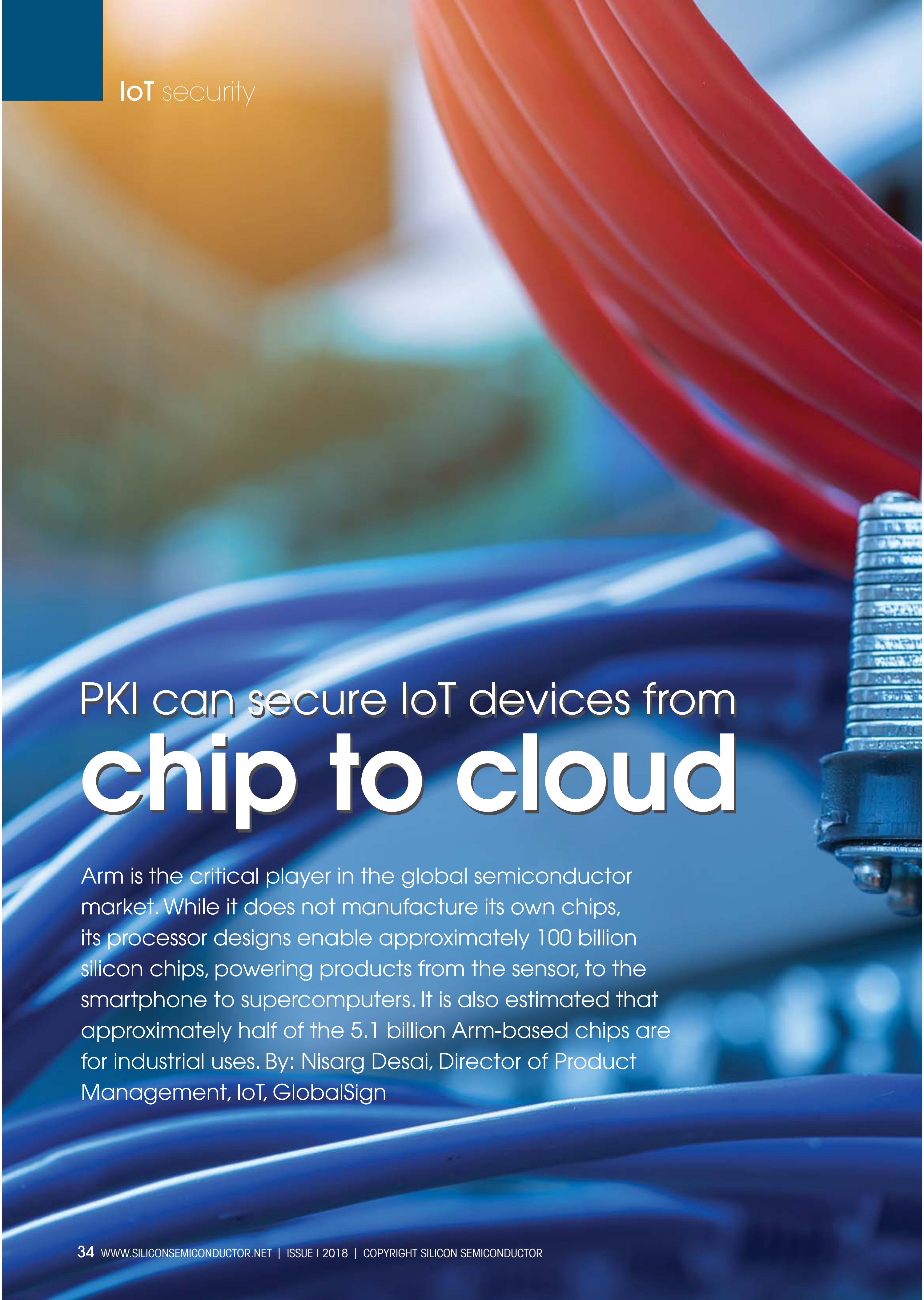


PKI can secure IoT devices from chip to cloud

Arm is the critical player in the global semiconductor market. While it does not manufacture its own chips, its processor designs enable approximately 100 billion silicon chips, powering products from the sensor, to the smartphone to supercomputers. It is also estimated that approximately half of the 5.1 billion Arm-based chips are for industrial uses. By: Nisarg Desai, Director of Product Management, IoT, GlobalSign

LIKE ANY semiconductor company, Arm (now owned by Japan's SoftBank) is very much focused on security, and has a company-wide mandate to ensure secure products across the board from the chip up to the cloud.

Arm recently announced its 'Platform Security Architecture' initiative, aimed at providing security guidance for IoT device developers. It has four recommended security tenets, one of which is certificate-based authentication, a market that is expected to grow in the coming years. This is not a surprise given the current trends reported by The Ponemon Institute, one of the world's top providers of research on the information security industry. Its 2017 Public Key Infrastructure (PKI) Global Trends Study, which gathered input from more than 1,500 IT security practitioners worldwide to determine where PKI is heading, found that 43 percent of IoT devices will adopt digital certificates for authentication within the next two years.

GlobalSign has long been a provider of PKI-based solutions, because it is time-tested, open standards-based, easily implemented and a widely accepted technology. PKI is even more relevant in this case, because it lends itself very well to IoT devices. It can be implemented in a relatively lightweight fashion on different classes of devices. Most IoT devices, by definition, are data gatherers, data transmitters and sometimes, data processors. Thus, secure communication is very important to IoT devices, and PKI is a simple and cost-effective way to achieve this. Asymmetric cryptography, which forms the basis of PKI, is mathematically and empirically proven to be an effective means of providing secure distribution of encrypted messages to targeted senders.

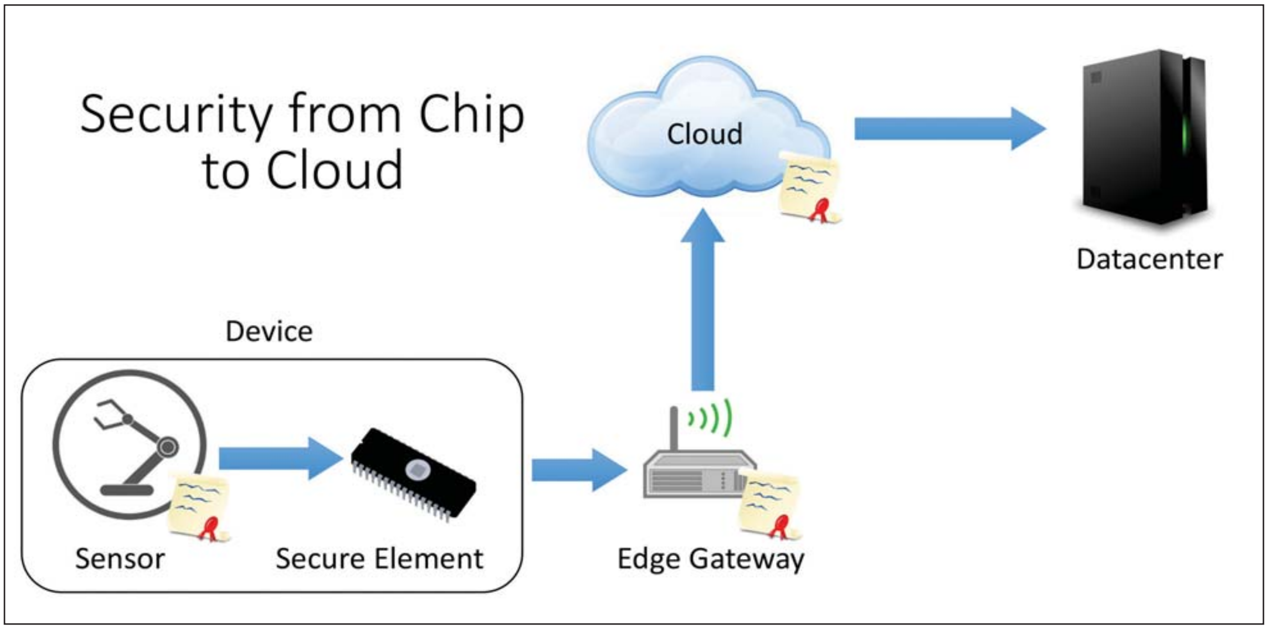
Security chips

Chip enabled and accelerated functions form the bedrock of most secure software and hardware implementations today. For example, the core identity of any device is stored in something called a Secure Element, a chip that forms the root-of-trust for a device. It serves as a Trust Anchor, which then enables other security functions such as Secure Boot and Remote Attestation. Many of these functions require a great deal of processing power – hence dedicated cryptographic chips accelerate these operations, making them faster and/or enabling them to consume less power. Quite a few of these chips are based on Arm designs. It is important to understand there are various options to adding a secure element. A Trusted Platform Module (TPM) chip is a crypto co-processor that sits alongside the primary processor and requires a redesign of the board to allow its integration. A more novel, equally secure but much more cost-effective option is to use a (Physically Unclonable Function (PUF). There are various other options, but discussing these in detail is out of scope of this article.

PKI for IoT devices

PKI's roles, policies, and procedures are needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. PKI has been relied upon since the 1970's and was first used in technologies such as e-signatures in the 1990's. Today, it is viewed as one of the most reliable ways to secure IoT devices.

All IoT devices require a strong identity and need to prove that they are who they claim to be, and not something else. This identity should be universal and easy to verify for the communicating party. Soon, they will



PKI enables 'lightweight' IoT security from chip to cloud. Image courtesy of GlobalSign.

even generate their own identity and store it safely, directly as a result of PKI's unique mathematical capabilities. Also coming soon are IoT devices that will each have their own individual and unique certificate to prove their trustworthiness. By using PKI in this fashion, IoT devices will be more trustworthy, limiting the chances of unauthorized access.

Chip to cloud security

As alluded to earlier, Arm has a directive to ensure security across the board, from its chips, through their IoT stack, and up to the cloud embedded onto a chip. Arm takes its own low power Cortex-M product family and adds support for its open-source Arm Mbed OS embedded operating system. This combination is easy to use and to configure out of the box, making it ideal for small scale developers designing an IoT device and are at the stage where they are ready to begin creating design applications – they can simply use Mbed OS as their embedded operating system.

The Arm Mbed family also includes a cloud platform as a service, called Mbed Cloud. Since most IoT use cases today involve collecting sensor data from an IoT device on the edge and then transmitting it up to a cloud application for further processing, this cloud service is very useful. Mbed OS can natively integrate and connect to Mbed Cloud. Now, Transport Layer Security (TLS) is the protocol of choice for most device to cloud connections. This requires the use of digital certificates.

What is significant about Mbed Cloud is that it supports a "bring your own Certificate Authority (CA) program." You can have a third-party CA create a dedicated PKI hierarchy and upload the Root CA Certificate to Mbed Cloud. This enables certificate-based authentication to automatically accept connection requests from all your devices that have a certificate issued from that particular hierarchy.

Getting started

A very important first step for IoT device developers is enabling security across the vertical IoT platform stack – right from the end device or sensor node, through the edge and fog layers, up to the cloud-platform and underlying data and application infrastructure. This can be achieved by ensuring that, as data is passed through these layers, each step in the chain is verifying it is communicating a party's identity and authority, while ensuring data privacy and integrity. This is attainable through PKI.

For those not intimately familiar with PKI, it is a commonly used approach to encryption and authentication. The architecture provides a greater level of confidence for sharing information electronically. First, we can look at how devices can ensure integrity within themselves. One way to achieve this is Secure Boot. A Digital Signing Service can be used to sign and compute the hash of any firmware, before loading onto the device. The public key used to sign the firmware is stored on the device, in non-erasable memory. Whenever the device boots up, a hash of the bootloader (the process of applying an algorithm to generate a small string from a larger file that can later be used to verify the file's integrity) is generated and signed by the public key. Now if we can trust this public key, and verify this signed record to be accurate, then we have proved that the bootloader (and anything else that was checked) is genuine. If we then send this signed report or file to a remote server, periodically, to prove that the bootloader is genuine, we have remote attestation.

Now that we have established a device and its code are genuine, we can move onto secure communications outside it. A device can present its identity certificate to the edge router or gateway it is communicating with. The gateway can then inspect and validate the certificate, and following that, accept the incoming data packet. Now the edge gateway can establish a (TLS) connection with the cloud platform server and prove its identity to the server via its own certificate. Conversely, the edge gateway can also require and verify the server's identity certificate thus enabling a mutual TLS connection.

This bi-directional verification provides security against eavesdropping, injection and other Man-in-the-Middle (MITM) attacks.
Device certificates can also support role-based authorization. Since the certificate cannot be modified once issued by a CA, one can insert specific identifier fields (or roles) that this device is allowed to assume. Now, we can not only verify the source of data, but also whether a device is allowed to transmit or accept that piece of data.

These two basic security tenets – authentication and authorization – can easily be implemented by device designers by simply integrating a secure certificate provisioning step into their device manufacturing process. This then easily extends to stricter security techniques like secure boot and firmware attestation. Some CA's, including GlobalSign, have tools and platforms available to help achieve these security goals. One example of this would be our new device enrollment service. All of the suggested cryptographic techniques mentioned here utilize asymmetric cryptography as a basic building block. Device certificates, publicly trusted roots and code signing, are all implemented using PKI.

By allowing support for third party CAs, ARM has effectively and easily enabled adopters of Mbed a plethora of options to implement device-based security features.

Conclusion

This is an exciting time for PKI, and it is likely that many organizations will embrace it as a first step to securing their IoT devices. Identity is the foundation of security, and secure authentication and authorization the first two targets to accomplish – PKI seamlessly enables this. Device designers and manufacturers relying on PKI will find that this tried-and-true technology will enable them to successfully launch secure applications and products such as the one that are described, opening up new windows of possibility to them. With both silicon vendors, embedded OS makers and cloud platform providers natively supporting, and in some cases requiring, a PKI-based credential, IoT makers should now find it both easy and cost-effective to include security as part of their product design. This will ultimately lead to a more secure Internet of Things for all of us.

Real-world application in the retail industry

THERE are an increasing number of projects being developed using the approach outlined above. One such example is an effort by GlobalSign, where we are leveraging ARM's Mbed OS and Mbed Cloud for a project on behalf of a Japanese bookseller.

The project involves tracking the sales of new books with hidden sensors that are placed on the backside of an 8 ½ x11 polycarbonate board also called a plaque. The sensor tracking the books in the plaque's proximity runs Mbed OS on a Cortex-M based chip. Each chip uses a digital certificate provided by GlobalSign. That certificate then talks to Mbed Cloud, notifying that an event – in this case, a book being picked up from a stack – has occurred. In addition, a mobile app is available that enables users to view the number of books that were picked-up or sold. On the front of the plaque is an E-Ink display that shows details of the book such as the price, a description of the contents, etc. This can also be dynamically updated via the app.

A certificate identifies the sensor and display to prove the source of the data. When someone walks over to the table and picks up a book, a near-field proximity sensor is triggered which detects the presence (or absence) of an obstruction. Based on a configured image map, the application can detect that someone came near it, picked up a book, then left, leaving the book stack shorter. The sensor will then issue a notification via Mbed OS to be sent to Mbed Cloud. The bookseller can use the app to track the number of books picked up.

Why do we need to implement a security solution for such a benign use-case, and why does it have to be PKI-based? First, the bookseller might be integrating an inventory system into this workflow. Whenever a book is picked-up (without being replaced) an automatic counter decreases the available stock. Thus, we need to ensure the accuracy and integrity of this data. In addition, there may be several books and stations in a store, thus the identity of the plaque and reporter of the information are critical. Second, PKI is an easy way to implement this kind of a solution, and is what was used for the project. However, it is not the only way. Since Mbed OS has a low resource footprint, and Cortex-M chips are very power efficient, low-powered battery operated devices can be used to enable this application, without compromising security.

At this time, it is expected that approximately 100 plaques will be built by late spring 2018 and subsequently deployed. Once this pilot project is completed, it may be expanded to all of the bookseller's locations throughout Japan.