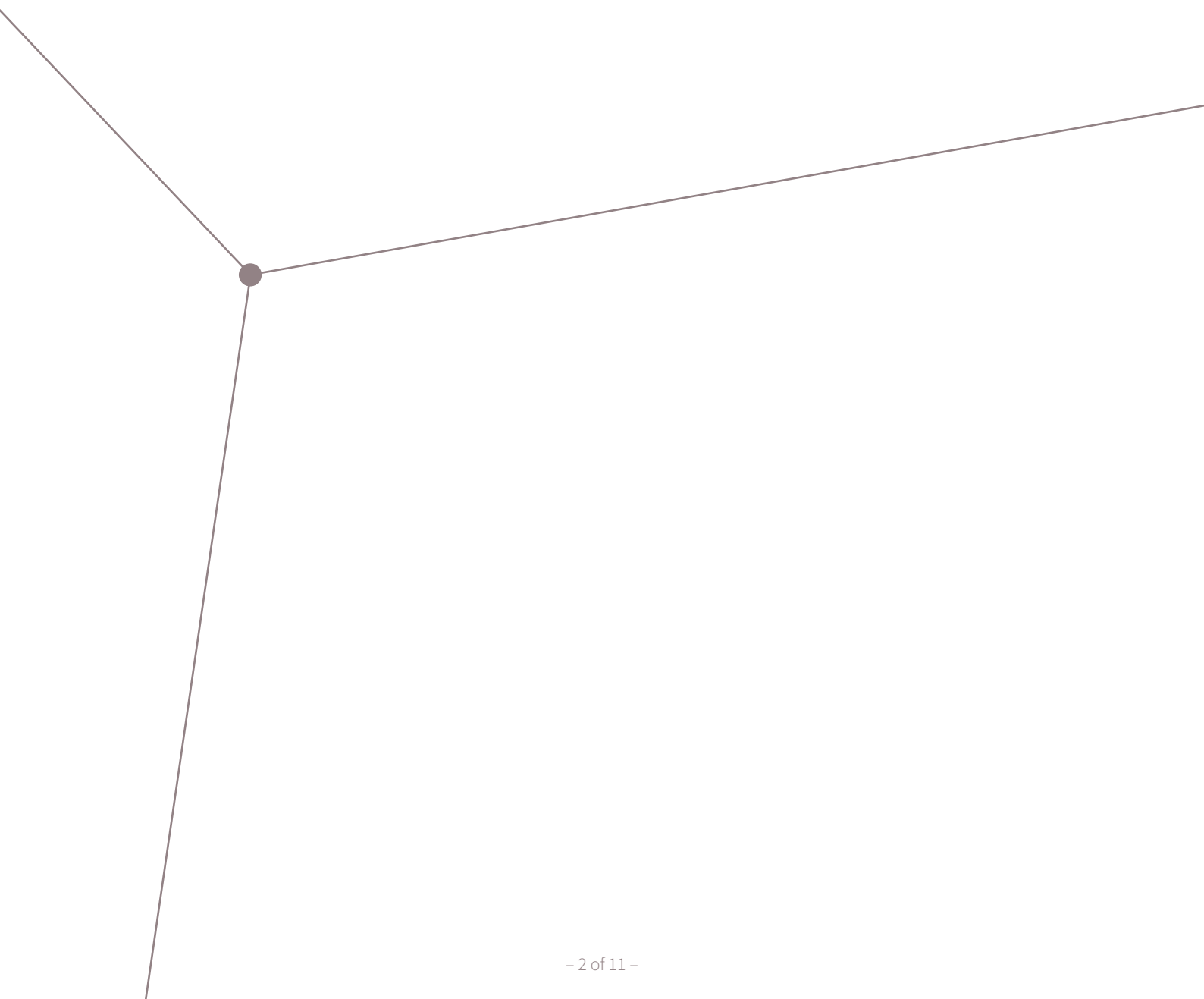
Authenticating batteries before rapid and fast charging

www.infineon.com/OPTIGA-authenticate

Contents



Introduction

If asked, most consumers will complain about the battery life of their smartphone. In reality, this is more a charging issue since, with traditional charging solutions, even a couple of hours of charging can result in a minimal improvement in charge on some handsets. Smartphone manufacturers are differentiating their offering by providing fast or rapid charging solutions. However, this places the battery at greater risk of catastrophic failure should it be replaced by a battery that is neither fast-charge capably, nor approved by the smartphone manufacturer.

While consumers are grateful for today's improved charging speeds, there are still challenges with regard to interoperability between chargers and smartphones, and even the cables used play a role. And, although authentication is available for these devices, none is being implemented between the smartphone and its battery. With an extensive market of third-party, potentially unsafe, batteries, the use of hardware-based security to hinder product cloning needs to be urgently addressed. This white paper explains how to place the smartphone at the center of trust for the entire charging process, and which authentication solutions allow the smartphone to check that the installed battery is suited to rapid charging.

Our high expectations for smartphone batteries

While sleek, gleaming, touchscreen smartphones have replaced the bulky, featureless mobile handsets of yesteryear, the only aspect that seems to have got worse is that of battery life. It is true that the old GSM handsets could be used for perhaps a week at a time by most people before they needed charging. However, this also overlooks the fact that the power demands, that were limited to the core features of telephony and sending SMSs, were relatively low, and that users spent less time 'on their phones'.

Today's smartphones have large high-definition color displays, touchscreen surfaces, and spend a lot of time executing complex algorithms to decompress video frames and images. On top, multiple radio standards are being used continuously to transfer data back and forth. According to some statistics[1], we grab our phones up to 58 times a day and spend on average 3 hours and 15 minutes a day using them: the top 20% of users spend 4 and-a-half hours on them per day. That is close to an entire day per week.

For electronics engineers, it is, quite frankly, incredible that smartphones operate on battery power for an entire day before requiring charging. But the average consumer, understandably, finds it wearisome to develop strategies that allow the daily charge fits into their routine.

With little room left to differentiate in terms of fit, form, and function, battery life and charging speed have become the new killer features.

1 blog.rescuetime.com/screen-time-stats-2018/

Fast charging

Since smartphones cannot really get any larger in terms of area, and the drive in recent years has been to make them even thinner, the volume of the battery across all smartphone suppliers is pretty much defined. While battery technology has made leaps-and-bounds progress in the past decade with the introduction of lithium-based technologies, the level of energy density we have today is unlikely to jump significantly for some time to come. One way in which battery life can improve is by implementing more energy-efficient displays, backlights, touchscreens, and processors, but here many of the energy-saving techniques have already been exhausted.

One of the big coups for European politicians was getting manufacturers of "data-enabled mobile phones[2]" to commit to USB as the connector of choice for the charging interface (standard EN 62684:2010). This type of approach was also standardized in China and was also adopted by the GSM associated with their Universal Charging Solution (UCS). While this greatly reduced the plethora of charging devices and connecters that had been in use down to a USB-A receptacle charger, it also baked-in smartphones to the (around) 5 V, 500 mA output supported by the USB 2.0 specification that was in place at that time. This of course limits the power output to 2.5 W.

This was not seen as being particularly limiting at the time but, since then, smartphone batteries have grown in capacity to 5,000 mAh in some top-of-the-range handsets[3]. Finding the time to charge to such battery capacities from a 500 mA source during our hectic daily schedules is a challenge.

To resolve this issue, a range of technical solutions have emerged. One comes from the USB Integrators Forum (USB-IF) themselves in the form of the USB Power Delivery (USB-PD) specification[4]. This allows, after negotiation, the use of output voltages of 5 V, 9 V, 15 V, and 20 V, and currents of up to 5 A. Thus, anywhere between 0.5 W and 100 W can be sourced from suitable USB receptacles.

To meet the needs of smartphone battery charging applications, there is also the USB Battery Charging Specification[5]. This defines additional power outputs beyond the standard for a typical USB host or hub port. The typical computer USB port is known as a Standard Downstream Port (SDP) and offers the following three output currents:

- Bus suspended: 2.5 mA average
- Not suspended; device not configured: 100 mA
- Not suspended; configured for maximum current: 500 mA

This, of course, assumes that the device being connected enumerates to the host computer, and the host computer is awake and ready to accept devices being connected.
Since that is not always the case, there are two further port definitions, as follows:

- Charging Downstream Port (CDP): By using a special hardware handshake using the D+ and D- data lines, devices can request to draw up to 1.5 A before the smartphone has even enumerated.
- Dedicated Charging Port (DCP): A simple short between D+ and D- signifies a DCP outlet, allowing this port type to be implemented in devices that don't enumerate, such as wall chargers. Such chargers can provide up to 1.5 A of current.

2 en.wikipedia.org/wiki/Common_external_power_supply
3 www.tomsguide.com/uk/us/smartphones-best-battery-life,review-2857.html
4 en.wikipedia.org/wiki/USB_hardware#USB_Power_Delivery_(USB_PD)
5 www.usb.org/document-library/battery-charging-v12-spec-and-adopters-agreement

Unfortunately, despite the clarity proposed within the USB-IF's collection of specifications, it seemingly doesn't go far enough for smartphone manufacturers. As a result, a plethora of 'fast charging' solutions functioning over what looks like a normal USB cable for the layperson, such as VOOC, SuperCharge, and Quick-Charge, have been spawned. Some of these are compatible with the USB-PD specifications, while others are not. The available data shows that such chargers can provide output voltages of anything up to 20 V output and provide up to 55 W[6].

Of course, charging of Li-ion batteries can be risky. There have been several high-profile cases of batteries exploding, overheating, and even inflating, even when using simple, low-power USB chargers[7]. In the era of fast charging the chances of incorrect voltages being supplied, cable use that cannot handle the currents being drawn, and the use of replacement batteries that cannot support rapid charges, are growing. Thus efforts need to be undertaken to allow users to safely charge their smartphones regardless of the combination of charger, cable, handheld device, and battery.

The issues associated with attempting to pass too much current through a USB cable have been largely resolved, thanks to what is known as Electronically Marked Cable Assemblies (EMCA) and informally as 'e-markers'. Small active circuits embedded into one or both ends of a USB-C cable share their characteristics with the downstream-facing port (DFP). Only once its capability has been established, the higher currents and voltages being requested are configured.

To tackle the issues that may be caused by 'poor quality' chargers and cables, the USB-IF has also created an Authentication Specification[8] for USB-C implementations. The intent is to allow devices such as smartphones to confirm that the charging port being used, either self-sourced hardware or a socket found at an airport, has been certified. What is considered certified may be set by the product's vendor, may be configurable by the user, or even defined by an organization, such as an employer, together with their other IT policies. As an aside, this authentication capability also extends to authenticating USB products, such as flash drives, allowing only certified USB devices to operate with an employee's laptop, as one example.

6 www.digitaltrends.com/mobile/how-does-fast-charging-work/
7 www.theverge.com/2016/9/8/12841342/why-do-phone-batteries-explode-samsung-galaxy-note-7
8 www.usb.org/document-library/usb-authentication-specification-rev-10-ecn-and-errata-through-january-7-2019

Keeping tabs on the battery

While all of these efforts, if followed, can help to provide not only a high-quality user experience but also a safer one, one risk vector remains open: the battery. With consumers looking for the best deal when replacing the battery in their old phones, there is no guarantee that any replacement battery inserted will be of the correct quality and suitable for the fast-charging capabilities of the smartphone. While this is currently recognized as a potential issue by the industry, there are currently no initiatives being undertaken to resolve it.

The ideal approach here would be to make the smartphone the central point of verification since it has the necessary processing performance and software flexibility required. It could establish trust using elliptic-curve cryptography (ECC) to the charger, establish the credentials of the USB-C cable being used, and also check if the battery is vendor-approved. If all the elements prove to meet the required level of trust, full fast-charging functionality can be engaged.

The process for establishing the integrity of a battery is very straight forward and could use established authentication processes (Figure 1). These typically operate in the following manner:

1. The smartphone host is provided with a public Certificate Authority (CA) signing key.
2. It then requests the certificate, public ECC key, ID, and other signed data from the battery.
3. The smartphone verifies that the public key was indeed signed by the expected party (approved battery).
4. It then sends a randomized challenge to the battery.
5. The battery calculates its response using its ECC private key.
6. This is then sent back in a response back to the smartphone.
7. The smartphone then verifies that the response is valid using the public key.

Since the smartphone does not require any private secret using this approach, it is only necessary to check if the battery is provided with appropriate security protection measures.

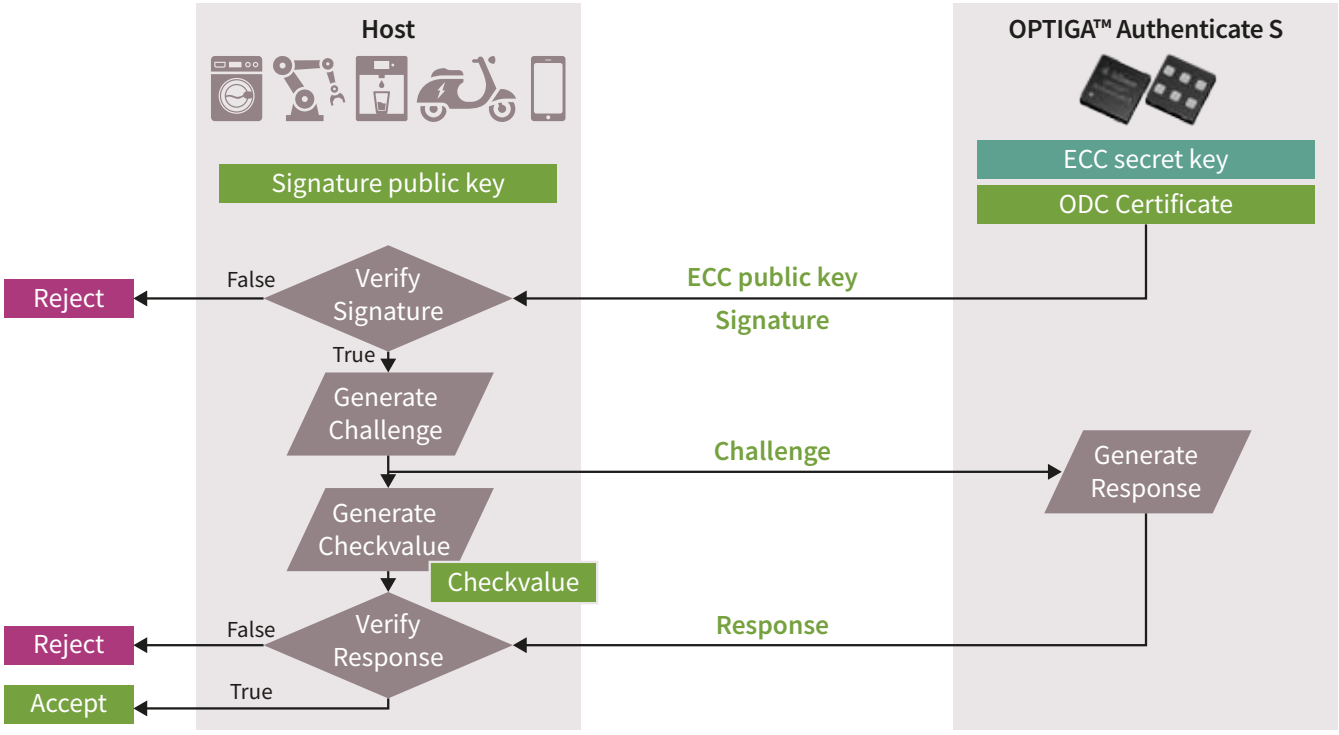


Figure 1: Battery authentication can be implemented using a simple, established process together with a suitable silicon solution, such as OPTIGA™ Authenticate devices.

Optimal security implementations for batteries

Implementing such asymmetric authentication is very simple nowadays with single-chip solutions available for this very purpose. Session secrets are generated implicitly during the authentication procedure using a 'secret calculation'. Finally, to provide further robustness and to protect from forged batteries that are spoofing approved batteries, the communication is accompanied by a Message Authentication Code[9] (MAC) based upon the session secret used. This not only provides data integrity but additionally provides authenticity, the goal that is trying to be achieved here with the battery.

Perhaps the bigger challenge for most manufacturers is that the carefully crafted security implementation between smartphone and battery can be programmed securely during manufacturing. After all, the integrity of the entire security implementation relies upon the secrets stored within the battery remaining secret. Thanks to solutions such as the Infineon OPTIGA™ Authenticate S, both the security implementation and the secrecy of the secrets are efficiently protected (Figure 2).

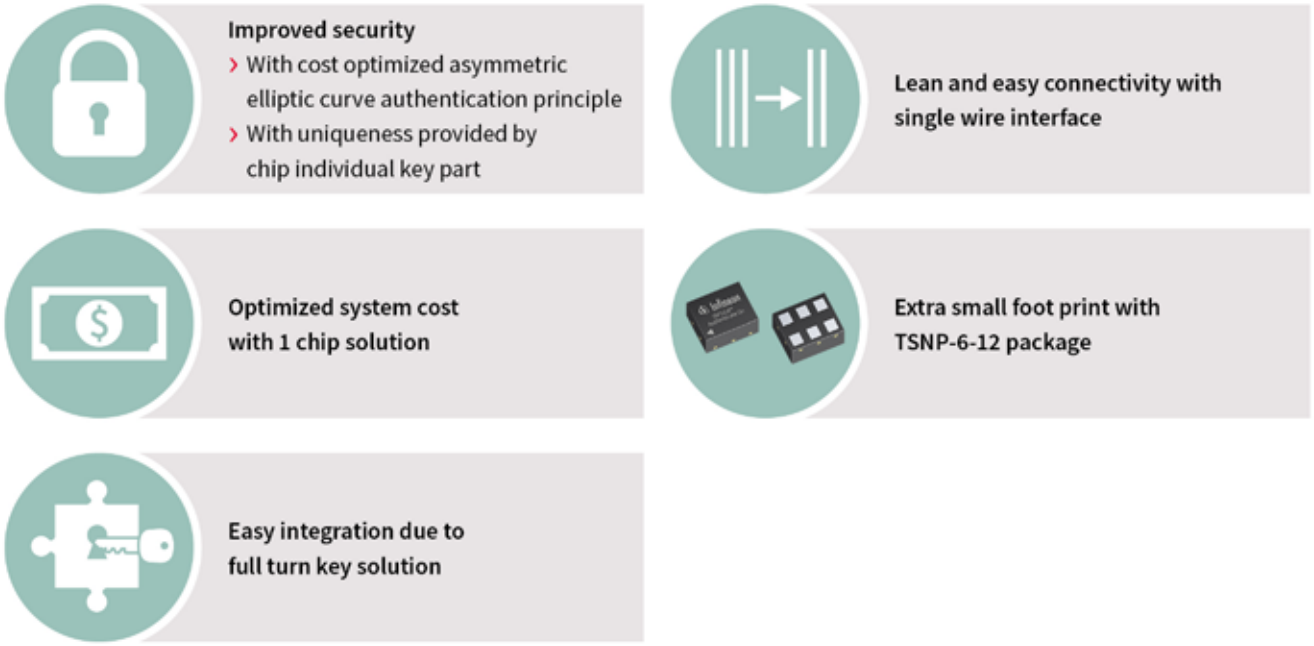


Figure 2: Easy to integrate, lean and simple connectivity, as well as extra small, make the OPTIGA™ Authenticate S the ideal solution for smartphone battery authentication.

9 en.wikipedia.org/wiki/Message_authentication_code

These silicon solutions are programmed in secured facilities that are also used for other secured devices, such as smartphone SIM cards. This means that manufacturers only need to order the number of devices they require for their assembly partners, pre-programmed with the certificates thus minimizing the risk that those certificates become compromised.

The OPTIGA™ Authenticate S Authentication IC lends itself well to battery authentication applications. Its tiny TSNP package measures just 1.5 mm × 1.5 mm with six pins. The implementation only requires three connections to the smartphone host: a ground, supply, 400kHz I^2C, and Single-Wire Interface (SWI). The SWI is a bidirectional, half-duplex, multi-slave interface, operating at up to 500 kbps. This provides plenty of scope for a wide range of implementation scenarios, should multiple batteries or other devices be added to the authentication chain. The device also provides a general-purpose output pin to enable external functionality based on the host authentication result or status of a lifespan counter.

To further simplify the interface implementation, the number of connections to the smartphone host can be reduced to two by indirectly supplying power via the SWI interface (Figure 3).

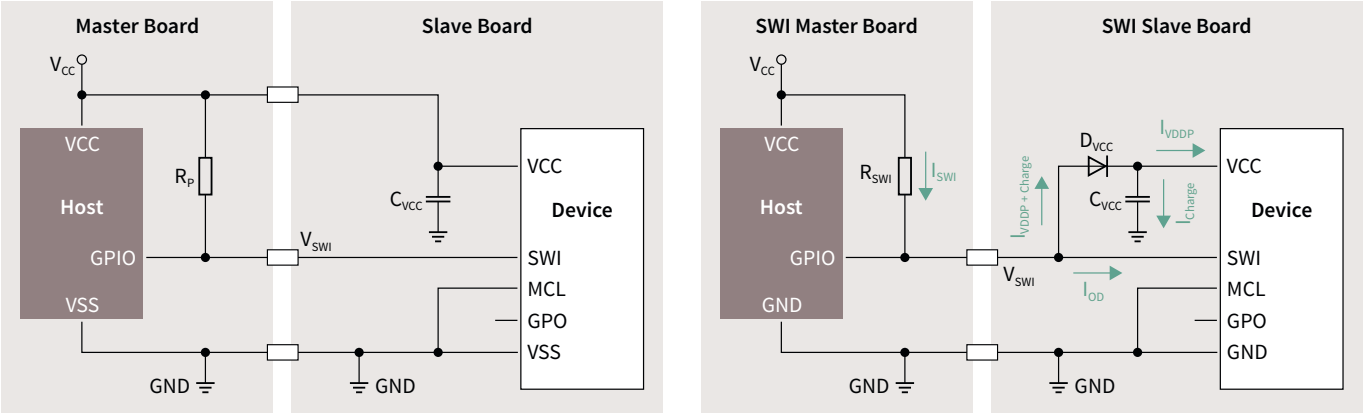


Figure 3: The OPTIGA™ Authenticate S only requires three connections to the host (left) but can be indirectly powered via the SWI communication interface (right,) if required.

The device also provides various non-volatile memory (NVM) space for application-specific requirements. It provides different NVM options to support 1024, 2048, and 5248 bits of user-mode data that may also be locked if required.

A robust level of security is afforded thanks to the 163-bit ECC engine, MAC function, 193-bit digital certificate (ODC), and 96-bit unique identifier (UID). It also makes use of Infineon's proprietary Physical Reverse Engineering 'PRE Technology', further adding to the security afforded. Four 32-bit Lifespan Indicators, read-only counters decremented using a single command, are also included. Software developers are provided with code for the host device, further simplifying the integration process.

Getting started

In order to undertake a full evaluation of devices such as the OPTIGA™ Authenticate S an application board is available. This features two devices and provides ample configuration flexibility. The interface can be easily connected to a logic analyzer tool, and both the direct and indirect power options are supported thanks to jumper options and the inclusion of a Schottky diode and a suitable capacitor (Figure 4).

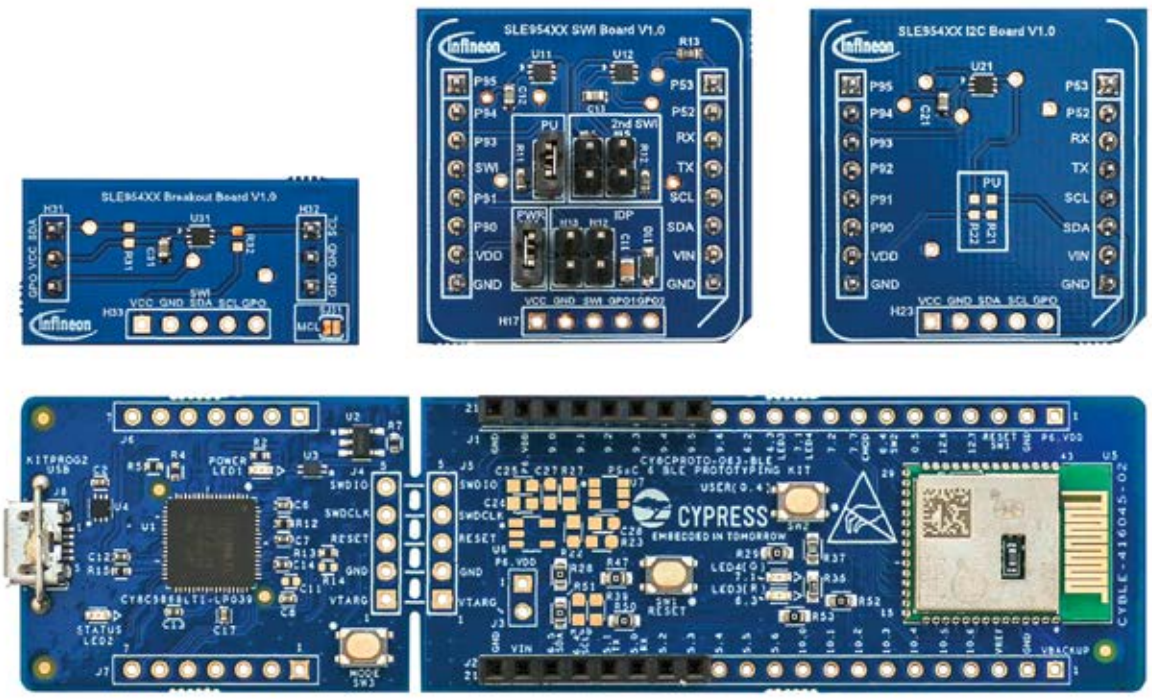
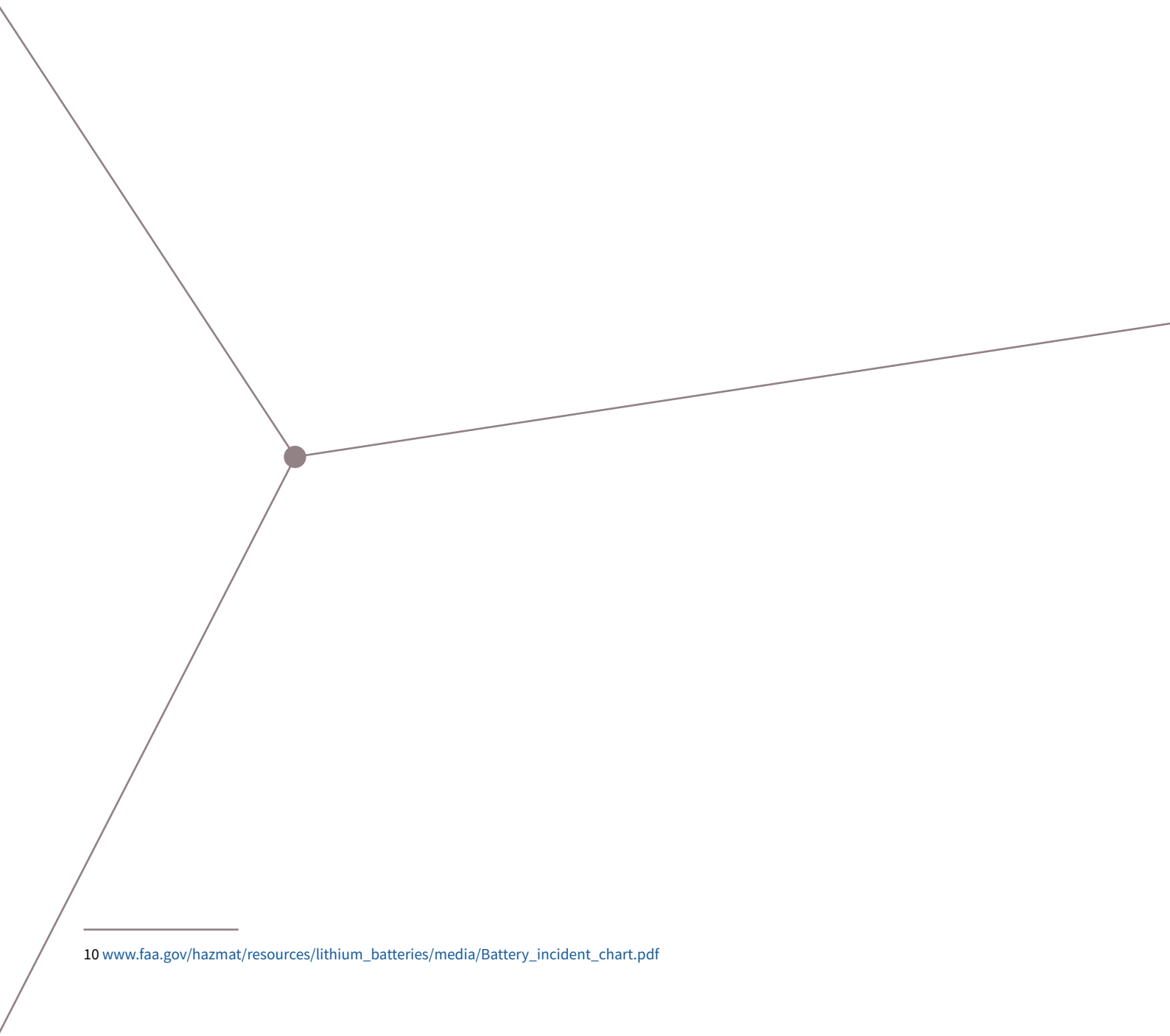


Figure 4: Evaluation of the OPTIGA™ Authenticate S is eased thanks to an evaluation board based on Infineon's PSoC™ 6, supported by a range of header options and a debugging interface.

Securing brand image

Room to differentiate in the smartphone market is diminishing rapidly, with cameras providing more pixels than we can use, and enviable levels of processor performance and memory capacity. However, one of smartphone users' core complaints remains battery life. The ability to perform a fast partial or full charge of today's high-capacity batteries is a real differentiator. However, even standard charging of Li-ion battery chemistries have proven to be a challenge and a few well-known brands have had their image bruised by large-scale failures of such batteries[10].

With consumers looking for the cheapest solution when replacing batteries, it is essential that a smartphone can check that the battery installed is an approved replacement that is capable of handling fast or rapid charging. While authentication is already included within the USB specifications, allowing the capability of the charger and cable to be checked, this is not implemented between the battery and smartphone. Solutions such as those provided by the OPTIGA™ Authenticate family provide robust, secure, and tiny silicon solutions, coupled with software that simplifies their evaluation and integration. This enables smartphone vendors to implement battery authentication, helping to shield consumers against potentially dangerous battery charging incidents while also protecting smartphone supplier's hard-won brand image.



10 www.faa.gov/hazmat/resources/lithium_batteries/media/Battery_incident_chart.pdf

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Document number:
Date: 11/2021

Please note!
This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.