whishes:
The flexibility and security level that authentication using public/private keys gives but with lower resource requirement.

Easy and flexible key management is needed.
Fast and Secure way to generate and program Key’s into the Device during production. Produced in 100k numbers.

Protocol must support a slow authentication session as the product must operate as normal.

Recovery procedure when the product gets hacked.

A BIT ABOUT ME
Jørgen Karkov has several years of experience with embedded development in control and regulation and 20+ years of experience within Telecommunication (including participation within standardization, BroadBand Forum).