Security is a "Must Have" for IoT Devices

There are predictions that there will be 50 billion (or more) connected IoT objects by 2020, many made possible using today's mobile and computing technologies. Promising an exciting time for the electronics industry, however the biggest challenge and the number one concern is security. Lack of trust or poor security quality in the IoT objects will inhibit the adoption rate and slow down the IoT growth.

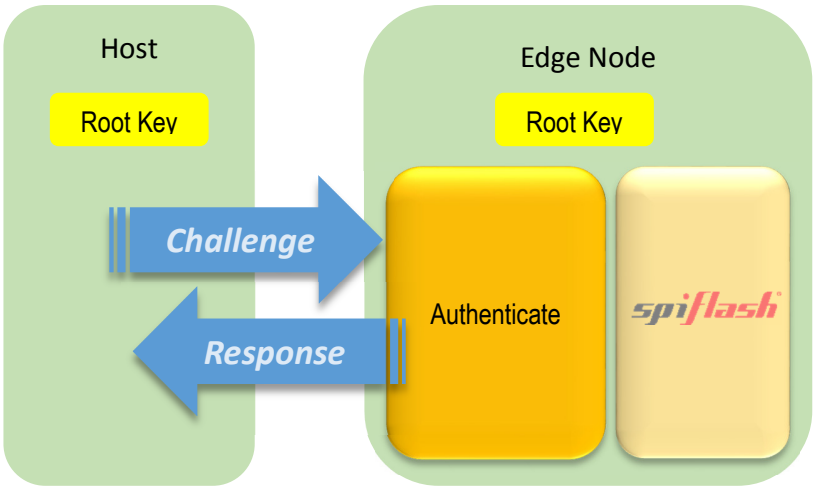
Within the IoT ecosystem hardware and software have to work together to stay ahead of the cyber hackers. Winbond introduced a new family of products called TrustME™. These new devices provide a secure, Trusted Memory Environment that can work with a multitude of microprocessors or SoCs to raise the level of security in many systems. Combining Winbond's proven flash technology with 12 years of security design experience, the secure Flash family provide designers simple, elegant and scalable solutions.

Flash Memory for Enhancing System Security

The security features in flash memory continues to evolve as hardware security requirements increases. The latest security feature involves authentication before access and execution of that code. Authentication is performed as needed and initiated by the host.

Serial Flash with Authentication

Validate Before Access and Execution



TrustME™ W74Mxx Family

- Proven flash memory technology
- Broad density range: 32Mb to 2Gbit
- HMAC-SHA256 algorithm engine
- 4 sets of OTP 256-bits
- 4 sets of volatile 256-bits for HMAC key storage
- 4 sets of 32-bit non-volatile monotonic counter registers
- Protection against replay attack and device cloning