Reducing manufacturing costs & complexity with CIRRENT™ Cloud ID security

www.infineon.com

Introduction

For all cloud-connected products, secured connectivity should be easy, flexible, and robust. But secured connectivity depends on building a cryptographically protected, authenticated, unique device identity (ID) into every Internet of Things (IoT) device. Configuring that identity is a tough problem to solve. A good solution provides an easy technique that works from the simplest IoT product, such as a lightbulb, to sensitive applications like health care or factories, video cameras, and more. A good solution also enables remote verification that the ID is valid to prevent unauthorized access from bad actors. The process needs to be easy not just for the consumer to use but also for the manufacturer to implement to avoid disruptive cost implications.

To address this problem, Infineon Technologies has developed a system that makes it easy (not disruptive) for manufacturers to obtain a unique identity during the manufacturing process for their various products. With the device ID located in a secured chip installed during production, the end product manufacturer can easily and securely access the cloud and all the associated services and licenses they desire and encrypt the communications channels between them. This white paper addresses the challenges of device security, current high-level solutions, and why CIRRENT™ Cloud ID is an ideal approach for IoT applications involving a variety of IoT devices.

Background on the technology for IoT and cloud connectivity

Infineon has a variety of hardware security products that come with a cryptographically secured, authenticated, unique identity, stored in a protected portion of the device to prevent malicious actors from obtaining access to it. That identity takes the form of a certificate – including a public key - and an associated private key installed in a secure environment. What has been added is the ability to easily link that ID later into the cloud for original equipment manufacturers (OEMs) and their customers.

Problem definition (secured connectivity – it’s not easy)

The unique ID problem applies to all IoT applications. Regardless of whether it is a smart home appliance or industrial equipment, anything that will be communicating with the cloud at some point requires a unique identity and the stronger the identity the better. This strong ID prevents supply chain issues such as cloning and grey market counterfeit devices as well as man-in-the-middle attacks from interfering with or changing the data and commands to the device. The device should be protected from being impersonated. While this primarily includes communication with the cloud, it can also include communications between devices, such as a temperature sensor talking to a thermostat to control the temperature in a home or office.

Subscription management is an especially desirable implementation of this type of device authentication since paid subscriptions are an important aspect of many manufacturers' business plan and product success. Examples include a system for moisture monitoring on a farm and an energy optimization service for a business or smart home. Companies must securely identify each product connecting to such a service to be able to check they are charging for all services that they are providing.

With the many types of IoT devices that exist, some are more mission critical than others. Some are more prone to attract the attention of attackers even to the point of government sponsored or criminal attacks with extremely serious consequences without the proper identification. If a counterfeiter can make a clone very cheaply and then sell them at a much lower price than the actual device, the manufacturer suffers from image loss, and the user may have to live with degraded quality with a knock-off component. In addition, subscription service and license providers risk significant revenue loss from the access of non-authorized products. Perhaps an even more damaging situation for a product company is for a counterfeit device to access their cloud and manipulate or extract data.

It may not appear to be that difficult to provision a single unique IoT device identity. When this provisioning needs to be integrated with an existing manufacturing process, the degree of difficulty increases significantly and becomes quite challenging. The manufacturing line cannot be interrupted and slowed to generate new public/private key pairs and consult with a certification authority to sign every product on the line. This is especially true when some IoT products could be as simple as a cloud connected light bulb. The boards in these products need the simplest soldering or other assembly processes to get the end product out of the factory in the most cost-effective manner. Simplification is essential.

Current solutions and challenges (moving towards secure cloud connectivity)

In history, device identity has often been established through serial numbers attached to the product. To read a serial number in the modern digital world, a digital serial number was installed within the device. This added an installation process to manufacturing, requiring the serial number to be entered during the manufacturing process with serious potential for errors. After this, the number can be sent to the cloud at log-in, but the number is very easy to copy and there is no counterfeit protection. It almost like having an open password that anyone can read and use.

Next a self-signed default certificate was used. In this case, when the device is powered on in the factory for its self-test, it makes itself a certificate. However, there is no proof of authenticity, since anyone can make a certificate. This is similar to a false driver's license that underage drinkers use to defeat age requirements. They are easy to make and not reliable or, in this case, secure. To overcome these limitations, a trusted authority must provide the certificate.

Table 1. The evolution towards improved cloud connectivity.

Timing	Device ID solution	Process	Security	Complexity
Before ICs	Serial number stickers	Physically attached stickers	None	Easy for OEM; hard for end user, especially in case of errors
Late 20th Century	Digital serial numbers	Installed in the factory on all devices	None	Easy
Next phase circa 2005	Unique PKI certificate and matching private key	Installed during device manufacturing on MCU	Better but still low	Complex
Next phase circa 2010	Unique PKI certificates and matching private key in a secure chip or a secure portion of a chip	Pre-installed in semiconductors	High	Complex
Next generation (CIRRENT™ Cloud ID)	Unique PKI certificates and matching private key in a secure chip or the secure portion of a chip	Pre-installed in semiconductors, available for cloud access	High	Easy

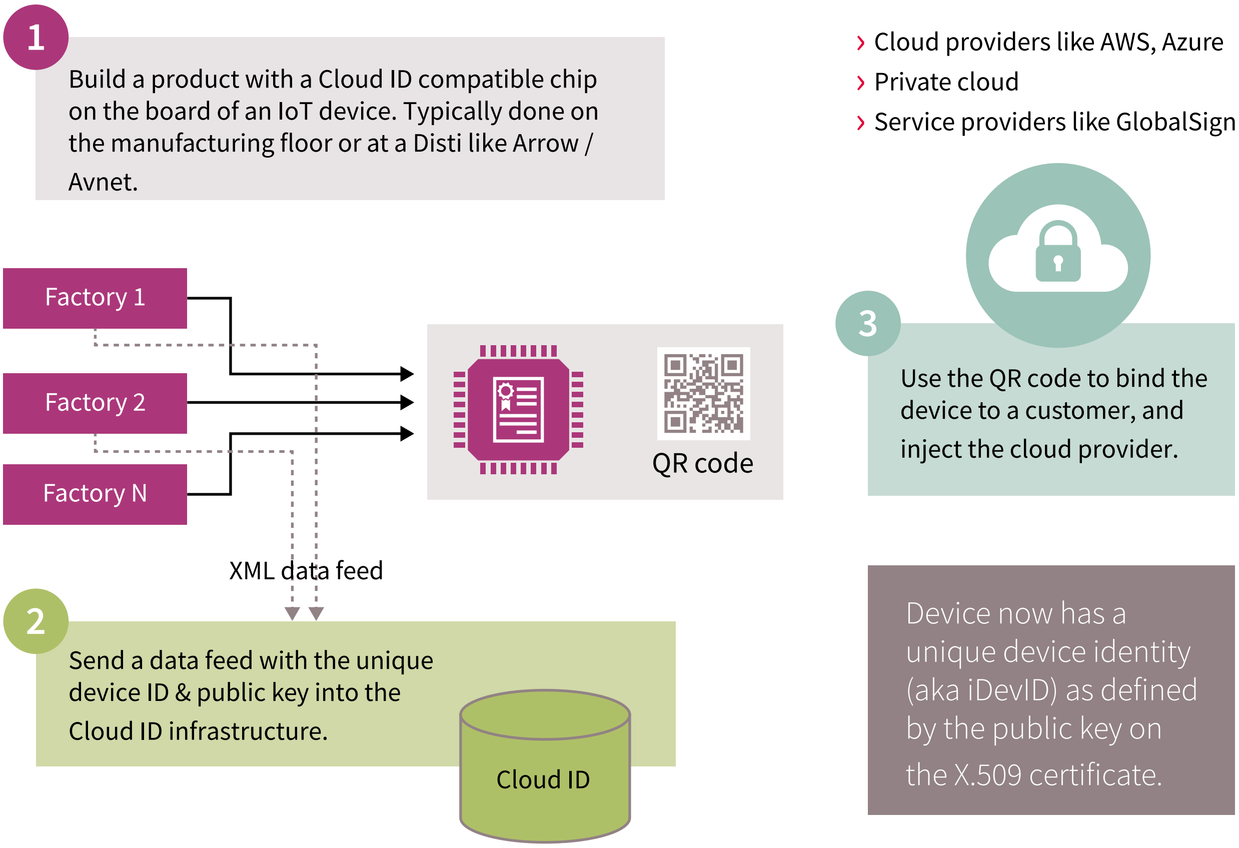
In the next improvement, a unique public-key infrastructure (PKI) certificate and matching private key are installed during device manufacturing. As noted previously, this is quite disruptive to an existing manufacturing process since it requires each device to be handled to get the certificate inserted or read. Generating the key pairs and generating the certificate are difficult and not very effective, especially if the manufacturing line is not very secure for the IoT device.

Another similar approach involves unique PKI certificates and matching private key that are pre-installed in semiconductors. In this case, the security chip comes from the semiconductor factory with these items. The OEM does not have to do anything special in its manufacturing process. However, this method makes it hard to determine which security chip was installed in a particular end product because the manufacturing staff must stop the line to read this information, adding another manual process. With CIRRENT™ Cloud ID, this step is not necessary.

How CIRRENT™ Cloud ID eases device ID

With an Infineon cryptographically unique security chip that supports CIRRENT™ Cloud ID, you get a device presence in the cloud that can be used to provision it in your cloud. Here's how it works. Each reel of chips has a batch identifier (Batch ID), which is noted in a QR code inside the box that contains the reel. A manifest listing the ID certificates for that Batch ID is available to download on the CIRRENT™ Cloud ID service. When the reel arrives and is ready for installation (installing the security chips onto a board), the OEM or their contract manufacturer can scan the QR code and use the CIRRENT™ Cloud ID service's web-based console to retrieve the list of certificates that are included in the reel of security chips.

As shown in Figure 1, mapping from the QR code into one or more sets of chips is performed by the Batch ID where there is no limitation on the number of chips (it could be 1:1 or 1:N).



Build a product with a Cloud ID compatible chip on the board of an IoT device. Typically done on the manufacturing floor or at a Disti like Arrow / Avnet.

- Cloud providers like AWS, Azure
- Private cloud
- Service providers like GlobalSign

Use the QR code to bind the device to a customer, and inject the cloud provider.

Send a data feed with the unique device ID & public key into the Cloud ID infrastructure.

Device now has a unique device identity (aka iDevID) as defined by the public key on the X.509 certificate.

Figure 1. Cloud ID simplifies the manufacturing of IoT Devices without the need for personalization.

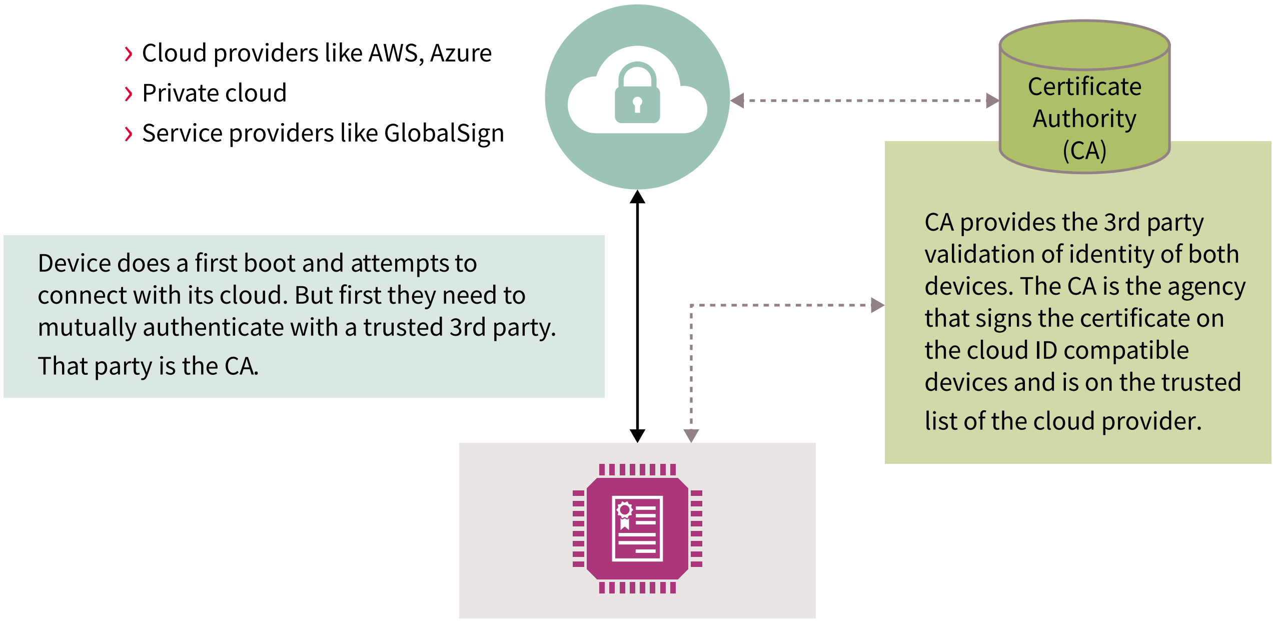
The OEM can import those certificates into a cloud like Amazon Web Services (AWS) and others (using Cloud to Cloud APIs), or they can use their own cloud, or they can interface with a certificate authority to verify an authorized device. Once the chip is soldered to the board and it shows up in the field, when the end user connects to cloud they are using, such as AWS, the service has already been preconfigured by the OEM supplier to expect a communication from the end product.

Why the cloud ID service is useful to product manufacturers

CIRRENT™ Cloud ID uses a high security approach that has been developed for IoT device identity, where a security IC with unique PKI certificates and matching private key are all handled by the semiconductor manufacturer in secured fabs. However, the addition of a Batch ID and the CIRRENT™ Cloud ID service keeps OEM device manufacturing costs low while uploading all of the device certificates to the cloud.

When the OEM's customer buys the device and boots it up, the customer experience is simple. The device communicates with the cloud and the cloud identifies and authenticates the product via its unique PKI certificates and matching private key. This feature allows the device to be recognized as a particular OEM product, such as a dish washer. At this point, no further steps are required, such as installing new certificates into the end product or gathering the certificates from the device. The QR code included on the reel has already identified the certificates and provisioned them in the cloud. If custom certificates are desired, the device can inform a Certification Authority (CA) when it boots up and use the certificates uploaded to the cloud to request a certificate designed for this particular device. That new certificate can be used to access software, services, and other options that are restricted to this device.

As shown in Figure 2, the CA provides three-way authentication between the device and the product cloud to establish trust between both parties.



- Cloud providers like AWS, Azure
- Private cloud
- Service providers like GlobalSign

Certificate Authority (CA)

CA provides the 3rd party validation of identity of both devices. The CA is the agency that signs the certificate on the cloud ID compatible devices and is on the trusted list of the cloud provider.

Device does a first boot and attempts to connect with its cloud. But first they need to mutually authenticate with a trusted 3rd party. That party is the CA.

Figure 2. The device's unique ID is in the field at its birth.

The advantages of the CIRRENT™ Cloud ID approach include:

- Easy to verify ID and hard to copy
- Easy to manufacture devices
- Easy to integrate with clouds
- Easy to add device-specific certificates, if desired

With these advantages, CIRRENT™ Cloud ID provides the security that OEMs, and their customers need to safely and uniquely ID a specific product and authorize its connectivity to the cloud.

Simplifying IoT/cloud security

To summarize, today's cloud-connected IoT devices require a unique identity and installing the identity into a secure device at the time of manufacture provides a high level of security for the lifetime of the end product. However, implementing this identity has been a challenge.

To solve the identity problem, Infineon Technologies CIRRENT™ Cloud ID automates cloud provisioning of device certificates during the manufacturing process. This unique approach to device-to-cloud authentication, makes identification easier, more cost effective, and more secure. Compared to a software only certificate, CIRRENT™ Cloud ID delivers greater security without requiring expensive an on-site CA and network infrastructure.

References

CIRRENT™ Cloud ID, https://documentation.infineon.com/html/cirrent-support-documentation/en/latest/cirrent-could-id.html

Quick Start Guide: Cloud ID Virtual Developer Kit, https://documentation.infineon.com/html/cirrent-support-documentation/en/latest/cid/quick-start-cloud-id-virtual-dev-kit.html

www.infineon.com

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Date: 04 / 2022

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.