

# Opening the door to smart battery design

Robert Rozario, Application Engineering Manager, Infineon Technologies

The worldwide transition to ever smarter mobile devices, including phones or connected tablets, has obliterated the line that once existed between phones and computing devices. Today's multitasking devices enable work, finance, entertainment and social interaction on the go like never before. This mobile revolution presents challenges for device designers that need to produce nearly constant innovation in design while achieving ever tighter cost margins. It also opens market opportunities for both authorized and unauthorized third parties to offer aftermarket devices such as batteries. Work by an organization called the MIPI Alliance is helping the engineering community respond to these overlapping design challenges. Here's how one MIPI Alliance defined standard has opened the door to a new generation of smarter batteries.

### **The mobile device Achilles' heel**

As part of its continuing study of consumer product customer,<sup>1</sup> J.D. Power and Associates found that smartphone owner satisfaction is greatly impacted by battery performance, particularly the length of battery life before recharging is required. The study found that this issue is exacerbated by the transition to 4G technology, where more energy intensive network search and more frequent access to data networks place greater demands on the battery.

Clearly, users of smartphones and other connected mobile devices would benefit from improved batteries. But engineers who set out to design a "smart" battery have to consider more than just the time between charges. Design goals also include shorter charging time, increased safety and reliability. The mobile device supplier, which is accountable to the consumer for the end product performance, of course has a stake in ensuring product quality and reliability.

### **A simple, smart battery interface**

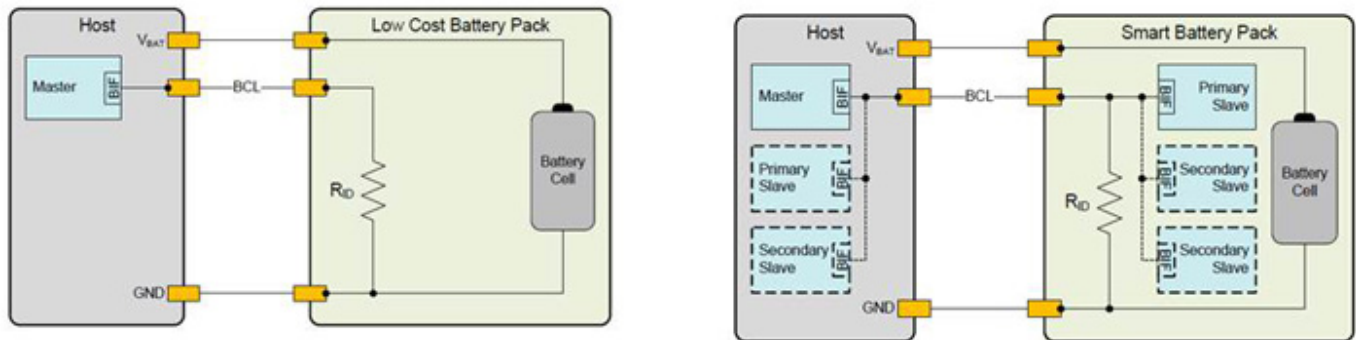
To address all of these interests, a collaborative industry group called the MIPI Alliance developed and published a key specification to enable the creation of smart batteries for mobile devices. The MIPI Battery Interface (BIG), released in early 2012, defines a standard interface for mobile device batteries. Designed with input from the complete mobile device ecosystem, the MIPI BIF is an enabler with the potential to reduce battery cost by achieving higher volumes across product and brand lines, simplify supply chains, and improve consumer safety via features that operate through the interface, including authentication and over-temperature monitoring/turn-off.

The MIPI Battery Interface (BIF) Specification<sup>2</sup> was defined to offer a cost-efficient and flexible communication interface solution between a mobile device Host and Battery Packs. The fundamental requirement for a battery interface is to provide a method to communicate battery characteristics information to ensure safe and efficient charging control under all operating conditions. Two forms of interface are

## Opening the door to smart battery design

Published on Electronic Component News (<http://www.ecnmag.com>)

provided in the BIF: an interface to low cost batteries that supports detection of battery chemistry and capacity for basic safety, and a smart battery interface that supports enhanced features.



The BIF recognizes on insertion whether a battery is a low-cost device (detection, chemistry and capacity) or a smart battery interface. It's this second interface that opens the door to truly smart batteries, in which multiple tasks like safety, monitoring the health of battery cells, charge control, and authentication can be implemented.

To meet goals of simplicity, low cost and ease of implementation, the BIF is specified as a single wire interface with a silicon footprint of approximately 1k gates. On the host side, it typically is integrated onto the power management or digital baseband IC. In some cases, it may be implemented as software in conjunction with a general purpose input output (GPIO) pin. On the battery pack, the BIF may also be implemented in hardware or as a combination of hardware and software. Since battery size is of course a paramount concern for mobility, high levels of integration to reduce required PCB space inside the battery pack is important.

A MIPI Alliance White Paper describes the pre-defined functions of the BIF.

1. BIF Protocol; a data independent transport interface scalable from 2kbit/s - 250kbit/s (average)
2. Slave control providing status and control information for tasks executed on slave device(s)
3. Temperature sensor providing single and periodic routines and threshold triggered interrupts
4. Authentication executed at minimum with 80-bit symmetric key length or equivalent
5. NVM allowing reading and writing of device (battery pack) information

While only the protocol function is mandatory for a Slave (battery pack) device defined as a low cost battery, the other functions are the ones at the heart of a smart battery. A look at how these added functions are implemented in battery pack ready IC demonstrates their value.

### The solution

A smart battery is one that is able to perform the following tasks:

## Opening the door to smart battery design

Published on Electronic Component News (<http://www.ecnmag.com>)

---

1. Hardware Authentication
2. Data storage
3. Data Integrity
4. Health monitoring (temperature)
5. Safety (over voltage protection)

Engineers implementing a hardware (IC) solution should check-list chip features against the requirements of the MIPI Alliance BIF specification for data transport, available non-volatile memory, temperature sensing as a reliability feature, and authentication. There also are alternate approaches to authentication to consider. Asymmetric cryptography (see sidebar) can be used in a software-to-hardware authentication configuration that does not need a hardware master device on the host side. The host-side implementation runs on the host processor in software without compromising the security of the system, unlike in symmetric cryptography systems (e.g. SHA/DES/TDES/AES).

Incorporating hardware authentication into smart batteries (and the corresponding hosts they are intended for) benefits both consumers and suppliers. The system can notify a user if an unauthorized and possibly dangerous aftermarket battery is connected and it can be programmed to not charge. In addition to consumer safety, this protects the supplier from the risk of illegal aftermarket products leading to possible warranty issues. If an unauthorized battery is somehow used, a system log is available for service/warranty verification of the chain of events.

Over temperature protection, which reduces the risk of battery cell damage due to overly fast charging, potentially increases both safety and longevity of the battery. This is also true for the overvoltage protection implemented as part of the IC's power management features. Collectively, this integration eases design of a safer, more reliable and verifiable battery. That translates to more satisfied customers, while assuring that participants in the device ecosystem have a well-documented and traceable supply chain.

# # #

### **SIDEBAR: Asymmetric cryptography**

In symmetric cryptography the same key is used for encryption and decryption. If one key is hacked, the entire chain of security protection is broken. Software stored keys also can be comparably easy to access and read out. Typically, symmetric algorithms are used in situations where a secure surrounding environment can be established, like in banking and data transmission.

On the other hand asymmetric cryptography uses two different keys for encryption and decryption. One key, the so-called public key (P-Key), can be made public (and therefore used in the Software implementation), as long as the other key, the secret key (S-Key, sometimes also called private key), is still in the safe hardware environment of the chip. Asymmetric cryptography is typically used in applications requiring a high level of security in a critical environment like military or government implementations and it is used for identity protection in electronic passports worldwide.

## Opening the door to smart battery design

Published on Electronic Component News (<http://www.ecnmag.com>)

---

Leveraging the advantages of asymmetric cryptography, Infineon implemented a product authentication and security scheme that is most suitable for embedded applications. This approach uses a specific elliptic curve cryptography (ECC) algorithm implementation. This is a mathematically very complex and highly secure form of encryption that combines top level operational security with cost efficient implementation. It protects data such as the Private Key, the unique chip ID and other customer information in a protected memory space that is secured from modification.

<sup>1</sup> JD Power Associates, 2012 U.S. Wireless Smartphone Customer Satisfaction StudySM--Volume 1 and the J.D. Power and Associates 2012 U.S. Wireless Traditional Mobile Phone Satisfaction StudySM--Volume 1, March 15, 2012

<sup>2</sup> MIPI Alliance, Battery Interface Specification Home Page, <http://mipi.org/specifications/battery-interfac> [1]e, February 2012

### **Source URL (retrieved on 01/26/2015 - 4:35pm):**

[http://www.ecnmag.com/articles/2013/05/opening-door-smart-battery-design?qt-video\\_of\\_the\\_day=0](http://www.ecnmag.com/articles/2013/05/opening-door-smart-battery-design?qt-video_of_the_day=0)

### **Links:**

[1] <http://mipi.org/specifications/battery-interfac>