Application Report
SLUA346A–July 2005–Revised August 2014

Battery Authentication and Security Schemes

Portable Power Battery Management Applications

ABSTRACT

Driven by integrated functionality and shrinking form factors, the demand for portable devices continues to grow. These portable devices need rechargeable batteries and peripherals that must be replaced before the life of the portable devices expires. This has opened a huge market for counterfeiters to supply cheap replacement batteries and peripherals, which may not have the safety and protection circuits required by the original equipment manufacturer (OEM).

These counterfeit batteries may violate both mechanical and electrical safety requirements related to short-circuit protection, charge safety, and other specifications. It is usually impossible for the consumer to determine the quality without making a purchase and possibly learning the hard way. This can lead to a potentially dangerous situation for end-users.

Adding simple and effective authentication technology to the portable system allows the OEMs to ensure customer satisfaction and to protect their businesses. More importantly, safety is improved throughout the life of the product.

This application report discusses in detail the simple identification (ID) and the more complicated challenge and response SHA-1/HMAC-based battery authentication schemes. The presented battery authentication architectures meet the counterfeit battery challenges to protect OEM businesses and to promote end-user safety and satisfaction.

Contents

List of Figures

1 Identification-Based Authentication Scheme

Several authentication schemes currently are used to identify that a battery pack is intended for specific portable products. The most common is the form factor or physical connection. Every cell phone battery pack on the market has a different form factor. However, the physical size of the battery pack is not even consistent within all phones manufactured by the same company. Whereas this method of identification affords some level of protection for low-volume manufacturers, batteries from manufacturers with high volumes are much more likely to be counterfeited. It would be an inexpensive solution to standardize form factors and keep them unchanged. Many OEMs are moving toward this economic model. However, this provides an opportunity for counterfeiters to replicate the battery pack by measuring the physical dimensions.

To improve battery identification, an electrical identification scheme could be used so that simple physical counterfeiting is no longer enough to replicate the battery. Figure 1 shows the ID authentication functional block diagram. The challenger or host sends a command to read the data from the device (responder). The data include product family code, identification number (ID), and cyclic redundancy check (CRC) value. Each device has a unique ID number. The response data is compared with the data in the host. If the data from the device is valid, then the host allows enabling the system operation. Otherwise, it inhibits the system operation and provides an error code and a warning signal to the end-user. Integrated circuits (IC) such as the bq2022A, bq2024, bq2026, and bq2028 provide a unique ID for each device.

Figure 2 shows the battery pack typical application circuit with the ID chip. The host communicates with the chip through a dedicated general-purpose I/O to determine if an ID is available and valid. The ID authentication scheme eliminates a significant number of non-OEMs. However, the ID issued by the device is available to anyone with an oscilloscope. It is still possible for the counterfeiters to replicate the ID to the issued command. But, it increases the cost to implement a fake ID. Even so, some non-OEMs still go after batteries and peripherals for high-volume products and adding a cheap microcontroller to the system is acceptable to them. To counter this threat, a more robust authentication scheme is required.

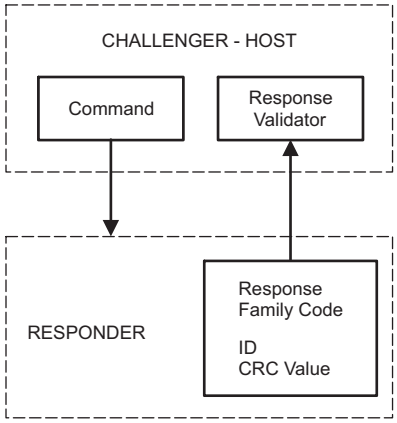

Figure 1. ID Authentication Functional Block Diagram

2 Challenge and Response-Based Authentication Scheme

A straight ID authentication increases the complexity for the counterfeiter to identify the ID and the command. It is secure by adding cost to the system. If cost is important, a non-OEM will opt for a battery or peripheral without this functionality. But for those non-OEMs that are willing to add cost to their system to secure a business opportunity, something more robust than an ID authentication is needed.

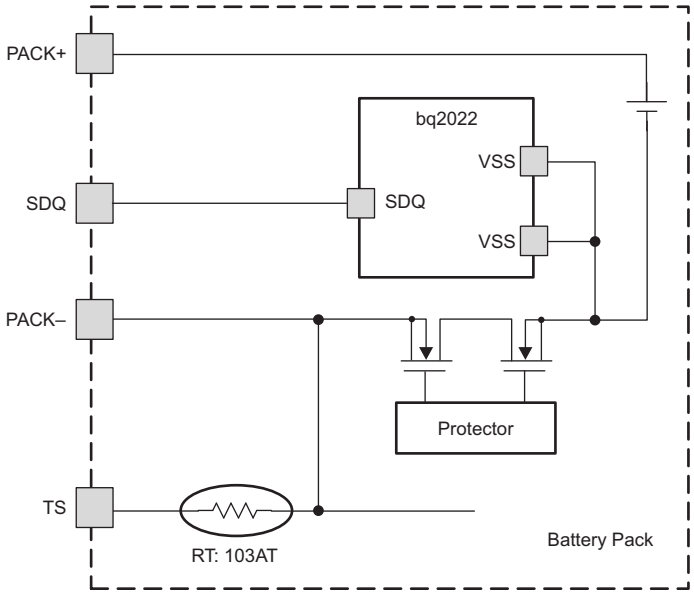

Figure 2. Typical Application Circuit With ID Chip

A more cost-effective and robust approach is based on a challenge and response scheme as shown in Figure 3. In this scheme, the host sends a random challenge to the battery pack that contains the identification device, or responder. The random challenge consists of a number of bits of random data generated by the host. The secret key is shared by the challenger and the responder. When the authentication device receives the challenge information, it performs the authentication transform with the secret key stored in the private memory of the device to calculate the response. On the other side, the host performs the same transform using the same secret key. The challenger compares the value it computes against the response obtained from the identification device. If the calculated data from the authentication device matches the expected answer from the host, then the host authenticates the battery and allows the system to start operation. Otherwise, it may inhibit the system operation and provide a warning signal to the end-user.

Why is this scheme more secure than the straight ID-based scheme? The single ID authentication scheme has a fixed response to a fixed challenge or command. It is relatively easy for counterfeiters to find out the fixed challenge and command. However, the challenge and response secure scheme changes the query and response every time. A relatively large and random challenge makes a look-up table solution expensive in terms of memory. It has a direct correlation with the monetary cost and is difficult to guess. In addition, part of the transform involves a secret key shared between the challenger and the responder. Security then resides in the secret key, allowing the scheme to use a public authentication transform algorithm. Public authentication transforms are effective because they can be thoroughly and properly evaluated for robustness against attacks seeking to uncover the secret key.

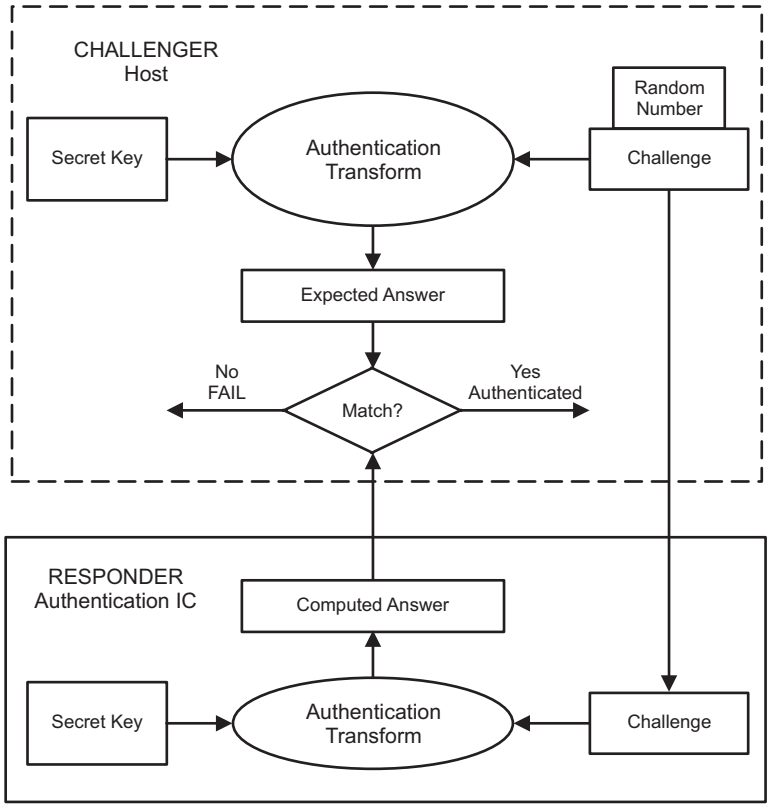

Figure 3. Challenge and Response-Based Authentication Scheme

3 Challenge and Response SHA-1-Based Authentication Implementation

To achieve a high level of authentication, a more sophisticated algorithm such as the SHA-1/HMAC secure hash algorithm can be used. The SHA-1/HMAC has been used for years to authenticate Internet transactions for Virtual Private Networks, banking, and digital certificates. The algorithm used in SHA-1/HMAC is iterative.

One way hash functions can process a message is to produce a condensed representation called a message digest. It enables the determination of the integrity of the message. Any change to the message results in a different message digest with a high probability. This property is useful in the generation and verification of digital signatures and message authentication codes.

To authenticate a battery pack, the host generates a 160-bit random challenge. The generated random challenge is transmitted to the authentication device, which uses the secret key along with the 160-bit random challenge from the host to calculate the authentication digest value.

The host uses the same secret key along with the same 160-bit random challenge that is sent to the authentication device to calculate the authentication digest value. When the host and the authentication device have completed the calculation, the host reads the authentication digest value from the authentication device. It then compares it to its own value. If the values match, the battery pack is authenticated. Otherwise, the host may not initiate the system start-up command or provide a warning signal to the end-user. Because there is a 160-bit random challenge, it generates 2^{160} possibilities. This significantly improves the security level.

4 Summary

The selection of the battery authentication scheme between the simple ID authentication and SHA-1/HMAC-based authentication depends on the security level needed and cost for the applications. The simple ID authentication is the least expensive and is good for cost-sensitive applications, but it is easy to replicate. Although challenge and response SHA-1/HMAC-based authentication is the most expensive, it has the highest security and is good for high-end portable applications. The bq2022A, bq2024, bq2026, and bq2028 integrated circuits all provide the simple ID function, as well as including additional scratch memory and other functions. The bq26100 is an option when SHA-1/HMAC authentication is required.

In addition, both ID and SHA-1/HMAC features are included in many battery fuel gauges that reside inside the battery pack. For example, the bq27541-G1 and bq27742-G1 fuel gauges have general-purpose flash memory locations, and the ability to perform SHA-1/HMAC encryption in addition to their full set of battery gauging functions. The bq27742-G1 fuel gauge further integrates the protector function, making it the only IC required in a single-cell battery pack. For multi-cell packs, fuel gauges, such as the bq40z50, also include the SHA-1 function.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

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