WHITE PAPER

IOT SECURITY AT DESIGN AND MANUFACTURING

TRUSTED DEVICES DRIVE THE VALUE CHAIN: SECURING IOT DEVICES DURING MANUFACTURING

HARMAN Connected Services

August 2017

Entrust Datacard™

Trusted Identities | Secure Transactions

HARMAN

A SAMSUNG COMPANY

Contents

Abstract

Over the last 5 years, we have seen an unprecedented level of changes in the way we lead our lives and how we use computing devices. The introduction of connectivity into everyday objects and the ability to access real time information from a wide variety of devices means that we are now starting to see the vision of the Internet of Things (IoT) become a reality. The promise of IoT offers a path to a world where many of the day-to-day bottlenecks will be eliminated, as devices and services around us intelligently work together to anticipate our needs and adapt accordingly. However, we are also witnessing a surge in the number of security breaches as more rogue hacking attacks target IoT devices.

Recognizing the potential of the IoT market and the growing need for IoT security, HARMAN Connected Services and Entrust Datacard have formed a strategic partnership (initially announced in April, 2016) with a common goal to build trust within the IoT ecosystem by securing the data and IoT infrastructure. HARMAN's IoT domain, industry vertical and product development expertise complement Entrust Datacard's identity solutions to enable transactions in high risk and constrained environments.

The joint solution enables organizations to conveniently establish trust within infrastructure and secure the interaction between users, devices, and systems. The trust is implemented in a manner that recognizes the customer preferences to leverage existing environments and remain flexible in their choice of devices, backend applications, and data analytics environments.

This white paper is part of a series of resources aimed at raising awareness about IoT security. The white paper is intended to offer companies and end customers key insights about solutions that can enhance the security of their IoT implementations.

The Growth of IoT and the Implications for Security

Today we are at the genesis of a revolution. We have seen a wide range of devices being connected. And this will continue to increase as connected devices become pervasive in our offices, homes and cars. The car indeed is rapidly becoming a fully connected device in its own right. Added to this are the upcoming wireless networking technologies such as 5G, with its support for MESH networking, LoRA, SigFox and the continued enhancements to Wi-Fi, Bluetooth and ZigBee. It is not difficult to envision that in a short span of time, we would be living in a truly connected and always on world. But this comes at a cost. The implementation of connected device ecosystems imposes very specific operational and security challenges, especially as the number of points of attack becomes greater.

Unlike a traditional Windows or Linux environment, an IoT implementation usually covers a diverse set of devices with a diverse set of capabilities that are connected to a single or series of platforms requiring disparate means of addressing operational and security challenges. The question is how to bring this diverse set of IoT devices together, securely, into an IoT ecosystem.

Why is securing these systems so complex?

Many of these devices and systems were designed to work in confined environments, which are not exposed to an external network. Newer, more widely available connectivity technologies are opening connections between the traditional industrial or automotive networks and the digital platform, thereby introducing a new set of threat vectors. These threats require a new approach to handle system security and integrity.

Longevity

When one considers the long-lived nature of these devices, the risk and the scale of threat becomes more evident. In any of the sectors addressed above, devices could potentially operate for a period of 10-15 years and would need periodic security updates. For devices with such long lifecycles, it is important to ensure that new features and services can be added enabling device manufacturers to adapt to new industry developments, changing consumer requirements, and to embrace relevant new industry standards and protocol enhancements along the way.

Identity

It is also critically important that the overall security architecture on such devices be kept up to date with new methods and models as used by the rest of the ecosystem that the device might be interacting with. Furthermore, the devices in question may not have the ability to enter a password. To establish the identity of those devices, appropriately authenticating and authorizing them becomes a critical issue. The challenges go beyond authentication and authorization, as data security is the next important item to consider.

Diversity

With a wide range of 3rd party sensors and gateways from different makers available, IoT is an evolving technology where device protocols are not yet standardized; managing and controlling such a complex ecosystem is becoming a key challenge for many organizations. Moreover, most of the solutions in the market today are closed in nature and were not designed for extensibility, further complicating the management headache.

New Threats

Hackers are finding new potential ways to enter into a system and extract sensitive information. Consider the risks to the user of a connected car, if a hacker were to take control of the steering wheel, while the car is in motion.

Most of the players in the IoT industry take such concerns seriously and are diligently working towards various solutions to mitigate and eliminate the risk from such challenges. However, the solutions which are available in the market still mostly rely on one-time authentication mechanisms. For the next generation of devices thinking about the overall lifecycle of the device from manufacturing till the end of life is key. A onetime authentication mechanism will not be enough. Any IoT solution today, in order to be successful, should be built on a strong trust model. The connected car example discussed above requires a mechanism in place that should take care of the device and individual component identity to ensure that all interactions are authenticated and authorized.

Future Proofing IoT Security

The solution, which HARMAN and Entrust Datacard have co-developed, enables organizations to tackle these challenges head on and to be assured that they can embrace the new digital, connected reality while driving their businesses forward. Indeed as organizations implement digital transformation strategies, security will become a core building block not only for their own services but also the products and services that they source from suppliers and partners.

Trust in the Automotive Industry

Like other vertical markets, the automotive industry is exploring how it might leverage the trends in connectivity and the opportunity for enhancing customer relationships that the trend represents. The "connected vehicles" journey will embrace many different technologies such as Telematics, Advanced driver-assistance systems (ADAS) and autonomous driving to name but a few. It will also see vehicles of all types begin to connect with the world around.

The usage of real time and cloud based connected platforms and services has greatly expanded the number of use cases that a connected vehicle could support. These cloud based platforms would not only work within the car but also have the ability to connect to a wide range of third party data sources and applications. This connectivity enables the creation of advanced and intelligent services ranging from smart transport solutions to cars that learn about your driving style, preferences and then personalizes on demand. Imagine renting a car from the airport that downloads your unique driver profile and personalizes your driving experience specifically to your preferences.

Vehicles will also increasingly connect to the infrastructure around them to both share and receive information. For example, imagine being able to reserve a parking space before arriving at the parking garage or that when you are planning your route, the navigation system can check real time traffic light data to factor in the frequency of when the lights will turn amber or red to create a fully personalized and optimized route that minimizes the amount of time you'll be waiting for a green light.

Of course, this new hyper connected environment brings with it, a new set of challenges. No longer will it be enough to focus only on protecting just the hardware inside the vehicle. The concept of automotive security needs to extend and cover the entire ecosystem from the vehicle to the cloud and any third party that is providing data feeds.

Identity Management Solution

By adding identity management to a vehicle, many such challenges could be addressed. Once the vehicle has an identity, it can understand who/what it can talk to and specifically what they can talk about. Thus, the vehicle will know that it can talk to a given cloud server, which APIs can be interacted with and what data may be shared. The vehicle will also understand other important elements such as the typical pattern of behavior (such as time of day and frequency of interaction, type of data exchanged etc.). And the vehicle may flag abnormal behavioral patterns – implementing a "trust-but-verify" based approach.

Using identity management enables the trust based relationships to be extended to cover the end to end connectivity path from the cloud to the vehicle. However, as the market for automotive services continues to develop, it would be important for enabling new, consumer oriented, "vehicle-to-thing" connectivity to emerge.

Imagine a scenario where your car and home have established a trust based relationship and thus when you leave, your home your car can issue instructions to your home to turn off lights, start the robot vacuum cleaner, enable the alarm system, or turn down the heating. Similarly, when returning home, your car could check with the refrigerator to see if you need to order groceries, or are running low on other supplies, prior to your arrival.

Vehicle occupants, drivers, and passengers will also have access to an increasing range of value added services directly from the vehicle, such as shopping, media content streaming, productivity. This underlines the need for robust security methods as much of the potential content being delivered to the vehicle is received from third party sources and hence driving an even stronger need to have a complete end-to-end chain of trust in place.

When and Where to Add Identity Management

As you can see adding identity management will have a wide range of benefits for the automotive manufacturers as well as the drivers - whether private or commercial. Thus, the key question becomes when and where to add identity management. HARMAN and Entrust Datacard believe that best practice should be to add identity at the point of manufacturing. on the production line, as this will provide the manufacturer with greater confidence in their end to end supply chain integrity. Some of the key benefits:

- The manufacturer will have greater confidence in their end to end supply chain integrity.
- The manufacturer will be able to fully verify the implementation of identity management into the vehicle.
- The vehicle can be pre-configured for secure relations – such as with the OEMs cloud service.
- It can be fully integrated with other security mechanisms within the vehicle.
- The vehicle will be protected from the first drive.

Working together with Entrust Datacard, HARMAN has developed a wider range of assets that support the Entrust Datacard identity management solution including the HARMAN Ignite cloud platform, over-the-air (OTA) software updates, consumer and Enterprise IoT portfolio such as HARMAN's Smart IoT gateway. Thus, a complete solution for the entire automotive ecosystem from the product line to the dealerships and from the driver to the home can be provided.

Furthermore, Entrust Datacard security framework builds on the existing security solutions such as HARMAN's 5+1 Hardware protection model that are already offered to many customers around the world and the leading OTA solution, which is already deployed in more than 30 million vehicles worldwide.

Entrust Datacard ioTrust™ Security Solution

Entrust Datacard is known for delivering trusted identities and secure transactions in the financial, government and enterprise sectors. However, their presence spans almost all the industry verticals. The key value proposition of this Entrust Datacard solution is that the identities can be trusted and associated transactions can be secured to deliver business value in a secure manner. Entrust Datacard provides a trusted Internet of Things by securing devices and data flows – from sensor to cloud – that drive transformational digital business outcomes.

The Entrust Datacard ioTrust Security Solution allows pre-integration of identity management and data security into any IoT device. The Entrust Datacard ioTrust Security Solution gives you the power to bring connected devices and secure infrastructures to life. ioTrust Security Solution is based on enterprise-grade encryption technologies and establishes trusted identities for devices across IoT infrastructures, creating secure ecosystems that transmit data from devices in the field to your value engines — efficiently and securely. (***Figure-1***)

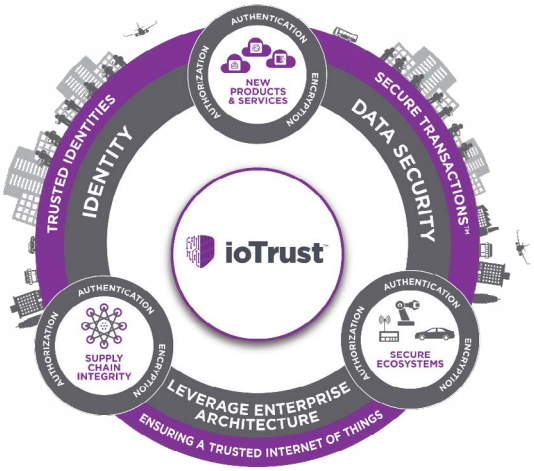

Figure 1

The solution offers software that enables identity, data security and infrastructure for connecting devices and sensors to the cloud. The ioTrust Security Solution addresses the complete lifecycle of the device starting from supply chain integrity, which means establishing a root of trust during the device manufacturing and enabling the identity management when the devices becomes active in an operational environment. During the operational lifespan of a device (the authentication, authorization, data encryption and services-rooted) managed identities ensure that solutions are secured and up to date. The solution helps in launching new products through configuration bootstrapping and service discovery and preserves the enterprise architecture and existing investments that a customer has made by delivering services from a customer's local IT environment or cloud based hosted services.

Pillars of ioTrust™ Security Solution

This solution approach is built on four primary pillars:

Create a Trusted Ecosystem – Starting from device manufacturing ioTrust Security Solution helps manufacturers establish the root of trust for devices, ensuring that every component or device is securely and uniquely identifiable. These unique identities enable operational use cases such as configuration bootstrapping, operational identities and security such as transport and payload encryption. The value commitment from the solution is that every device which is connected to this ecosystem will be uniquely identified, authenticated and authorized while providing the visibility to the supply chain in terms of where and when a device was manufactured.

Secure Outcomes from Connected Ecosystems – Securing the data acquisition from the device as a point of origin and securely cryptographically enforcing the access control while delivering the data to the cloud platform for which it is provisioned.

Leverage the Enterprise Architecture – The idea is to build a solution which is platform agnostic both from the end device and cloud infrastructure point of view. ioTrust Security Solution is a pure software based solution that adheres to the very specific requirements of constrained IoT devices allowing for support of devices which may or may not be able to run embedded IoT agents.

Enhance User Experience – By making security an enabler for enrollment, provisioning and data acquisition, customers can extract value and automate laborious manual tasks.

ioTrust™ Security Solution Model

The diagram below depicts some of the ecosystem components of the ioTrust™ Security Solution.
A key attribute of the solution, is that it can handle both green field and brown field deployments. Devices can download unmanaged or managed security identities if they have the required footprint, or leverage an edge gateway to provide a proxy mechanism. Highly constrained devices (either via resource or inability to affect change in software) are secured side by side with modern device manufactured with ioTrust™ Security Solution.

Based on the needs of the implementation in question, the architecture can be tuned and designed to meet the needs of an end user organization. The platform may be either hosted and delivered by Entrust Datacard or deployed on premise within the end user IT environment.

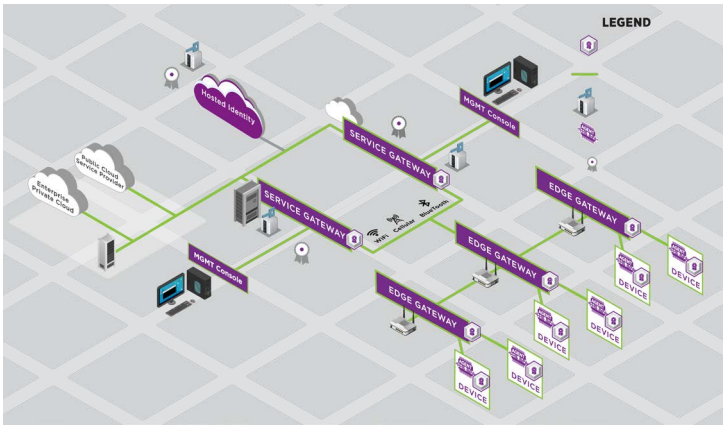

Figure 2

ioTrust™ Security Solution Offerings

ioTrust Security Solution offerings are divided into three different tiers of service dealing with device manufacturing and operations.

Tier 1: Identity Issuance - Allows device manufacturers to establish a root of trust and enables them to connect every device or component they produce through a chain of trust. Being able to uniquely identify where, when and by whom an object was manufactured allows for complete supply chain visibility and rapid enablement of operational services. When the trust moves from the manufacturing to the operational state, customers can leverage the second tier.

Tier 2: Identity Management – This solution addresses operational security needs. Secure device enrollment, dynamic configuration acquisition and storage of cryptographic material available and enabled by a managed identity ensure appropriate levels of authentication and authorization in device-to-device and device-to-application interactions.

Tier 3: Identity and Data Security - This tier of service integration allows customers to enforce granular level of control in terms of data acquisition and command execution. It also allows customers to decide when and how data acquisition will be done and what kind of access controls should be applied to a given data stream.

	MANUFACTURING	OPERATIONS	
Offering	TIER 1 Identity Issuance	TIER 2 Identity Management	TIER 3 Identity & Data Security
Primary Focus	Secured devices manufacturing	Secure channel for acquiring data from devices and submitting to enterprise data hubs	Granular control over access to data and command execution
Market Segment	Device manufacturer and Tier 1 component providers	Device operator focused on operational state of security deployment	Device operators with analytics-driven business use case
Tech Foundation	PKI: Root-of-trust delivered via IoT-centric infrastructure design	Scalable provisioning of managed identities enabling authentication and authorization policy management	Integrated secured data acquisition and ingestion with policy-driven equipment data management

Figure 3

Key highlights

As outlined in the previous section Entrust Datacard provides a highly robust and flexible approach to securing IoT devices while creating end-to-end chains of trust. Through the partnership with Entrust Datacard, HARMAN is developing a range of IoT solutions that will include the following security elements as standard.

Endpoint Data Security

- Offer Data security beyond Transport Layer Security (TLS) and pre-shared key mechanism by using Identity based solutions.
- Protect data path with industry standard payload encryption mechanism.
- Protect endpoints in cases in which traditional authentication and cryptography cannot be implemented due to resource constraints and long device cycle outliving encryption effectiveness.
- Obtain anti-tampering functions for devices used in high risk environments since IoT devices require strong device identity and a root of trust as a foundation.
- Satisfy personal data privacy expectations between individual and organization in the IoT era.

Device Identity Management

- Enable device identity and key/credential management which offers IoT scalable, federated, and secure device management implementation.
- Tackle secure cryptographic key provisioning and management risks in use cases where a mass number of IoT devices are concurrently deployed in a challenging environment.
- Provide quick, secure, scalable and device-independent identity, access and relationship management experience.
- Manage and provision IoT devices by delivering firmware updates, software patches, and security updates - to address any vulnerability - periodically using an Over the Air (OTA) based solution.

Device Discovery

- Detect IoT devices in enterprise networks which are either proprietary or non-IT standard.
- Real time visibility and control of every network connected IoT device.

Embedded Trust

- Vendors that provide hardware root of trust certificates to secure many variety of functions at the endpoint.

Self-Provisioning Infrastructure

- Components within an IoT ecosystem should be self-discoverable. Just installing the device will securely discover its parent and its hierarchy. There shouldn't be any need for manual provisioning.

Seamless Integration

- For IoT deployments to be successful, products and solutions from partnering technology manufacturers should easily integrate.

Case Study: Security Solution Incorporated and adopted by a HARMAN customer

Key Customer Requirements involved supporting security between HARMAN IoT Gateway and their cloud infrastructure via SSL sockets created using Entrust Datacard managed identities. The overall goal was to have their IoT solutions work along with strong security from Entrust Datacard and HARMAN's IoT Suite with analytics services to provide automation and efficiencies to commercial real estate environments as part of their new initiatives.

The HARMAN customer, a mobile technology company powered by its suite of IoT Solutions, enables interoperability for various IoT devices, networks and industries through global standards like oneM2M. The customer was initially relying on their own hop-by-hop security implementation, which is based on PSK Certificates. They realized that their existing security implementation had certain limitations i.e. PSK Certificates are stored in a file on file system, certificates are self-signed, and not designed with scalability into consideration. There was a risk that security credentials could be stolen from the file system of a compromised device/server. Moreover, it is not easy to identify and block a compromised device, making the whole system vulnerable.

The customer felt the need for automatic security credential configuration i.e. certificates that are pre-configured or configured to gateways/devices automatically during either the manufacturing or operations process. That's where the Entrust Datacard™ ioTrust™ Security Solution came into the picture. ioTrust Security Solution identities are safely stored into a soft keystore instead of storing them on the file system. This significantly reduces the possibilities of security credentials from being stolen.

Additionally, ioTrust Security Solution allows for the possibility of upgrade to hardware security provided by Trusted Platform Module (TPM) once available in newer hardware generations. ioTrust™ Security Platform provides a scalable solution, wherein security credentials for large numbers of devices can be easily managed. In a worst scenario, if there is ever a security breach, end devices can be easily blocked by the identity revocation mechanism without impacting other modules. A unique selling point of ioTrust Security Solution is that each device/gateway within the ecosystem will be identified using the unique certificate, where the server and the device can both mutually authenticate each other before establishing the data connection.

Recommendations for Execution

For a winning IoT strategy, security should be viewed not just as another item to check-off on the product development "to do" lists but rather as a foundational component. HARMAN and Entrust Datacard recommend organizations to pursue a security strategy that entails adoption, but not the development of a technology based product. Some of the steps involved are:

- Identify a long-term partner who has the ability and accountability for the overall security solution.
- Choose a deployment model: Selecting from on premise or cloud-based, managed or unmanaged;
- Initiate a prototype to implement the security solution to address the highest priority needs while also demonstrating the business value.

Engagement models can be designed to meet the customer requirements through mutual discussion in the early phases of the project. Milestones could be built in for accomplishing an organization's desired goals during each phase of the project such as planning, design, prototype and validation phase. If required Entrust Datacard can also be involved in the monitoring, maintenance and review to optimize the performance and outcome.

Summary

The opportunities generated by the growth of IoT will continue to shape the world. While the challenges for securing your IoT environment may initially appear daunting, the benefits will far out weight any obstacles. A secure IoT ecosystem will open the doors to new revenue streams, new business models, new industry partnerships and critically new ways to engage and delight end users.

About HARMAN Connected Services

HARMAN Connected Services, a leader in software design and development, helps global brands dramatically reduce time-to-market while improving quality and productivity. Our end-to-end software engineering, IoT and data analytics services enable the world's top automotive, mobile and communications and software-enabled businesses drive innovation-led growth. Via our over-the-air (OTA) software update, virtualization and device management solutions we keep billions of mobile, automotive and IoT devices of all sizes and complexity continuously and reliably relevant and secure. The mobile devices and intelligent systems that we power are connected, integrated and protected across all platforms and reach every corner of today's digital world.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

Partner with an industry expert

HARMAN Connected Services, a leader in software design and development, helps global brands dramatically reduce time-to-market while improving quality and productivity. Our end-to-end software engineering, IoT and data analytics services enable the world's top automotive, mobile and communications and software-enabled businesses drive innovation-led growth. Via our over-the-air (OTA) software update, virtualization and device management solutions we keep billions of mobile, automotive and IoT devices of all sizes and complexity continuously and reliably relevant and secure. The mobile devices and intelligent systems that we power are connected, integrated and protected across all platforms and reach every corner of today's digital world. HARMAN Connected Services is a division of HARMAN, the leading global infotainment, audio and software services company.

Visit our website at **https://services.HARMAN.com/**

Entrust Datacard™
Trusted Identities | Secure Transactions

HARMAN
A SAMSUNG COMPANY