



# Hardware-based Secure Identities for machines in smart factories

**Martin Klimke**

Lead Principal for Technical Marketing Chip Card & Security

**Dr. Josef Haid**

Principal for Technical Marketing Chip Card & Security

[www.infineon.com/security-for-smart-factories](http://www.infineon.com/security-for-smart-factories)



# Abstract

Security is a top priority in in the manufacturing sector. Decentralized, automated smart factories rely heavily on network technologies, making them vulnerable to attacks from outside and accentuating the need for more robust security. Within the framework of Industry 4.0 – a term used to describe the technologie and concepts used in smart factories – security is vital for enabling manufacturers to capitalize on the benefits offered by the Internet of Things (IoT).

Typical security applications and use cases include unique component authentication, monitoring and safeguarding system integrity and protection of data and communication. Effective IP protection is a further key enabler in the successful delivery of new, trustworthy services and tech-

nologies. To develop suitable security solution concepts, designers need integrated, hardware-based system solutions capable of protecting infrastructures and components against attacks, fraud and sabotage.

Secure Identities are the cornerstone of security concepts for smart factories. This whitepaper looks at how Secure Identities can be implemented in industrial automation systems.

**“85 percent of responding companies will have implemented Industry 4.0 technologies in their key areas by 2020”**

**Source: Strategy& and PWC**

# Content

|   |    |
|---|----|
| Secure Identities enable security solutions for smart factories | 4  |
| Hardware- based trust anchors for Secure Identities             | 6  |
| The value of hardware-based trust anchors                       | 9  |
| Using Trusted Platform Modules as standardized trust anchors    | 11 |
| Summary   | 11 |

# Secure Identities enable security solutions for smart factories

The conventional manufacturing landscape is changing. More and more machines, warehouse systems, resources and products are being intelligently networked around the globe, leading to the creation of smart, connected factories. All this connectivity, however, is opening virtual factory doors around the world to an enormous – and constantly rising – stream of data traffic. This flow of data must be protected at every step in the production process.

The rapid and successful development of smart factories worldwide is thus presenting many manufacturing companies with new security challenges. Malware, manipulation, sabotage, faulty firmware updates and counterfeit components are all digital threats that can bring entire production lines to a halt and lead to significant costs for manufacturers. Any security gap in a company's infrastructure may result in the theft of data, intellectual property (IP) and process know-how. This sensitive information is often what gives a company its competitive edge and therefore requires special protection.

## Secure Identities

### Enabling and supporting

**Unique identification**



**System integrity protection**



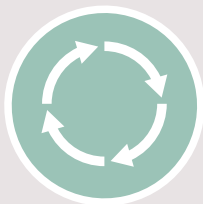
**Network protection**



**Automated commercial process enabling**



**Lifecycle management**



**Remote Access management**



**And more**





As a result, security standards in industrial automation need to be tightened as we move forward. This calls for tailored solutions that deliver end-to-end protection yet also strike the right balance between security performance requirements and financial constraints. Manufacturers need powerful, reliable security technologies to safeguard communication between devices and machines within heavily networked infrastructures.

Secure Identities provide the anchor for all measures to protect electronic communication and stored data. Just as people use ID cards or passports to identify themselves every day, machines also need Secure Identities to communicate safely in a networked environment. As a result, these Secure Identities have to be protected against manipulation, duplication and theft.

“Secure Identities form the anchor for security solutions in smart factories.”

From a technology perspective, Secure Identities are essential for implementing the cryptographic measures used to protect against digital threats. These include measures that prevent unintended software updates on computers in automation systems as well as measures that protect stored data and communication networks. Secure Identities will also be increasingly used in automated commercial contexts to maintain trust between the transacting parties.


# Hardware- based trust anchors for Secure Identities

Secure Identities are established using secret keys and cryptographic processes that utilize secret keys. They are fundamental for the entire chain of security measures required to protect industrial automation systems.

When it comes to security, there is no one-size-fits-all solution for industrial automation systems. Thorough risk analyses have to be carried out to identify the specific threats to individual systems. In most cases, Secure Identities are exposed to a high level of threat as they are used to protect know-how and intellectual property, safeguard the integrity of industrial automation systems and protect stored data and data distributed over networks. Hardware-based security solutions provide the robust levels of security required to protect secure identities.

**Secure Identities are established using secret keys and cryptographic processes. Hardware-based solutions provide robust security performance and make it hard for attackers to extract secrets.**

Hardware-based solutions such as those provided by security controllers deliver a greater level of security than software-only concepts. Software-only solutions often do not deliver robust security performance. This is because it is relatively simple to read and overwrite software, which, in turn, makes it easy for attackers to extract secret keys. In contrast, security controllers can be used to store access data and keys in much the same way as a safe is used to store confidential documents.



## Comparing hard- and software trust anchors

|         |                      | Main CPU | SW | Main CPU | SW | HW |
|---------|----------------------|----------|----|----------|----|----|
| Product | Crypto functionality |          | ✓  |          | ✓  |    |
|         | Security certified   |          | ✗  |          | ✓  |    |
|         | Tamper resistant     |          | ✗  |          | ✓  |    |
|         | Secure sourcing      |          | ✗  |          | ✓  |    |
| Process | Secure manufacturing |          | ✗  |          | ✓  |    |
|         | Secure shipment      |          | ✗  |          | ✓  |    |

In order to protect systems, security chips are integrated at all critical nodes and used as secured hardware anchors. These chips can check component authenticity and system integrity to detect manipulation. They also check and protect data confidentiality.

Hardware trust anchors provide secured storage for keys and also execute the associated cryptographic processes that use these keys. Identities and rights such as licenses can be linked to keys. Hardware trust anchors support the secured key management function required to grant and revoke these rights in operational mode.

Hardware trust anchors are also used to check the authenticity of software updates and protect remote access activities. In addition, they offer robust protection against low-quality, counterfeit spare parts and repair tools. This is because the manufacturer certificates integrated into the anchors can easily check the authenticity of prospective accessories and new parts.



## Key integrity is essential for system security

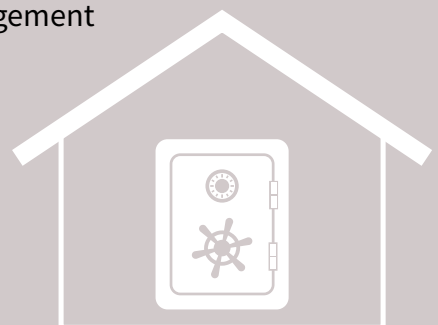
1 Compromised keys = no security

2 Cloning of key leaves no traces

3 Key handling must be secured through the whole lifecycle including manufacturing

### Trust anchors

- > Key store
- > Crypto operation
- > Key management







# The value of hardware-based trust anchors

Dedicated security components that function as hardware-based trust anchors have long proven their value in other industries, including the PC and server segments. Very similar technologies have also been used in chip cards and identification documents to effectively protect large infrastructures for many years now. Today, this technology is increasingly making its way into industrial manufacturing equipment.

Trust anchors provide cryptographic functionality such as public key cryptography and key management. These functions can be implemented in software and hardware. For industrial applications, however, a hardware-based solution such as a dedicated security chip has clear benefits and can add real value for manufacturers.

**“Hardware-based trust anchors reduce infrastructure costs.”**

Silicon manufacturers use highly secured, certified processes to personalize hardware-based trust anchors, for example, assigning a Secure Identity to individual security chips. In many cases, this involves storing a set of keys and certificates on the chip, which allows other devices in the same industrial automation system to securely authenticate remote devices, establish secured connections and exchange data securely.

Proper hardware anchors are security-certified components. This means that they are also equipped with measures to protect them against physical attacks and are therefore secured during transit. In other words, a hardware anchor's protection is so robust that the dispatcher can reduce costs for special security measures during shipping and can therefore send it via cost-efficient logistics channels. This not only applies to the security chip itself but, more importantly, to devices that contain a hardware anchor with customer-specific keys. These physical protection capabilities can reduce costs particularly during installation and delivery processes.

Using security chips as trust anchors is therefore beneficial for manufacturers as they do not have to transfer unencrypted keys to their devices. This saves security infrastructure costs at the factory and also increases process security.

Security chips also provide greater flexibility in production. If a device manufacturer wants to outsource production, for example, the fact that keys can be securely transferred from the personalization server to the hardware anchor makes it much easier for them to choose a contractor because the third-party companies no longer have to meet such strict security requirements. This saves significant costs, in many cases offsetting the original cost of the security chip.



#### Device authentication

- > One-way authentication
- > Mutual authentication



#### Trust anchor

- > Secured boot
- > Memory integrity



#### Secured channel

- > Key generation
- > DH/ECDH key exchange



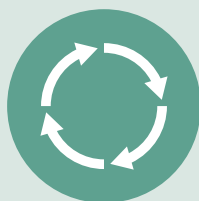
#### Information integrity

- > Command integrity
- > Message integrity
- > Data integrity



#### Audit information

- > Incident logs
- > Protected storage



#### Lifecycle management

- > Supply chain tracking
- > Lifecycle counter



#### Secured updates

- > Secured channel
- > Access control



#### Secure Clock and Time

- > Reliable clock when offline
- > Timer and Monotonic Counter

Figure: Broad range of security-relevant use cases supported by a Trusted Platform Module (TPM).

# Using Trusted Platform Modules as standardized trust anchors

A Trusted Platform Module (TPM) is a dedicated security chip that enables a more secure computing environment. In the past, TPMs were primarily used in the computer industry. In recent years, however, other industries, including industrial automation, have started to realize the value of TPMs in protecting industrial applications.

Unlike proprietary solutions, TPMs such as Infineon's OPTIGA™ TPM come with a standardized scope of functionality defined by the international standard ISO/IEC 11889. This means that customers can build on existing security solutions and benefit from the expertise and many years of experience that specialist manufacturers have developed and channeled into their products. This includes process chains extending from development through production to delivery. The ability to reuse existing software and processes reduces security risks. Professional solutions available on the market have to undergo rigorous test cycles to check they meet strict requirements. They also support a broad application spectrum.

TPMs implement Secure Identities very efficiently. When the TPM is produced, the silicon manufacturer uses a secured, certified process to embed a unique endorsement certificate and a corresponding secret, private key in the TPM. Based on this key, the manufacturer can use a cryptographic process to cost-effectively check that the TPM is from a trustworthy source and not a counterfeit. This key can also be used to securely embed additional keys in the device that contains the TPM. To do this, the endorsement certificate is used to establish an encrypted line of communication with the customer personalization system.

Once the key material has been stored on the TPM, it serves as a powerful hardware anchor for a wide range of security measures, including the two use-cases described above.

## Summary

The entire concept of smart factories hinges on security. The success of smart factories and Industry 4.0 as a whole depends on manufacturers' ability to cryptographically and securely identify machines and devices. Hardware trust

anchors provide robust protection for these keys and can lower overall security costs for device manufacturers. Trusted Platform Modules (TPMs) offer a standardized solution for efficiently implementing Secure Identities.

**Infineon Technologies AG**

81726 Munich  
Germany

Published by  
Infineon Technologies AG

© 2016 Infineon Technologies AG.  
All rights reserved.

Order number: B189-I0326-V1-7600-EU-EC  
Date: 06 / 2016

[www.infineon.com](http://www.infineon.com)

