Strong Device Identity

Combining Infineon TPMs and GlobalSign Managed PKI to secure connections and enable trusted communications between devices

GlobalSign

Infineon

SOLUTION BLUEPRINT

Purpose

The purpose of this document is to provide information and guidance on implementing the GlobalSign-Infineon Secure Device Identity (SDID) solution, which addresses device identity needs using Infineon's Trusted Platform Modules (TPMs) in combination with GlobalSign's Managed Public Key Infrastructure (PKI) platform.

Contents

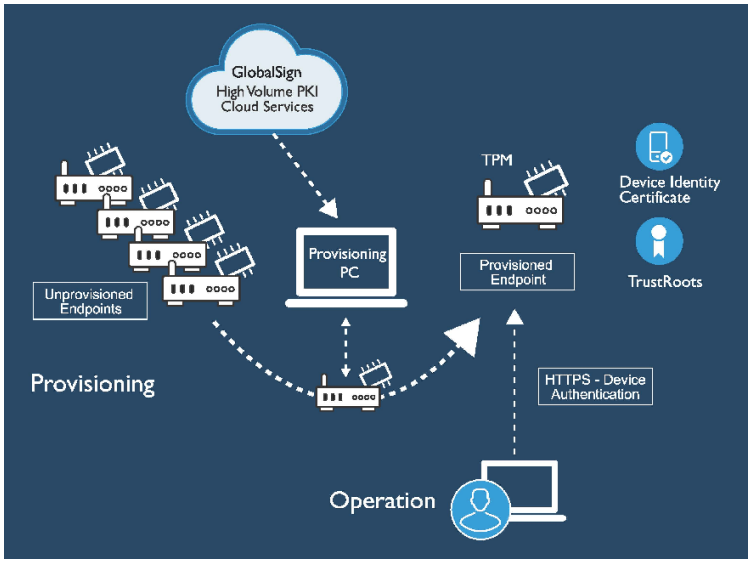
Purpose 2
Introduction 3
Document Audience 3
TPM Tutorial Breakout 4
PKI Tutorial Breakout 4
Core components in a PKI 5
The Value of Strong Device Identity in the Internet of Things 5
Implementing the Secure Device Identity Solution 6
Phase 1: Manufacturing 6
Network requirements of manufacturing environment 6
Mitigation approaches for network connectivity 7
On-premise vs. Cloud PKI solutions 7
Phase 2: Operation 7
Design Considerations 9
System Requirements 9
Software Available for Integration 9
Partners 9
Scaling Capability of the PKI Systems 9
Building vs. buying a PKI Solution 10
Choosing a TPM 11
Security Best Practices 11
Building on Secure Identity 12
Conclusion: Infineon and GlobalSign Partnership Delivers Strong Device Identity 12
Talk to us today to learn how to get started: 12
About Infineon 13
About GlobalSign 13

Introduction

The Internet of Things (IoT) and the broader trends toward smart connected products, systems, and operations are changing many industries, including manufacturing, energy, mining, transportation, healthcare, and networking, by enabling advanced functionality and improved efficiency. As devices become connected to achieve these new value propositions, organizations also adjust their risk profile, creating new concerns for the enterprise and operators.

Forward thinking organizations should consider these new capabilities, which afford auto-configuration and feature licensing, data monitoring, and remote operation of ecosystem assets, while also being mindful toward reducing risks, including counterfeiting, piracy, and network trust. Connected devices rely on trusted communications for safe and secure operations, and trusted communications require strong identity for establishing the channels. In addition, how can a device identity solution address the scale of the IoT, not only in sheer number of devices, but also with the diverse device operating environment? In this light, we present a technical overview for how organizations can address these concerns through Infineon and GlobalSign's Strong Device Identity (SDID) solution.

As illustrated in the diagram below, we will discuss the elements of provisioning a strong device identity in the manufacturing process, as well as then operating the device in a connected environment.



Document Audience

This document assumes many strategic business decisions of why to build a connected product or system solution have already been decided by the organization. The content here is focused on expanding the technical context and details around mitigating environmental and connectivity

risks of a smart, connected solution and proposing a flexible technical solution for these risks. The audience of this document is intended to be fairly technical in nature, expected to fall in roles such as: Technical Architect, Principal Engineer, Solution Engineer, Application Engineer, Product Manager, Security Architect, as well as individuals profiling solutions from a Systems Integrator perspective

TPM Tutorial Breakout

Over the years, embedded systems designers have learned through painful experience that software security alone is not enough for most applications. Hardware security is required to achieve high levels of reliability and security. TPM is one of the most popular ways to implement hardware security.

The Trusted Platform Module (TPM) is a standardized security component that implements a standardized set of hardware security features and commands. The TPM specification was defined by an industry consortium (the Trusted Computing Group) and standardized as an international standard, ISO 11889. Because TPMs are standardized, support for TPM is built into many operating systems already (e.g., Windows, Linux, etc.) and open source libraries to support TPMs are also available.

TPMs provide the following security features:	Which enable the following use cases:
✓ Secured storage for keys and other secrets	✓ Reliable strong device identity
✓ Strong random number generation	✓ Secured communications
✓ Hashing, signing, and signature verification	✓ Remote device management
✓ Encryption and decryption	✓ Anti-counterfeiting
✓ Measured boot and remote attestation	✓ Secured software and firmware updates

For a list of certified TPMs, see the Trusted Computing Group web site at https://www.trustedcomputinggroup.org/membership/certification.

PKI Tutorial Breakout

Public Key Infrastructure (PKI) is a collection of technologies and systems that enable the distribution and usage of keys and certificates - traditionally using the x.509 format. PKI aids in providing cryptographic-based mechanisms to help ascertain the identity of organizations, people, devices, and services.

Deploying PKI allows protection against:	By enabling:
✓ Eavesdropping	✓ Confidentially / Encryption
✓ Tampering	✓ Integrities / Hashing Algorithms
✓ Impersonation	✓ Authentication / Digital Signatures
✓ Repudiation	✓ Non-Repudiation

PKI relies most heavily on asymmetric cryptography. Asymmetric cryptography allows one key (the Public key) to be transmitted in the open, while still enabling trusted and private encryption and signing activities through the protection of the private key.

Core components in a PKI

Certificate Authorities (CAs)

- ✓ These are the core trust anchors in the PKI system and are responsible for signing and maintaining digital certificates issued.

Registration Authorities (RAs)

- ✓ These are the business process focused entities of the PKI system. These services are responsible for verifying identity claims and enforcing policies under which certificates will be signed by the CA.

Validation Authorities

- ✓ These are entities that provide services to verify current validity of a digital certificate.

Digital Certificate

- ✓ This is an electronic document signed by a CA, which attests to the binding of a public key with a set of identifying information to entity which owns a corresponding private key.

The Value of Strong Device Identity in the Internet of Things

Successful IoT systems can provide tremendous positive benefits: innovative products and services, greater efficiency and reliability, and the convenience of smart systems tailored to customer needs. The potential for greater profits is tremendous.

But when things go wrong, those hoped-for profits can quickly turn to massive losses. Consider the steel plant where hacked control systems caused massive equipment damage or the IoT device manufacturer whose fielded products were rapidly infected in a way that could not be remotely repaired, leading to a large and expensive recall.

Fortunately, strong device identity can protect the IoT device manufacturer and customer from the negative impacts of hacking risks, while opening new doors to after-market profits. Here are the key features provided and enabled by the GlobalSign-Infineon Strong Device Identity solution:

- ✓ Confidential upload of sensor data with reliable provenance
- ✓ Secured remote control of devices
- ✓ Remote device management to ensure safety and prevent infections
- ✓ Device autoconfiguration (plug-and-play)
- ✓ Detection and blocking of counterfeit devices
- ✓ After-market sale of features, services, and upgrades
- ✓ Network access control using device identity and integrity

By carefully provisioning devices with a strong device identity when the device is manufactured, these features can even be added with a firmware or software update after the device has shipped.

Implementing the Secure Device Identity Solution

Many design alternatives may be selected, as described in the Design Considerations section below. This section describes the most common method of implementing the Strong Device Identity Solution.

Phase 1: Manufacturing

Device identity provisioning usually occurs towards the end of the manufacturing process. At this point, hardware assembly is complete and the initial software has been loaded. A 'manufacturing PC' is connected to the device to perform device enrollment and identity provisioning. The manufacturing PC is running GlobalSign client code that interacts with the GlobalSign cloud service via a RESTful API.

At the time of device enrollment, the manufacturing PC first establishes a secure connection to the GlobalSign cloud service. The provisioning software then performs the following steps: sending a device identifier to the device, instructing the device to create key pairs and a Certificate Signing Request (CSR) using the TPM, receiving a CSR from the device, and packaging the CSR into the correct API call.

In advanced TPM enrollment scenarios, there may be additional communication steps used between the device and manufacturing PC, which will enable the attestation of the TPM component based on the endorsement certificate of the TPM which was provided by Infineon at the time of TPM manufacturing. GlobalSign's cloud service receives the request from the manufacturing PC, validates the request based on the required business logic, and signs a device identity certificate, which is returned to the manufacturing PC. Upon receiving the signed certificate, the manufacturing PC passes this on to the device, which loads it into the TPM. This entire process generally takes only a few seconds and completes the Strong Device ID provisioning of the device.

Network requirements of manufacturing environment

A core component of the Strong Device Identity solution is the GlobalSign Managed PKI platform. The suggested operational workflow is for the device to get provisioned with an identity towards the end of the manufacturing process when it is being loaded with its firmware and checked by quality control. At that time, the provisioning software on the manufacturing PC needs to connect to the GlobalSign Managed PKI platform, establish a secure connection, and request an identity certificate. The network requirement for this is very low, with a total data consumption of approximately 10KB per device. For this reason, a 100kbps connection is adequate for most manufacturing plants.

Mitigation approaches for network connectivity

Due to the cloud service nature of this solution, it is expected that the provisioning software will be able to access the GlobalSign Managed PKI platform over the internet at the time of device provisioning. However, various factors can lead to outages or disruptions in network connectivity within the manufacturing environment. We suggest that the manufacturer set up a redundant system - a failover network device that will temporarily keep the manufacturing PC connected to the Internet. This can be achieved easily and cost-effectively through satellite cellular data modems. Popular network redundancy designs typically make use of redundancy protocols (RSTP or Link-aggregation) and managed switches in conjunction with alternative sources of cellular connectivity.

On-premise vs. Cloud PKI solutions

While the GlobalSign Managed PKI platform has redundancy, fail-over and disaster recovery built into the platform, GlobalSign is also able to partner with some great providers who are capable of helping design fail-over on-premise network solutions, which greatly reduces or eliminates the probability of network outages. This means you can benefit from cloud-based value propositions including:

- ✓ GlobalSign can make fixes to core services remotely and maintain it without coming to your site
- ✓ You can't have someone physically tamper with the service because it's in the cloud
- ✓ Auditing and record keeping can be maintained safely offsite and requested at any time from GlobalSign

GlobalSign takes security very seriously. In addition to operating the infrastructure under best practices, they are Web-Trust Compliant. Their certificate management platform does not communicate without encryption. GlobalSign leverages PKI, certificates and mutual authentication to ensure that only the right people have access to the platform and that they have access to the right places within the platform.

When adopting a cloud-based solution like the one GlobalSign offers, you can save money by eliminating a need for an appliance-based solution, which will inevitably lead to more on site support and maintenance costs. You can rely on a focused party to maintain and update the cloud services, keep auditing and records safe and keep people from tampering with the service.

Phase 2: Operation

Now in the Operation phase, we'll cover the usage of this newly minted device identity from the Manufacturing phase. The Operation phase covers the usage of the device as part of a larger system.

The operation model and trust model will depend greatly on the nature of the overall system architecture, which varies from one application to another. However, PKI-based credentials in

the Secure Device Identity solution leverage the X.509 standard, so they are very flexible and interoperable across a wide variety of software, operating systems, and communication protocols. Flavors or views of the trust model might look at the following relationships:

- ✓ Device to Cloud
- ✓ Device as Gateway to Cloud
- ✓ Device to Device
- ✓ Device to User

Here we'll dive a bit further into the common use case of Device to Cloud or Device as Gateway to Cloud.

When the device attempts to connect to the cloud, the device should be configured to present its client certificate as part of the authentication process. One of the most common protocols to do this is TLS / SSL. When the initial handshake between the device and the cloud occurs, the server will request the device's certificate, which contains the public key associated with the private key (the private key is protected by the TPM capabilities).

When the server receives the certificate, it has the ability to perform a range of validation logic checks on the data contained in the certificate. Often first and most essential is a challenge to assert that the device in fact contains the private key that is associated with the public key in the certificate. This typically involves encrypting a random string with the public key, and requiring the device to decrypt it. After that validation, the server likely also wants to check that the certificate is signed by a trusted root CA and likely that the certificate is not revoked by checking via CRL or OCSP. The server accomplishes this by checking the name of the issuing entity as well as the digital signature in the certificate, and ensuring that that data matches with its pre-configured trust store of CAs.

If all those checks pass, then the server is able to trust the device and bootstrap into an encrypted communication channel with the device to perform the required task, whether it's collecting data, being a proxy for communications, or issuing commands.

Ultimately the scenario described is going to be slightly different for each use case. All the following components are important in the solution implementation, as well as the enforcement of validation rules and logic:

- ✓ Communication protocols and interfaces between device to gateway, device to cloud
- ✓ Operating software and hardware environment of relying parties - both server/cloud, gateway/device
- ✓ Variety of devices that will be authenticating, and if there are any logical differences between them in the authentication validation

- ✓ Type of relying parties, and the approach to distribute the trust anchors (CA certificates) into the environment

Design Considerations

When building the Strong Device Identity solution into an IoT product or system, the following issues should be carefully considered.

System Requirements

Can PKI and TPM really fit into a small embedded system? Yes. Many embedded systems already include PKI and TPM, from Smart Home gateways to slot machines. The key is to simplify your design and only include the features needed for your product. PKI can be considered as an information security toolbox in which you can select and choose the components that meet your requirements, some of which might be a resource-constrained environment. For example, to reduce bandwidth, processor usage, and connectivity requirements, you might not need to do revocation checking and certificate chain validation for server certificates in your device. You can build a device trust model relying on a single CA for issuing server certificates. If a server certificate is revoked (which shouldn't be necessary), blacklist it via a software update.

Software Available for Integration

If you need a full PKI and TPM implementation, you can use OpenSSL and TSS. But if you only need a subset of the standard PKI and TPM features, talk to one of the companies that makes embedded security software libraries. Many of them are adding support for TPM.

The Trusted Computing Group Software Stack (TSS) provides a standardized API for building trusted computing applications. The TSS' hardware-abstracted design allows for portability across a diverse range of operating environments such as Windows®, Linux, and more. Commercial and open-source implementations of the TSS offer choices in terms of licensing, support, and cost. The TPM is particularly well suited for systems which require advanced security features, such as software integrity measurement and remote attestation.

Partners

Although any engineer can add strong device identity to an IoT device or system, gaining the help of a partner who has experience in this area will pay real benefits. For example, designing a secured firmware upgrade system is beyond the scope of this document, but is needed for every IoT device. Both GlobalSign and Infineon have networks of experienced partners who can help with your design and even supply to you software libraries and services that are much cheaper to buy than for you to rebuild.

Scaling Capability of the PKI Systems

There are many organizations, companies, nation states and global entities that are trying to setup large Industrial IoT systems to realize the potential benefits that it brings. However, scaling an Industrial Internet System (IIS) comes with its own set of challenges – issues of how

scale to a large number of devices safely and securely, how to manage their lifecycle, and how to makes these compatible and interoperable with current and future disparate systems.

The PKI model traditionally used in the enterprise lends itself very well to addressing these challenges while still being used for these applications, as it can be implemented in a relatively lightweight fashion on different classes of IoT devices. However, the scale of IoT brings a new range of challenges, including how to provision massive numbers of identities, as well as how to verify them in operation.

The number of identities served by the top five Certificate Authorities (CAs) in the world ranges in the tens of millions and has slowly grown over a long period of time. In contrast, IoT hardware manufactures often wish to bring to market tens or hundreds of thousands of devices at a time. Multiplying that by several hardware revisions or generations, new and unprecedented scales are reached. Identities must also be delivered to the entire batch of devices before they reach the shelves, at the speed of the assembly line.

GlobalSign offers a high volume, secure and scalable, geographically distributed platform that is able to create thousands of digital identities each second and manage billions of them. This platform uses traditional PKI principles (X.509 certificates), enabling this system to be massively scalable, redundant and fault-tolerant while still being interoperable. The high per-second throughput rate can match that of high volume manufacturing on the assembly-line.

When PKI is operated in the field, one of the benefits of the technology is that the relying parties don't need to connect to a database or integrate into a 3rd party system to verify the credentials. This aids in the operation scale that PKI can afford as the validation of clients using certificates, can be done based on the roots of trust. If the relying parties are configured to trust the roots that sign the certificates, then they are able to efficiently and simply authenticate enormous ecosystems of devices.

Building vs. buying a PKI Solution

There are a number of reasons why cloud services are a great option to consider in your infrastructure. The main one following the traditional build vs. buy decisions - that if you're building an IoT ecosystem, product, or service, you want to be able to focus on the value proposition of that offering. Security often won't be at the forefront of the offering, but will be a requirement or expectation from the customers or stakeholders of the system. Dedicating resources toward building the core of your platform, while choosing the right services to buy and integrate is a proven strategy. This strategy, if done with sound security guidance and planning, not only offers a competitive cost model, but also allows the best security and identity management to be used.

GlobalSign can offer that security guidance and consultation. Additionally, to establish a strong, hardware based root of trust, this burden of this trust and risk management is better left to the experts. Being a large public CA with deep experience in PKI, GlobalSign can be that expert.

Choosing a TPM

When choosing a TPM, you have many options. For low-security applications, a software or firmware TPM may be adequate. But for applications where security is a high priority, there is no substitute for a "discrete TPM" – a separate chip that is designed and built by security experts with security as the top priority. Such a chip should have a security evaluation from an independent certification lab for at least EAL 4+ and be certified by the Trusted Computing Group as a compliant TPM.

Infineon is the market leader in TPMs, providing a broad range of products with different interfaces (LPC, SPI, I^2C), packaging, cryptographic algorithms, and temperature ranges. Infineon offers TPMs that support the well-established TPM 1.2 specifications as well as the newer and more flexible TPM 2.0. Customers can even purchase Infineon TPMs that can receive and install downloaded upgrades in the field as technology advances, providing the flexibility needed to maintain security for a long lifetime.

Whichever TPM you choose, you can be sure that the same standard set of commands and APIs will work with that TPM.

Security Best Practices

Security is much more than device identity. To build a secure system, secure techniques should be employed from system design through implementation, testing, operations, maintenance, and decommissioning. These techniques must include not only the device hardware, firmware, and software but also any services upon which the device depends.

Planning for resiliency is always a good idea. If one device fails or becomes infected, this should be detected so that the overall system can continue to function while the device is repaired.

The key message that we want to drive home is that Security should be thought of as central to any decision that is made with regards to your product – not as a feature, tool or subsequent add-on. As such, we advocate a 'security by design' mindset where at every step in the product and system design, implementation and operational process, we keep in mind the security rules and practices that are both required and preferred. Existing countermeasures in place should be continuously revalidated against new threats and attack vectors.

Along with these security principles, we advocate a 'privacy by design' mindset where data and resource privacy is considered and enabled from the start of any project and process.

While cybersecurity risks have always been on the radar of IT departments, with the advent of the IIoT, the OT (Operational Technology) groups within an organization also need to learn and plan for these threats. Various industry specific security guidance is available, for example NIST SP-800-161 has best practices for supply chain risk assessment and management for US federal agencies; while in manufacturing a similar resource is the ISO/IEC 27036-1:2014.

Building on Secure Identity

Once a secure device identity is included in your device, many features can be built using it. Although we don't have time to describe each of these in depth, a quick review is in order.

Secured communications is an obvious first step. Use the device identity to establish an authenticated, integrity-protected, and encrypted channel to upload sensor data and receive commands. But this is only the tip of the iceberg. Device owners can use device identity for their own purposes such as secure remote management and network access control. The remote attestation features of the TPM can be used to remotely monitor device health and ensure that firmware and software updates have been properly applied to the device. Manufacturers can tie licensed features to an individual device, enabling after-market feature upgrades and subscription services. And counterfeit devices can be identified and blocked to ensure safety.

Re-building Secure Identity

Depending on the device environment operators may have the need or desire to re-provision device identity certificates, either due to compromised/misbehaving devices, or for updating key material or cryptographic algorithms. Architects in this scenario will need to understand how to fall back toward a lower component of trusted elements, likely the TPM, to re-establish the trust chain and recreate or provision an updated identity of the device. There are other use cases architects may wish to consider for updating credentials in the field, one being a regular key material update.

Conclusion: Infineon and GlobalSign Partnership Delivers Strong Device Identity

IoT providers/manufacturers must address critical security concerns including authentication, privacy and integrity. Mitigating risks in securing trust credentials, as well as building proven solutions at IoT scale, are addressed in the Infineon and GlobalSign partnership, which combines Infineon's OPTIGA TPM with GlobalSign's Managed PKI platform.

The combined Strong Device Identity solution enables the provisioning and operation of IoT endpoints to leverage PKI and secure hardware in a scalable method. The joint solution reduces risks, such as key compromise and identity spoofing, while also being able to extend trust and deployment models at massive scale.

Talk to us today to learn how to get started:

Infineon provides a variety of TPMs and other hardware security chips suitable for IoT applications. Learn more: www.infineon.com/iot-security/.

GlobalSign offers a Managed PKI platform to meet the scalable security demands of your IoT ecosystem. Learn more: www.globalsign.com/en/internet-of-things/.

About Infineon

Infineon Technologies AG is a world leader in semiconductor solutions that make life easier, safer and greener. Microelectronics from Infineon is the key to a better future. In the 2016 fiscal year (ending September 30), the company reported sales of about Euro 6.5 billion with more than 36,000 employees worldwide. Infineon is listed on the Frankfurt Stock Exchange (ticker symbol: IFX) and in the USA on the over-the-counter market OTCQX International Premier (ticker symbol: IFNNY).

About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud-based service providers and IoT innovators around the world to conduct secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale PKI and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE). The company has offices in the Americas, Europe and Asia.

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00
sales@globalsign.com
www.globalsign.com