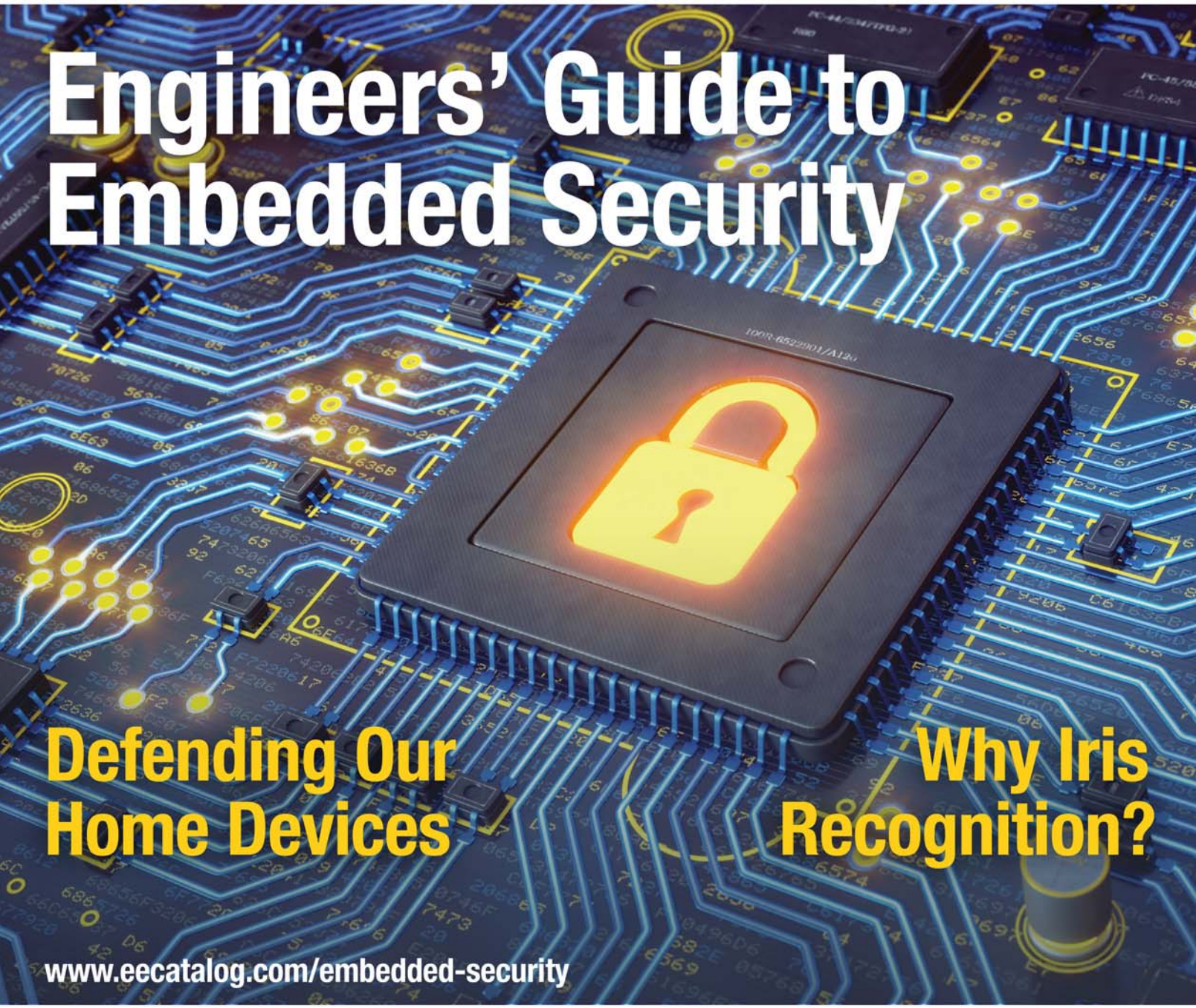
February 2017

EMBEDDED SYSTEMS ENGINEERING

powered by EECatalog

Guiding Embedded Designers on Systems and Technologies



Engineers' Guide to Embedded Security

Defending Our Home Devices

Why Iris Recognition?

www.eecatalog.com/embedded-security

IoT Data **Protection**

Your SSD data is safe with:

- Industrial-temp build (-40ºC to 85ºC)
- Built-in **vtGuard**® power-fail protection
- **vtSecure**™ with self-encrypting technology

Worth protecting?
Then, protect.

Virtium®
Solid State Storage and Memory

Industrial Embedded Technology for Our Interconnected World

CONTENTS

EMBEDDED SYSTEMS ENGINEERING

Special Features

ENGINEERS' GUIDE TO EMBEDDED SECURITY
2017
www.eecatalog.com/smart-energy

Vice President & Publisher
Clair Bright

Editorial
Editor-in-Chief
Lynnette Reese | lreese@extensionmedia.com
Managing Editor
Anne Fisher | afisher@extensionmedia.com
Senior Editors
Chris Ciufo | cciufo@extensionmedia.com
Caroline Hayes | chayes@extensionmedia.com
Gabe Moretti | gmoretti@extensionmedia.com
Dave Bursky | dbursky@extensionmedia.com

Creative / Production
Production Traffic Coordinator
LS Jerrett
Graphic Designers
Nicky Jacobson
Simone Bradley
Senior Web Developers
Slava Dotsenko
Mariam Moattari

Advertising / Reprint Sales
Vice President, Sales
Embedded Electronics Media Group
Clair Bright
cbright@extensionmedia.com
(415) 255-0390 ext. 15
Sales Manager
Elizabeth Thoma
(415) 255-0390 ext. 17
ethoma@extensionmedia.com

Marketing/Circulation
Jenna Johnson
jjohnson@extensionmedia.com

To Subscribe
www.eecatalog.com

Extension MEDIA

Extension Media, LLC Corporate Office
President and Publisher
Vince Ridley
vridley@extensionmedia.com
(415) 255-0390 ext. 18
Vice President & Publisher
Clair Bright
cbright@extensionmedia.com
Human Resources / Administration
Darla Rovetti

Special Thanks to Our Sponsors

Embedded Systems Engineering is published by Extension Media LLC, 1786 18th Street, San Francisco, CA 94107.

The Open Trust Protocol (OTrP) in Automotive

How to continue developing a truly connected world.

By Marc Canel, ARM

In the automotive and many other segments, what characterizes the IoT market is the connection of many devices to a centralized, decentralized or mesh network. The rollout of these devices in the field and the management of the applications is a logistics and security challenge.

Cars have multiple processors handling a large number of tasks. The applications cover various areas such as vehicle control, audio and video entertainment, mapping and navigation, payment, cockpit information and Advanced Driver Assistance Systems (ADAS). Over time, the requirements and regulations in all these areas change. New applications are created, and old ones need updates. The systems hosting these applications need to offer a mechanism which protects various software applications within secure domains to ensure each application's isolation. Isolating one application from the next is especially needed as automotive electronics become more and more powerful—and as these electronics take on multiple tasks instead of being specialized for one function or another. Other applications such as control systems will also need isolation and protection in secure containers.

These applications are not static. They require either functional upgrades, or they get updates with fixes. In a connected vehicle, depending upon the features purchased by the customer, various pieces of code will get downloaded and managed dynamically. Maintenance of the car becomes more sophisticated over time. Updating maintenance systems makes tracking additional data from the sensors and the car's other control systems possible. Navigation and management systems gain enhancements as the car learns driver and passenger use patterns.

Various parties can supply the applications. For example, the control functions may come from the car OEM, while a financial services company makes the payment applications available and still another entity, the IVI system vendor, supplies entertainment and mapping applications. The consumer may also choose the application developer in areas such as payment, entertainment and mapping. This situation

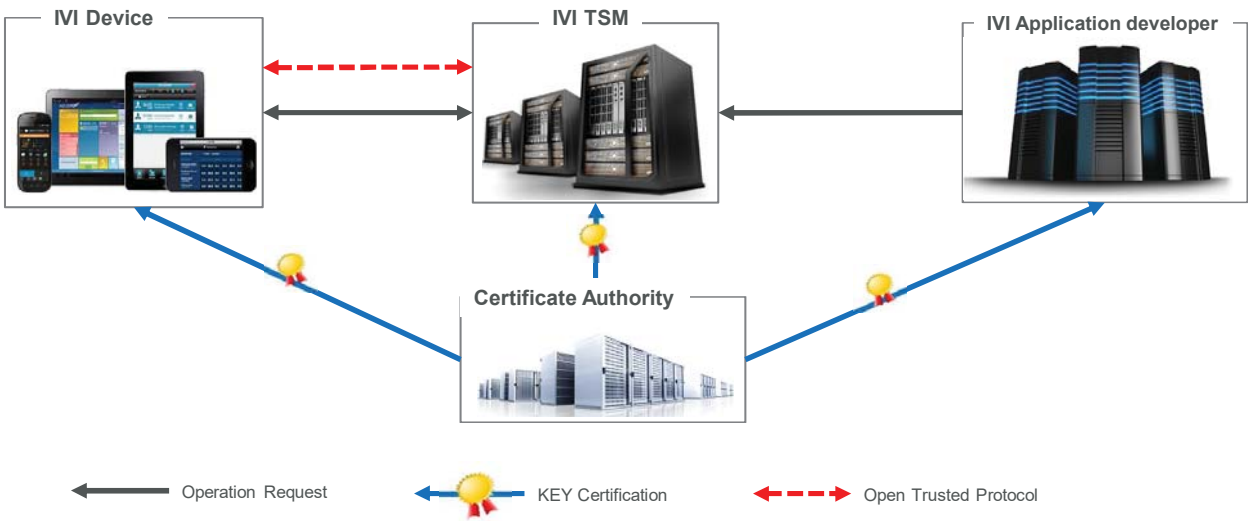


Figure 1: Key components of the OTrP system.

creates an applications provisioning challenge for the car OEM, as all these developers need to push their own code to the car.

A group of leading technology security experts led by ARM®, Intercede, Solacia and Symantec recently released the results of months of collaboration that set out to assess the security challenges of connecting billions of devices across multiple sectors, including industrial, home, health services and transportation. Their conclusion was that for the continued development of a truly connected world, trust between all processors and service providers is essential. In the case of the transportation industry and automotive, a flexible, secure and dynamic mechanism is required to establish trust between the multiple applications developers and various systems of a car. To deal with the risk, the companies collaborated on the Open Trust Protocol (OTrP), which combines a secure architecture with trusted code management, using technologies proven in large scale banking and sensitive data applications on mass-market devices such as smartphones and tablets.

Here, we explore OTrP objectives, how the technology works, its use cases, and the ecosystem that is delivering it.

WHY OTRP?

The objectives of developing OTrP are threefold:

1. Create an open protocol defining how devices trust each other in a connected environment. The protocol would be based on existing open technologies with proven robustness and commercial attractiveness in existing markets. The Public Key Infrastructure architecture (PKI), including the mature concepts around certificate authorities (CAs), was selected as the basic underlying system.

2. Given the reuse of the PKI architecture, it was imperative to create an open market for the certificates that would enable applications to authenticate resources in devices. It was a key requirement to have a mechanism by which certificate authorities can all compete and access devices in which they push their certificates to authenticate resources. In other words, having an open market for certificates was a key objective of the project.

3. With an open protocol, it is possible for multiple vendors to create either client or server solutions. This strategy enables an open and active market of developers of both client and server solutions.

Collaboration began in early 2015, and membership of the OTrP Alliance soon grew to 13 companies. To encourage widespread adoption, the Alliance also worked with international standards bodies such as the IETF and Global Platform to get OTrP adopted as a protocol within their organizations.

THE OTRP TECHNOLOGY

As a protocol, OTrP adds a messaging layer on top of the PKI architecture. OTrP is reusing the Trusted Execution Environment (TEE) concept that increases security and robustness in the system by physically separating the regular operating system of a device from its security-sensitive applications. Given the heterogeneity of the devices in the connected world and especially in automotive, Trusted Services Managers (TSMs) are used to manage keys in the processors to create security domains in the various ECUs, authenticate resources, and load applications. OTrP defines a protocol between a TSM and a TEE and relies on IETF-defined end-to-end security mechanisms, namely JSON Web Encryption (JWE), JSON Web Signature (JWS), and JSON Web Key (JWK). The specification assumes that a processor utilizing OTrP is equipped with a TEE and is pre-provisioned with a device-unique public/private key pair, which is securely stored. This key pair is referred to as the 'root of trust.' A service provider uses such a device to run Trusted Applications (TA).

The key components of the OTrP system are:

1. TSM: The TSM is responsible for originating and coordinating lifecycle management activity on a particular TEE. It is at the core of the protocol and manages the trust in the devices on behalf of service providers. In addition, the TSM provides Security Domain management and TA management in a processor, in particular over-the-air updates to keep TAs up to date.

2. Certificate Authority (CA): Mutual trust among a device, a TSM, and services providers is based on certificates. A device embeds a list of root certificates, called trust anchors, from trusted certificate authorities that will be used to validate a TSM. A TSM will remotely validate a device by checking that a device comes with a certificate from a trusted certificate authority.

3. TEE: The TEE resides in the processor chip security zone and is responsible for protecting applications from attack, enabling them to perform secure operations.

OTrP establishes appropriate trust anchors to enable TEE and TSMs to communicate in a secure way when performing lifecycle management transactions. Several trust relationships need to be set up:

1. The TSM must be able to ensure a TEE is genuine.

2. The TEE must be able to ensure a TSM is genuine.

3. The Device, though its Trusted Firmware, must be able to ensure that a TEE is genuine.

OTrP enables OEMs in the automotive industry to ensure that only approved applications developers will load code within the car throughout its life. Given the complexity of car systems, gate keeping access to the

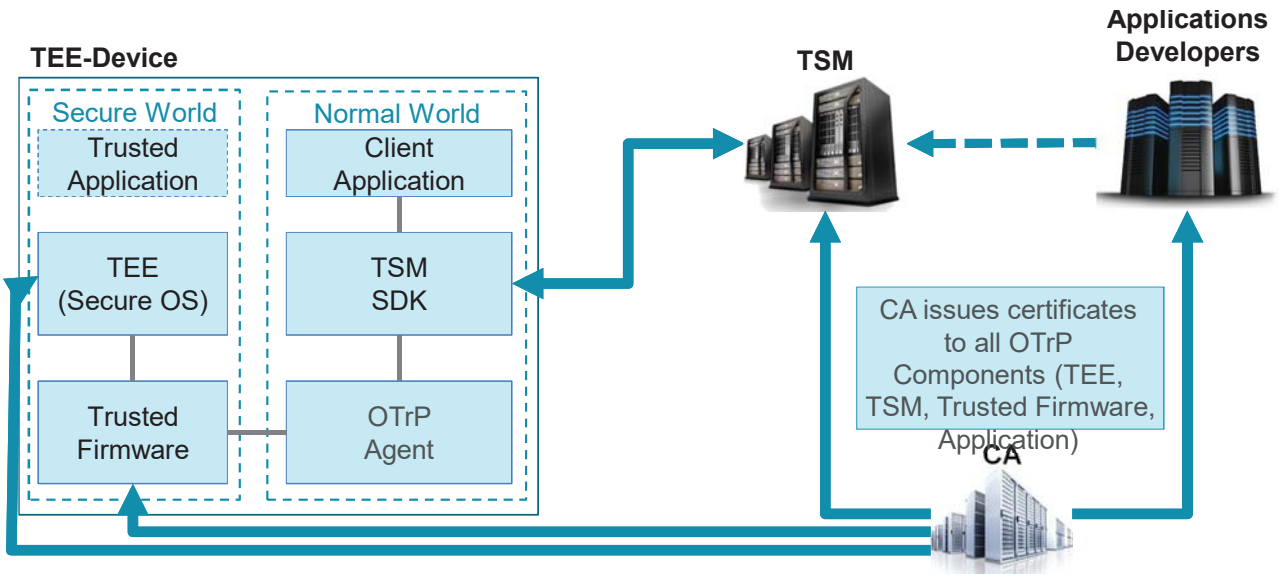


Figure 2: OTrP defines an ecosystem of partners that deliver trust in the applications of the devices.

various systems of the car is a key function of the OEM and its management of ongoing car maintenance.

TRANSPORTATION USE CASES

There are multiple examples of use cases for OTrP in the automotive industry. They are based on the dynamic loading of a security-sensitive application into the TEE of a client device, via a TSM to perform a task for a server system. Here is a small subset:

1. Installation of payment application
2. Installation of Digital Rights Management applications in the IVI system
3. Installation of advanced features: upgrade of cockpit functions, entertainment systems
4. User Management: authentication, profile management and privacy
5. Update of maintenance systems collecting data from the car
6. Update of control systems

OTRP ECOSYSTEM AND BUSINESS MODEL

By identifying the key components in the system, OTrP defines an ecosystem of partners that deliver trust in the applications of the devices. As indicated in Figure 2, the Trusted Services Manager (TSM) plays a central role in enabling trust between the partners.

The role of the TSM can be played by the automotive OEM or another party designated by the OEM as the gate keeper to the car. Several TSMs can be set up to control the car: for example, the OEM can choose to have a TSM for the navigation and mapping systems and a different TSM for the audio and video entertainment systems, offering further isolation between the management systems of the car. OTrP allows the OEM to have several TSMs for applications sharing the same processor: for example, the IVI vendor could operate as the TSM for the IVI system. Another TSM vendor will manage another set of applications such as the Cockpit Display applications.

OTrP as a protocol does not define a business model; it only defines the entities that take part in the ecosystem. The protocol integrates all the tracking elements to enable any business model selected by the partners. Therefore, the automotive OEM and its tier 1 suppliers can choose the business model that suits them best for the car. For example, the TSM managing the cockpit functions will have a business model controlled by the warranty and maintenance policies of the OEM, whereas the TSM managing entertainment functions that can be upgraded on demand by the consumer would be based on a different business model, involving usage fees.

The protocol is available for download from the IETF website today for prototyping and testing.

Marc Canel is VP of Security Systems, ARM.

Protecting Smart Home Devices from Security Breaches

Design security need not take a back seat, even in the race to be first to market with smart, connected home products.

By Hal Kurkowski and Scott Jones, Maxim Integrated

Hal Kurkowski, Managing Director, Maxim Integrated

Scott Jones, Executive Director, Micros & Security, Maxim Integrated

Navigating traffic on your way to work, you realize that you may have left your bedroom light on. No need to turn back. All you have to do is click off the lamp from your smartphone app. Smart home devices for applications like lighting, security, and temperature control can make our lives more convenient. But worries rise when these seemingly innocuous devices get hacked, opening avenues to potentially dangerous and harmful situations.

Last year, a Boston-based cybersecurity firm reported on how vulnerable Internet-connected baby monitors are because many lack basic security features. Rapid7 found problems like hidden, unchangeable passwords; easy access to device account numbers; and unencrypted data streams. Not only could a hacker gain access to the monitor's video stream of a child, but intruders could also transmit their own voices and video feeds through these systems. This past fall, hacked CCTV video cameras and DVRs were used to launch a large-scale distributed denial of service (DDoS) attack that sparked a massive Internet outage affecting many popular websites, including Amazon, Tumblr, PayPal, and Reddit.

Clearly, consumers have plenty of reasons for concern. But so do businesses that want to protect against cloning, counterfeiting, reverse engineering, and the brand damage that can follow. That's why security must be a primary—and early—consideration for the design of any smart, connected home device.

SECURITY NEEDS TO BE SMART, TOO

Gartner expects that by 2020, the world will have 20.8 billion connected things, up from 6.4 billion this year. That's quite a big jump in a short timeframe—and a big market opportunity that many companies don't want to miss. Yet, as Gavin Kenny notes in IBM's Security Intelligence blog, "In the race to be first to market and meet the need for zero-setup equipment, security on many IoT devices is woefully inadequate[1]."

What does it take to build more security into smart home products? First, account for the fact that many IoT devices are integrated into a network—a breach into one device could potentially expose others to malicious attacks. Next, integrate security early on into all levels of the design, from the sensor node to the chip to the system and the cloud. In his blog post, Kenny argues that security itself needs to be smart: "It has to be automated, self-maintaining, adaptable and maybe even cognitive[2]."

VERIFY, VALIDATE, AND AUTHENTICATE EVERYTHING

From a design standpoint, it's critical to verify every connection and interface, comply with relevant standards, and conduct quality assurance testing to root out potential problems. Techniques like secure boot, secure key storage, encryption, and authentication are essential. With secure boot in place, an electronic device executes authenticated, i.e., trusted software in order to operate. The device can accomplish this via a microcontroller containing software that cannot be modified (called the "root of trust"). Once the microcontroller is powered on, it runs this piece of software first; the software starts the application code after it has successfully verified its signature. Signature verification takes place using a public key that has been loaded into the microcontroller. In addition to ensuring that a system boots into a known, safe environment and providing on-chip storage of encryption keys, a secure microcontroller can also perform normal tasks, including executing software, monitoring sensors or other inputs, and controlling outputs within a system.

Secure, two-way authentication—where two entities must prove their identity to each other—helps protect against malicious attacks. Cryptographic algorithms involving symmetric keys, for example, the Secure Hash Algorithm (SHA-x), can be used for two-way authentication. With symmetric keys, the host and slave must operate from the same secret key, and the secret has to be protected from disclosure attack on both sides.

1. https://securityintelligence.com/smart-homes-need-smart-security/
2. Ibid

Two disadvantages associated with symmetric key-based systems are: (1) key distribution/management, and (2) the need to protect the secret key inside the host system as well as the slave system. Since the host and all slaves within each symmetric key-based system ultimately share the same unique secret key, a key derivation and establishment method must be deployed to prevent the number of keys growing to an unmanageable state.

To address these drawbacks, cryptographic algorithms involving asymmetric keys, for example the Elliptic Curve Digital Signature Algorithm (ECDSA), can be used instead. With asymmetric keys, the keys are different but related mathematically. The host utilizes a public key (which doesn't have to be protected against disclosure), and the slave utilizes a corresponding private key (which must be protected). ECDSA is advantageous because the party that is authenticating the peripheral doesn't have to securely store a secret. Instead, the authenticating party can use a public key that can be distributed freely. Thus, asymmetric algorithms solve both the key distribution problem and the need to secure the key in the host system.

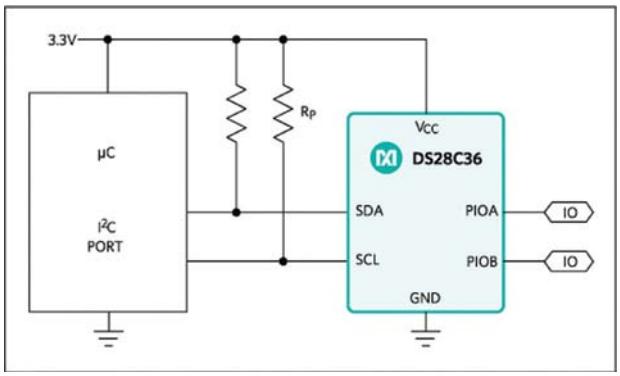


Figure 1: This diagram depicts a typical application circuit with the DS28C36 secure authenticator.

Within a system, there may be a need to go beyond simply authenticating a peripheral, sensor, or consumable to a host system. It may also be critically important to ensure that the data being monitored and sent from a sensor to an aggregation or decision point has not been modified, or that control signals being sent to a valve or actuator are not compromised. Authenticating the data chain from the protected sensor node to the web server, or from the web server to the system controller/actuator, is often an important consideration in order for any system to be deemed secure.

LOW-POWER, SECURE MICROCONTROLLERS AND SECURE AUTHENTICATORS

The foundation for safer IoT designs lies in their underlying technologies. Secure microcontrollers that integrate advanced cryptography with physical security can protect against physical tampering, reverse engineering, and side-channel attacks. For example, Maxim's DeepCover Secure Microcontrollers feature integrated secure NV SRAM that is erased instantly when an intrusion is detected. The low-power microcontrollers also feature built-in FIPS-certified hardware cryptographic engines that support industry-standard algorithms, as well as

Figure 2: This ARM® mbed™ based IoT embedded security reference design can be used to authenticate IoT device nodes, as well as to protect industrial applications from counterfeiting, track product lifetime and deliver smart notifications, and to invalidate unsafe industrial sensor nodes.

patented real-time code and data encryption to fully protect external memories. For quality and safety assurance, counterfeit prevention, secure boot, usage control, secure GPIO, and peripheral authentication, Maxim offers its DeepCover Secure Authenticators, which implement advanced physical security (Figure 1). And, to protect sensitive data from physical or environmental tampering, the company has its DeepCover Security Managers, which bring together advanced physical security with on-chip, nonimprinting memory.

To ease the process of developing smart and safe connected products, Maxim provides its ARM® mbed™ based MAXREFDES143# IoT embedded security reference design (Figure 2). This design protects industrial sensing nodes and sensors via authentication and notification over WiFi between the node and a web server hosted by Maxim. It uses the SHA-256 symmetric-key algorithm and enables you to quickly integrate your application. The reference design offers a way to eliminate the need to store the secure key in the processor memory. Access to the design is available on the mbed website

SUMMARY

In the dash to get to market first with the next must-have smart, connected home product, no one can afford to neglect design security. Techniques such as secure boot, secure key storage, authentication, and encryption can help you make homes smarter and safer. What's more, ICs with built-in security provide a head start and a strong foundation for you to build upon.

Hal Kurkowski is a Managing Director in the Micros & Security Business Unit at Maxim Integrated, where he has been involved with security-related products for over 30 years, including work at Dallas Semiconductor prior to its acquisition by Maxim in 2001. He is a graduate of the University of Illinois at Urbana-Champaign with a master's degree in electrical and electronics engineering.

Scott Jones is an executive director of Business Management at Maxim Integrated, where he leads a team responsible for secure authentication products. With over 15 years at Maxim, Scott is responsible for product line management and end-customer business development. Prior to joining Maxim, he spent 15 years in applications engineering and embedded HW/SW design roles at Dallas Semiconductor and other technology companies.

Iris Recognition for Secure Digital ID

Here's why the biology of our irises makes them reliable, secure digital ID tools.

By Dr. Salil Prabhakar, Delta ID

After the introduction of fingerprint scanners in mobile phones, biometrics has become a core feature of our mobile devices. Remembering, forgetting and recalling passwords is arguably one of the biggest pain points in digital lives, and biometrics is perhaps the easiest way of addressing it. There's no need to remember something that consumers always have, such as fingers, eyes, face etc. While biometric technology based on fingerprints was the first to find widespread use, of late, building on the success of fingerprints, more mobile phones are using the iris in their latest models.

Fujitsu/NTTDOCOMO launched the world's first mobile phone with iris recognition capability, the F-04G, in mid 2015, followed by F-02H in winter of 2015. Other mobile devices with this feature include the Lumia 950 and 950XL, HP Elite X3 (Figure 1), Fujitsu's F-02 tablet, and the ill-fated Samsung Note 7. The reason for the interest in the iris is primarily better reliability compared to even fingerprints, as well as higher security. Both these advantages stem from the iris's biological characteristics.

Figure 1: The HP Elite x3 has an integrated iris scanner. [Source: commons.wikimedia.org Maurizio Pesce, Milan, Italy]

INTRICATE AND YOURS FOR LIFE

The iris is the doughnut-like structure around the pupil of the eye. A muscle, the iris controls the size of the pupil to control the amount of light that can enter the eye. Like any of our bodies' other muscle structures, the iris has a rich and unique pattern. This unique iris pattern, as with fingerprint patterns, is what computer algorithms use to derive a unique identity for each iris and associate it with the identity of the individual.

The iris pattern is even more complex (richer) than any fingerprint pattern, so it has more information content, which translates into more entropy and a higher level of security. Think of how six-digit passcode security compares to four-digit passcode security. The iris gets its color from a pigment called melanin, and this pigment has a different color for different people. The iris is formed even before a baby is formed during the gestation period and remains the same for life. As an internal organ, the iris is completely covered by a transparent layer called cornea, a feature which makes the iris a more stable and reliable biometric modality.

OVERCOMING CHALLENGES

The Unique Identification Authority of India (UIDAI) has created the world's largest biometric based citizen and resident authentication system based on the iris. During its initial pilot studies the UDAI verified:

- The iris does not get worn out with age, or with use.
- Weather changes do not affect Iris authentication.
- Iris image capture does not require physical contact. Capturing the iris image is physically similar to the familiar practice of taking photographs.
- Iris capture requires simple instructions such as, "Look at the camera; keep your eyes wide open."
- A fake iris is difficult to synthesize, making impersonation harder
- The Iris image cannot be captured without the individual's cooperation
- The spread of low-cost consumer cameras has aided iris camera costs and manufacturing.

While these pilots and subsequent tests done by UIDAI have confirmed the advantages of the iris, early adopters of iris-enabled mobile phones have also reported some problems:

- Difficult use under direct sunlight
- Difficulty detecting the iris when using certain kinds of glasses
- Difficulty detecting the iris while the user is moving

Despite these problems, iris biometric technology is favored over fingerprint biometric technology, which is being found to be unreliable depending on the individual's age, occupation and other external conditions. Many young people have soft skins with wrinkles that affect scanning, and older people tend to have dry and brittle skin that does not have the appropriate contact for scanning. People involved in manual labor such as construction workers and farmers end up damaging their fingerprints. Additionally, fingerprints are easily left behind on devices and other objects we touch, which can make it easier for sophisticated adversaries to steal them.

One company which is taking on some of the challenges associated with iris biometric technology is Delta ID. The company's AvtiveIRIS® technology includes advanced algorithms to compensate for these challenges and provide users with an easy to use, secure iris recognition system that can work for mobile users across age groups, occupations, and usage conditions. The Delta ID ActiveIRIS software compensates for the motion blur that is introduced when the user is moving, occlusion of the eye by the eye lashes under direct sunlight or by reflections on the glasses, and many more usage scenarios.

Research and Markets predicts the global iris recognition in access control market (authentication, biometrics, cards, touch screens) to grow at a CAGR of 18.09% during the period 2016-2020[1].

Figure 2: "Unlike fingerprints, the iris-enabled identification can be touchless and seamless, adding to the in-cabin experience."

The higher security and reliability of the iris has significant appeal to multiple applications and services spanning multiple vertical markets. On mobile devices one of the primary adopters of biometrics has been for mobile payments and banking. The success of mobile enabled financial applications hinges on the usability and security of the biometric modality used for authentication. Performing better than fingerprints on both those fronts, iris biometric technology is expected to see more and more adoption in the near future. In the automotive sector, we're seeing interest in iris biometric technology for driver identification and driver monitoring. Unlike fingerprints, the iris-enabled identification can be touchless and seamless, adding to the in-cabin experience (Figure 2). Driver identification can then be used for multiple use cases—in-cabin customization, security, pay-as-you-go insurance plans, auto enabled payments—and at gas stations, parking lots, drive through restaurants, and more.

The applications of this technology can be endless once consumers recognize the superior user experience and security.

Dr. Salil Prabhakar is President and CEO of Delta ID Inc., a California technology company he co-founded in 2011.

He is an expert in the area of biometric fingerprint and iris scanning technology. Dr. Prabhakar has co-authored 50+ publications (14,000+ Google Citations), two editions of the award-winning Handbook of Fingerprint Recognition, five book chapters, and eight edited proceedings. He has several patents granted and pending. He has served as an Associate editor of IEEE Trans. on Pattern Analysis and Machine Intelligence, SPIE Journal of Electronic Imaging, EURASIP Journal of Image and Video Processing, Elsevier Pattern Recognition, and Current Bioinformatics. He was lead guest co-editor of April 2007 IEEE Transactions of Pattern Analysis and Machine Intelligence Biometrics Special Issue. He has been a co-chair/program chair for 10+ IEEE, IAPR and SPIE conferences, was general co-chair of the 5th International Conference on Biometrics in 2012 in New Delhi. He was VP Finance of IEEE Biometrics Council during 2010-2012.

1. http://www.researchandmarkets.com/publication/mtausix/3920634