Case Study

LEVERAGING THE SIM TO SECURE IoT SERVICES

gsma.com/IoTSecurity

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: @GSMA.

About the GSMA Internet of Things Programme

The GSMA's Internet of Things Programme is an industry initiative focused on:

- COVERAGE of machine friendly, cost effective networks to deliver global and universal benefits
- CAPABILITY to capture higher value services beyond connectivity, at scale
- CYBERSECURITY to enable a trusted IoT where security is embedded from the beginning, at every stage of the IoT value chain developing key enablers, facilitating industry collaboration and supporting network optimisation, the Internet of Things Programme is enabling consumers and businesses to harness a host of rich new services, connected by intelligent and secure mobile networks.

Visit gsma.com/iot to find out more.

Contents

Executive Summary

The SIM cards used by mobile network operators to authenticate devices accessing their networks and services can also be used to secure Internet of Things (IoT) applications. This report highlights how mobile operators in the Americas, Asia and Europe are developing and deploying SIM-based IoT security services to support IoT customers.

TELEFÓNICA AND AMAZON WEB SERVICES – CLOSE TO COMMERCIALISATION

At GSMA MWC Barcelona in February 2018, Telefónica demonstrated the secure provisioning and storage of a public key infrastructure (PKI) certificate on a SIM card in a smart meter. Using a custom application, the meter was connected via Telefónica's 3G network to the Amazon Web Services (AWS) IoT platform. Once it had been authenticated using the PKI certificate, the smart meter could send data to the AWS IoT platform about the electricity being consumed by the nearby light bulb. Telefónica and AWS are now partnering to provide secure end-to-end solutions that can facilitate IoT deployments at scale. For Telefónica, using the SIM card to securely provision and store credentials for IoT device authentication with an IoT platform is a way to generate more value from its existing assets. "The secure processes are already in place, so it is a question of extending those processes to new use cases based on the IoT," says Vicente Segura, Head of IoT Security at Telefónica. "You simply have to connect those devices to the mobile network."

TAIWAN MOBILE AND ABLE DEVICE DEMO PROOF OF CONCEPT

At GSMA MWC Shanghai in June 2018, Taiwan Mobile and Able Device demonstrated how a SIM-based solution can be used to update the passcodes on smart meters once they have been deployed in the field. This use case is designed to address the issue whereby many IoT devices leave the factory protected only by the default passcode, as this can be the most efficient way to manufacture these products. Now Able Device and Taiwan Mobile are commercialising the solution. "The next step is to develop distinct security solutions for different IoT applications and implement a proof of concept with individual customers," says Hermann Huang, Division Head of the IoT and Platform Service Division at Taiwan Mobile. "We should have a commercial proposition in 2019. This is a good opportunity for Taiwan Mobile, but the right business model is a question that the ecosystem needs to think about."

CHINA UNICOM AND TENCENT SUPPLY SIM-BASED SECURITY

In China, Internet platform Tencent is using China Unicom's SIM cards to authenticate smart watches and other IoT devices for its customers. The solution is designed to protect devices against unauthorised access and so-called "man-in-the-middle" attacks, which seek to intercept data transmissions. Unicom says this approach is both cost-effective and straightforward to implement, as no changes are required for the IoT devices, their modules, and chips. "For those enterprises that do not have a particularly high security requirement, but need to encrypt data, this simplified approach can meet the basic security requirements of these enterprises," says Fuzhang Wu. "The whole solution is very simple, very efficient and is low cost and has low power consumption."

AT&T AND G+D MOBILE SECURITY PREPARE TO SERVE FIRST CUSTOMERS

The US mobile operator AT&T and SIM security specialist G+D Mobile Security (G+D) have developed a solution to securely provision an IoT device's identity and credentials for secure authentication to cloud platforms and applications. The two companies plan to take their proof of concept into production before the end of 2018. Senthil Ramakrishnan, lead member of the technical staff at AT&T, says three AT&T customers are already gearing up to use the solution, including a large machinery manufacturer, an automotive OEM and a cloud service provider. "We also intend to use it for internal products, such as our end-to-end asset tracking and fleet management solutions," he adds. "It will be deployed in several end-to-end solutions we are deploying."

Introduction

Mobile network operators use SIM Cards (UICC cards as defined by 3GPP/ETSI) to authenticate devices accessing their networks and services. SIM cards can also support additional security capabilities that can be harnessed by Internet of Things (IoT) applications as explained in the GSMA report, Solutions to Enhance IoT Security Using SIM Cards[1].

That report outlines how a SIM card can provide a secure 'root of trust' to provision and store digital certificates and other kinds of security credentials, such as passwords. These credentials can be used to identify and authenticate an IoT device to interact with a server-side application or IoT platform. A mobile operator can use its existing provisioning infrastructure as a secure channel through which to cost-effectively install, validate and update the security credentials safely housed on SIM cards.

This paper outlines how mobile operators in the Americas, Asia and Europe are developing and deploying SIM-based IoT security services to support IoT customers. The case studies outlined in this report describe solutions developed by the following partnerships:

- Telefónica and Amazon Web Services
- Taiwan Mobile and Able Device
- China Unicom and Tencent
- AT&T and G+D Mobile Security

The intended audiences of this report include:

- IoT service providers (e.g. automakers, utilities, smart cities, etc.) who wish to understand how SIM-based security technology can be used to enhance the security of their services
- Mobile network operators who wish to offer enhanced SIM-based IoT authentication services to IoT service providers
- Technology vendors who supply mobile network operators and IoT service providers with security technologies

[1] https://www.gsma.com/iot/solutions-enhance-iot-authentication-using-sim-cards-uicc/

Case Studies

In each of the four case studies described in this paper, mobile operators and their partners are employing SIM cards to securely provision and store credentials that can be used to authenticate an IoT device with an application or an IoT platform. In many IoT deployments, these credentials will be public key infrastructure (PKI) certificates, which use a combination of public and private keys to encrypt sensitive data travelling between the device and the IoT platform or application.

The security of these certificate-based systems relies on the secrecy of the private key that is provisioned and stored within the device. Ideally, the private-public key pair will be generated within a secure part of the device itself, but many present-day IoT devices lack a secure processor that can perform that task. If private keys have to be generated externally to the devices, then a secure process needs to be established to provision them in the devices.

Mobile operators and their partners are demonstrating how their SIM cards and supporting SIM infrastructure can address this challenge by supporting strong, standards-based cryptography that can be used to provision certificates and generate key pairs either externally or on-board the SIM. A SIM card can perform cryptographic operations, such as authentication, encryption/decryption and digital signatures in a tamper-resistant manner.

TELEFÓNICA AND AMAZON WEB SERVICES – CLOSE TO COMMERCIALISATION

At MWC Barcelona in February 2018, Telefónica IoT demonstrated the secure provisioning and storage of a PKI certificate on a SIM card in a smart meter. Telefónica developed a custom application in partnership with Ikerlan to connect the electricity meter via Telefónica's 3G network to the Amazon Web Services (AWS) IoT platform. Once it had been authenticated, the smart meter could start sending data to the AWS IoT platform about the electricity being consumed by the nearby light bulb (see Figure 1).

Having worked together to develop the prototype solution demonstrated in Barcelona, Telefónica IoT and AWS are partnering to provide end-to-end solutions that can facilitate IoT deployments at scale. For IoT applications, AWS requires certificates for mutual authentication and TLS 1.2 to encrypt the communication.

Figure 1: The prototype solution demonstrated by Telefónica IoT and AWS at MWC Barcelona

THE CUSTOMER PAIN

Device credentials set up at IoT scale

Provisioning different credentials to a large number of devices using a secure bootstrapping process to avoid manual provisioning or insecure configurations.

THE SOLUTION

Cellular identity and standard SIM OTA

Network credentials broker able to identify the SIM card and to send OTA the corresponding X.509 certificate to the SIM card using standard 3GPP SIM RFM capabilities.

Source: Telefónica

For the proof of concept in Barcelona, Telefónica employed a credential broker component in the network. "Once the device is authenticated at the network level, then we can check that the device can be connected to the AWS IoT platform," explains Vicente Segura, Head of IoT Security at Telefónica. "If that is the case, we can generate an AWS certificate and send it to the SIM card of that device. We can do it through a HTTPs connection or we can do it on the OTA (over-the-air) platform. Once the device receives a certificate, a small application in the SIM uses the certificate to authenticate it with the AWS IoT platform."

Upon receiving a request from a device, the credential broker issues a device identity in the AWS IoT platform. It then generates a private/public key pair and a certificate signing request (CSR), requests the AWS IoT platform to sign the CSR, links the certificate to the device's digital identity and, finally, sends the credentials OTA to the SIM using binary SMS. A SIM applet is then used to handle the SMS and to store the credentials in a security domain within the SIM. This certificate could, for example, be used to establish end-to-end security between the AWS IoT platform and the security domain within the SIM card using secure channel protocols, such as the SCP11 protocol defined by GlobalPlatform®.

Cutting costs by harnessing existing assets

Up to now, securely generating such certificates and distributing them to a large number of IoT devices before they are deployed in the field has been an expensive manual exercise. "We detected the need to simplify the distribution of the credentials," says Vicente Segura. "We have defined a mechanism to authenticate them when they connect to the IoT platform. To do it manually has a cost, which can be huge, if there are many devices involved."

For Telefónica, using the SIM card to securely store credentials for device authentication with an IoT platform is a way to generate more value from its existing assets. "The secure processes are already in place, so it is a question of extending those processes to new use cases based on the IoT," says Vicente Segura. "You simply have to connect those devices to the mobile network."

Although Telefónica hasn't yet decided how to monetise the service, it is confident that many enterprise customers will be prepared to pay to secure their IoT solutions in this way. "If you want to deploy credentials on a device-by-device basis, that takes time and money, maybe a euro per device," notes Vicente Segura. "So the

> "Once the device receives a certificate, a small application in the SIM uses the certificate to authenticate it with the AWS IoT platform"
>
> **Vicente Segura,** Head of IoT Security at Telefónica

model could be that [the operator] receives some revenue for each credential deployed via the SIM card, similar to existing digital certificate charging models." However, he cautions that not all IoT deployments will need this level of security. "This approach won't make sense for all use cases. For example, for use cases where temperature and humidity sensors are involved, maybe the security requirements are not so demanding and other more cost-effective solutions could fit better."

Vicente Segura urges other mobile operators to move in the same direction as Telefónica, implementing SIM-based solutions in a consistent way that will help the IoT ecosystem benefit from economies of scale and interoperability. "We are competing as mobile operators, but we are on the same ship regarding the IoT," he says. "We compete with other forms of connectivity and protocols. We need to develop mechanisms like this to provide more benefits and give customers reasons to choose mobile networks and SIM cards to enable the IoT."

Having shown a proof of concept at MWC Barcelona, Telefónica is close to launching a commercial solution. "We can already offer the solution to customers that are interested on a project-by-project basis," explains Vicente Segura. "The next step is to industrialise this proof of concept, integrate it as a service that can be offered automatically to any customer. We are working on that. We are currently looking for the demand for the service in the market. We want to industrialise this in 2019." However, Vicente Segura notes the solution will need to be adapted to the requirements of each vertical sector.

Telefónica will provide the SIM cards and the network components, and is working with AWS to integrate it with its IoT platform using application programming interfaces (APIs) to generate the necessary PKI certificates. "Mobile networks are well-spread all over the world and SIM cards are, in many cases, a simple and secure way to provide connectivity to a device, all the while, leveraging all the security mechanisms that the operators put on their mobile assets," says Rodrigo Merino, IoT Partner Solution Architect at AWS. "We are also collaborating with mobile operators for additional security features in scenarios such as IMEI change, detection of "chatty" devices, authentication failures, etc."

> "The next step is to industrialise this proof of concept, integrate it as a service that can be offered automatically to any customer"
>
> **Vicente Segura,** Head of IoT Security at Telefónica

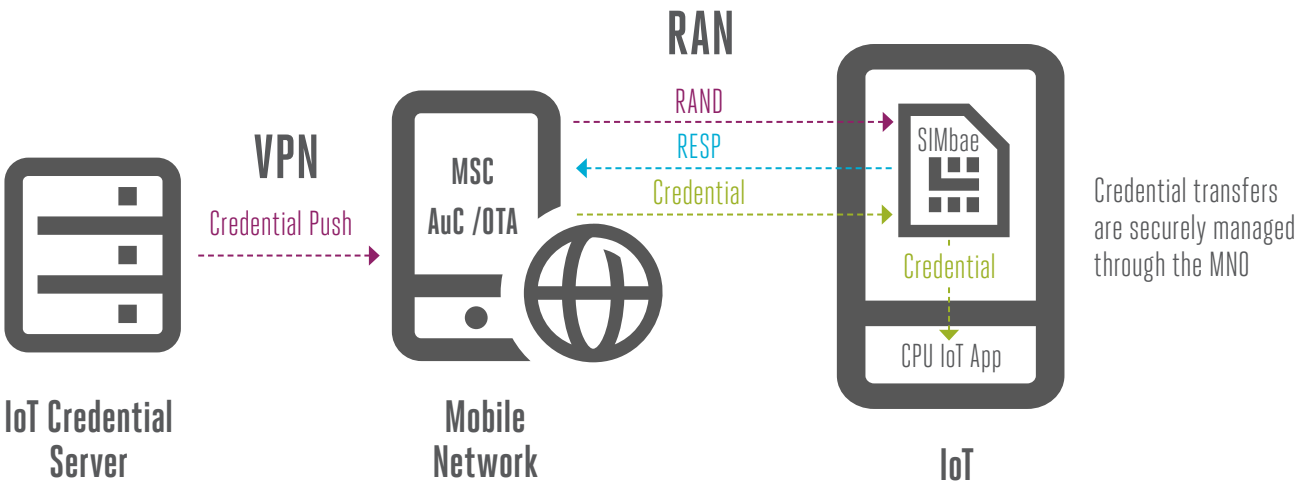
TAIWAN MOBILE AND ABLE DEVICE DEMO PROOF OF CONCEPT

Taiwan Mobile and Able Device put a spotlight on SIM-based security for the IoT at MWC Shanghai in June 2018. The two companies demonstrated how a SIM-based solution can be used to update the passcodes on smart meters once they have been deployed in the field. This use case is designed to address the issue whereby many IoT devices leave the factory protected only by a default passcode, as this can be the most efficient way to manufacture these products.

Hermann Huang, the division head of the IoT and Platform Service Division at Taiwan Mobile, says a SIM-based approach is both straightforward and low cost, as "there is no complicated integration with a device management platform."

The demo in Shanghai employed Able Device's SIMbae Credential Exchange Manager (S-CEM), which can use a VPN to deliver credentials to the mobile operator's secure infrastructure (Figure 2). For the demo, S-CEM delivered an updated password to the smart meter using a binary-encoded SMS Class 2, which can only be sent from a trusted source. The updated passcode was transferred from the meter's baseband radio via the single wire protocol to the SIMbae applet on the SIM card, which read it before passing it off to the IoT application in the device.

Figure 2: Using a VPN and secure SMS to update the authentication credentials on IoT devices



Source: Able Device

Taiwan Mobile provided Able Device with the keys it needed to add the SIMbae applet to the SIM cards used in the meters. The applet keeps the SIM awake, so it can read and, if necessary, store a password or another security credential. "The credential can be pushed or pulled and there is no need for unique network elements," says Roger Dewey, CEO and founder of Able Device. "Once you have the executable code, it is almost unhackable. Even if you had a supercomputer, you could only hack each device one at a time and at great effort."

For Able Device, the SIM card is the best mechanism through which to manage this process. "The SIM is a very secure element, which has processing on it, and this is under-exploited," notes Roger Dewey. "There is no need for a separate security chip, as you can use the SIM card. Moreover, it is a global standard. More than 10 billion SIM cards have been issued to date."

S-CEM is designed to support the mass deployment of any connected device with a processor, including industrial and consumer IoT devices, connected vehicles and IT equipment such as PCs, laptops and tablets. At MWC Shanghai, Able Device also showed how a SIM-based solution can be used to remotely and securely control a traffic light.

Now Able Device and Taiwan Mobile are moving towards commercialising the solution. "The customers who have seen the demo think the idea is a good one," says Hermann Huang. "The next step is to develop distinct security solutions for different IoT applications and implement a proof of concept with individual customers. We should have a commercial proposition in 2019. This is a good opportunity for Taiwan Mobile, but the right business model is a question that the ecosystem needs to think about."

In particular, mobile operators need to consider how they can achieve economies of scale. "Opening up the SIM is not something that the operator generally does, so the volumes need to be large enough to justify doing it in the SIM," says Roger Dewey, who suggests mobile operators could monetise the solution by charging for a premium SMS each time an update is sent to the SIM. "The only common element in every IoT device is the SIM. There is no Apple or Android in the IoT arena," he adds. "The only logical place to do this is the SIM."

> "There is no need for a separate security chip, as you can use the SIM card. Moreover, it is a global standard. More than 10 billion SIM cards have been issued to date"
>
> **Roger Dewey,** CEO and founder of Able Device

CHINA UNICOM AND TENCENT SUPPLY SIM-BASED SECURITY

In China, leading Internet platform Tencent is using China Unicom's SIM cards to authenticate smart watches and other IoT devices for its customers. The solution is designed to protect devices against unauthorised access and so-called man-in-the-middle attacks, which seek to intercept data transmissions.

To create the solution, Unicom and Tencent have developed and deployed three major components. The first is a security key management platform, which manages the whole life cycle including generation, distribution, writing, updating, and deletion of security keys on the SIM cards. The second is a SIM toolkit application, which helps IoT devices to communicate with the key management platform, create a security tunnel, and generate a temporary session key. Finally, an identity authentication centre is used to authenticate each IoT device (see Figure 3).

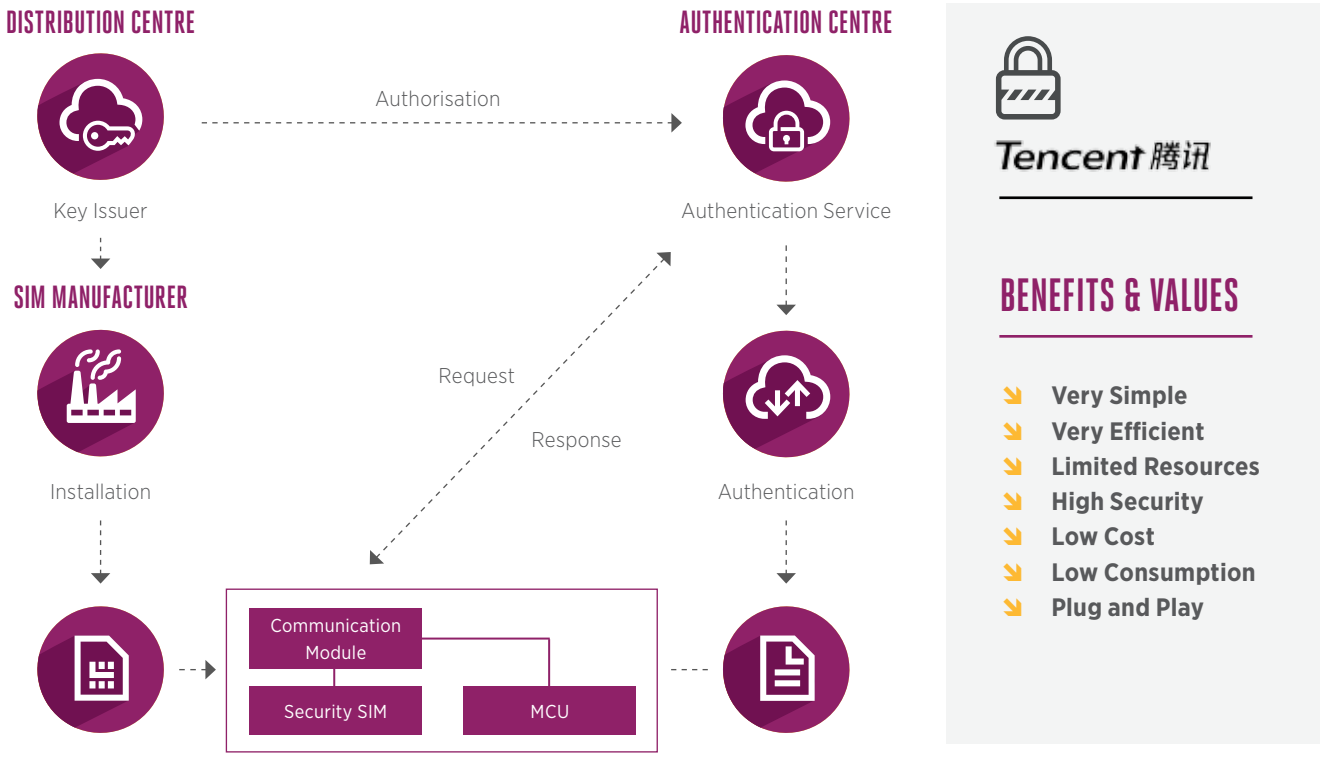
"In our solution, the SIM card is embedded with a unique key and authentication SIM toolkit application, which uniquely identifies the identity of the device," explains Fuzhang Wu, Principal Security Architect of China Unicom Internet of Things Co. "The device establishes communication with the SIM card by calling relevant instructions in the module, and the toolkit application in the SIM card performs identity authentication or encryption and decryption on the transmission."

When a remote server interacts with the IoT device, the communication module forwards the request to the SIM card, and the SIM card authenticates the identity of the requesting party using the SIM toolkit. Conversely, when the device accesses the IoT platform, a temporary session key is generated by the toolkit and the key in the SIM card, and the access platform invokes the authentication platform interface to authenticate the device's identity. The device then invokes the toolkit in the SIM card to encrypt and transmit the data. When the platform transmits encrypted data to the device, the toolkit in the SIM card decrypts that data.

China Unicom says this approach is both cost-effective and straightforward to implement, as no changes are required for the IoT devices, their modules, and chips. "For those enterprises that do not have a particularly high security requirement, but need to encrypt data, this simplified approach can meet the basic security requirements of these enterprises," says Fuzhang Wu. "The whole solution is very simple, but very efficient and

> "The whole solution is very simple, but very efficient and is low cost and has low power consumption"
>
> **Fuzhang Wu,** Principal Security Architect of China Unicom Internet of Things Co.

Figure 3: The components of China Unicom's SIM-based security solution



Source: China Unicom

is low cost and has low power consumption." For now, the primary way in which China Unicom is monetising the solution is through the up front charge for the SIM card. This approach "guarantees the security of customer data on the one hand and the advantage of allowing customers to choose our other IoT services," says Fuzhang Wu.

Serving as the platform provider and technical supporter, Tencent has integrated the key distribution and identity authentication systems into a Unicom data centre. Unicom is responsible for promoting the security SIM card and leading the partners, card vendors and module manufacturers to jointly develop the security SIM card specifications. Unicom says the next step is to develop different levels of security authentication and encryption solutions, which reflect the security level requirements of different enterprises and different industries.

Other operators going down the same route should "consider the needs of all stakeholders, whether the module should be changed, whether it will increase the cost, whether there is regulation, whether the module can be mass-produced…Can you meet the customer's actual situation?" says Fuzhang Wu. He also stresses the importance of specifications and standards. "The unified standard enables fast and accurate docking of various links, reducing the complexity of the adaptation," he says, while also highlighting the benefit of being able to source solutions from multiple suppliers.

AT&T AND G+D MOBILE SECURITY PREPARE TO SERVE FIRST CUSTOMERS

The US mobile operator AT&T and SIM security specialist G+D Mobile Security (G+D) have developed a solution to securely provision an IoT device's identity and credentials for secure authentication to cloud platforms and applications. The two companies plan to take their proof of concept into production before the end of 2018. During MWC Americas in Los Angeles, AT&T and G+D have demonstrated how the solution uses PKI certificates installed on SIM cards inside IoT devices. G+D's SIM-enabled security solution securely connects IoT devices to Amazon Web Services (AWS) using AT&T's LTE network.

"Today, customers have to put a lot of effort into identifying devices at the application level, using a very cumbersome process to enable PKIs," says Senthil Ramakrishnan, lead member of the technical staff at AT&T. "It is difficult to manage. It needs to be done in the factories during the device manufacturing. They also need to deploy systems to check its validity to keep it secure through its lifecycle. They then need to identify a storage mechanism, which makes it very expensive. We can replace all of that by using a SIM to store the identity and provision it using an API or an AT command. The customer doesn't have to deploy anything new: from the customer point of view, this will essentially be zero-touch."

Senthil Ramakrishnan says three AT&T customers are already gearing up to use the solution, including a large machinery manufacturer, an automotive OEM and a cloud service provider. "And we also intend to use it for internal products, such as our end-to-end asset tracking and fleet management solutions," he adds. "It will be deployed in several end-to-end solutions we are deploying."

As well as increasing security, Tomi Ronkainen, Director, Advanced Technology at G+D Mobile Security, says employing the existing SIM card ecosystem affords cost, speed and flexibility advantages over alternatives. "We have secure facilities, certified by the GSMA, where we produce SIM cards," he notes. "Today, the option is to add some kind of co-processor to the device, but since the SIM card already has that functionality, it removes an extra item from the bill of materials. We can also add the PKI certificate or other credentials to the SIM card over-the-air and secure the device identity throughout the device lifecycle."

AT&T and G+D first demonstrated a proof of concept at an Amazon event in November 2017 where they showcased how to secure an AT&T IoT Starter Kit with a SIM card. For the demo, the solution used a PKI certificate on the SIM to enable the authentication of the device. The AT&T IoT Starter Kit was used to send sensor data, such as humidity and temperature, to the AWS IoT platform - all secured by the SIM card.

For the demo at MWC Americas, G+D has extended the solution's capabilities to support some real-world uses cases. "We created demo programmes that use the security of the SIM card to secure data and connectivity in smart city and smart home IoT devices," says Tomi Ronkainen. "We will also show secure over-the-air updates of the certificates based on the standards used for updating mobile network operator credentials and profiles."

As AT&T and G+D turn the concept into a commercialised product, they are looking to extend existing SIM standards to meet IoT-specific requirements. To develop the SIM-based solution, G+D had to create its own interface to enable the IoT device to communicate with the SIM card. "There are variations among different modems about how they support this interface," explains Tomi Ronkainen. "We plan to work with OEMS, cloud/platform providers and application developers to define a common, standards-based approach. We believe this approach, with the SIM card providing tamper-proof storage of credentials, mutual authentication and encryption, enables essential security for the Internet of Things."

> "We plan to work with OEMS, cloud/platform providers and application developers to define a common, standards-based approach. We believe this approach, with the SIM card providing tamper-proof storage of credentials, mutual authentication and encryption, enables essential security for the Internet of Things"

Tomi Ronkainen, Director, Advanced Technology at G+D Mobile Security

Conclusions

As the IoT expands and plays an increasingly pivotal role in the operations of businesses and the daily lives of consumers, the security of connected solutions is paramount. The proofs of concept, pilots and commercial services outlined in this paper highlight the value of using SIM cards to help secure IoT applications in a cost-effective manner. The featured case studies clearly demonstrate how the existing SIM-based authentication mechanisms employed by mobile operators can be used to protect IoT device identities and ensure that traffic between IoT devices and applications is not intercepted or spoofed.

Leading mobile operators and their partners are moving toward commercialising dedicated SIM-based IoT security propositions in response to demand from IoT users for low cost and robust security solutions. While mobile operators have generally yet to finalise their business model for these services, the executives interviewed for this paper believe SIM-based security can be monetised, while also expanding the role of operators in the IoT value chain. In the next six months, they expect to begin rolling out solutions tailored to the needs of different vertical sectors. As a result, mobile operators are likely to widely deploy commercial SIM-based IoT security solutions from 2019 onwards.

For more information please visit:
www.gsma.com/IoT

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601