Application Brief

Key Generation and Authentication Mechanism for TMP1827

Amit Ashara

Temperature and Humidity Sensing

Control systems often rely on inputs from sensors that can be part of a sub-system or module on a chassis or perhaps an off-board component. These components can be an ultra-high accuracy negative temperature coefficient (NTC) thermistor or platinum resistance temperature detector (RTD), which are often expensive and require additional engineering time and resources for calibration. In key industrial applications, where accurate temperature compensation is required, often a Class-AA RTD or a 0.01% tolerance NTC thermistor is used. However it is very easy to replace these expensive components with off-the-shelf RTD or NTC thermistor. Additionally, end equipment such as application or vendor specific battery-packs, medical disposables and reposables, require a mechanism by which the host controller can make sure that the plug-in module is genuine. To address the challenges and requirements of authentication, TI developed the TMP1827, a 1-wire based ±0.3°C accurate temperature sensor with integrated 2048-bit EEPROM and SHA-256-HMAC authentication engine which features:

- FIPS 180-4 compliant Secure Hash implementation
- FIPS 198-1 compliant HMAC implementation
- Authenticated write protection mode for EEPROM
- NIST traceable factory-programmed non-erasable 64-bit identification number
- IEC 61000-4-2 ESD for 8-kV contact discharge for plug-in applications

Challenge-Response

As previously-mentioned, the host controller is not capable of distinguishing such replacement devices and can have large errors and possibly be a hazard for safety applications. This becomes even more critical in medical applications where strict standards must be met. An optimum way of detecting such replacement is by adding authentication for the replacement device using the TMP1827. The host can issue a challenge message, which is generally a set of random data bytes, to the target device and receive a response, which is the hash signature for the message. By verifying the received response to expected response, the host can now verify that the temperature sensor is authentic and the digital value can be trusted.

However, the host and the target must share a common key so that both devices can generate the same digital signature. A common method is to use the same key for all targets, which poses a problem, where if one target device key is extracted, it is possible to compromise an entire batch of target devices. Thus, it is always advisable to have a unique key per target device, which while providing enhanced security, can make the process of key generation more complicated.

Key Generation

Figure 1 shows a method to make sure the key generation is unique per target device by using cryptographic means. To simplify the cryptographic scheme, an example with the SHA-256-HMAC is used. The host reads the 64-bit unique identifier, which is factory programmed, and then mixes the identifier with a user specific secret message and keys. This results in a unique 256-bit hash for every TMP1827, which can then be programmed back to the device securely and protected by the TMP1827. However, since not every host MCU can have a SHA-256-HMAC block, the SHA-256-HMAC engine of the TMP1827 can be used in a secure environment to generate the key. Otherwise, use the software implementation available here.

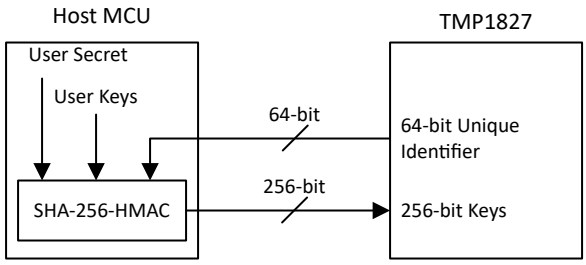

Figure 1. Key Generation Flow

Key Verification

Having generated and programmed the keys, in-field deployment now becomes easier. As shown in Figure 2, the same procedure now can be used by the host to re-generate the key and then use the key for generating the hash when writing to the TMP1827 or verifying the hash from TMP1827, without having to exchange the keys. With the use of a new challenge-response data payload for every transaction, the host can dynamically change the expectation from the target device, thus counteracting a replay attack model.

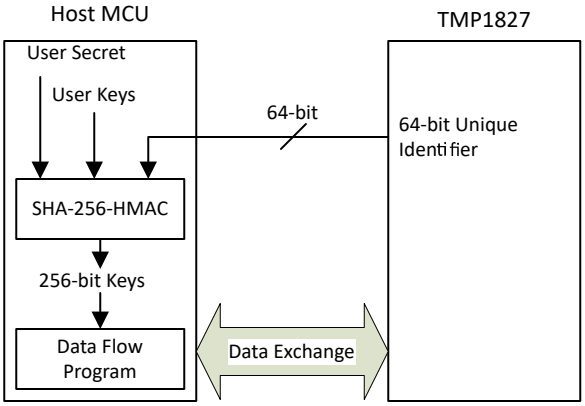

Figure 2. Key Regeneration and Data Flow Model

Summary

The TMP1827 is a unique ±0.3°C accurate temperature sensor, with an integrated SHA-256-HMAC authentication engine, which can allow industrial applications such as heat-cost allocators and cold-junction compensation, that depend on accurate temperature measurements to securely read temperature and update key system calibration contents in the 2048-bit EEPROM, while at the same time deterring counterfeits and evading tampering of the end equipment.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265