infineon

Security Partner Preferred

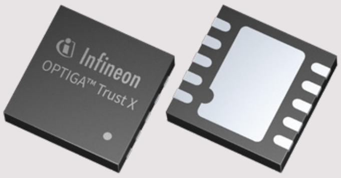
Partner Use Case

Secured Provisioning Services for hardware based security devices

Arrow Electronics offers Secured Provisioning Services for hardware based security devices, such as the OPTIGA™ Trust X. These Services enable customers of all sales and demand profiles to take full advantage of silicon based security features.

Products

OPTIGA™ Trust X



Use case

Application context and security requirements

With the increase of connected devices and applications to the internet, the need for strong device authentication with the cloud and secured communication protocol is of the utmost importance.
Infineon offers the OPTIGA™ Trust X as a turnkey security solution for industrial automation systems, smart homes, consumer devices and medical devices. This high-end security controller comes with full system integration support for easy and cost-effective deployment of high-end security for your assets.

Challenge

Implementing strong end-to-end security solutions requires (a) the establishment of a secured Chain of Trust throughout the supply chain; (b) Secured Development Lifecycle; (c) Device Management in the Cloud; (d) Cybersecurity. All these aspects of the supply chain must be involved and measures need to be taken to provide this Chain of Trust. This requires knowledge and investments in infrastructure, technology and processes.

Implementation

Arrow Electronics is now offering Secured Programming and Provisioning Technology, based on a highly secured and reliable chain of trust, taking care of the implementation of security at the important first part of the supply chain. Arrow Electronics has the infrastructure, technology and knowledge to enable customers of all sales and demand profiles to take full advantage of silicon based security features.

Benefits for the user

- User can rely on device authentication, based on a highly secured Chain of Trust embedded in their applications at reasonable cost
- Users are protected from counterfeit products
- Users can protect their critical data from being tampered with at the source or in transit to the cloud
- Users can trust their devices and can verify the status via remote attestation

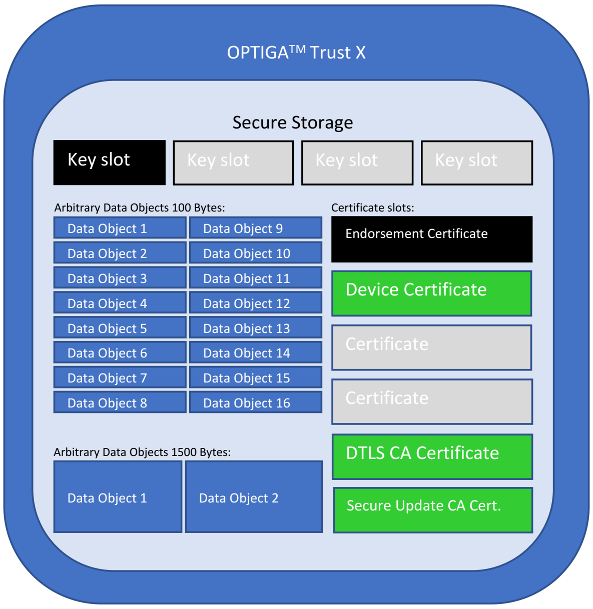
Further benefits for Original Equipment Manufacturers (OEMs)

- OEMs are protected from third parties cloning their products, thus protecting the user experience and the company's brand
- OEMS can protect their networks / clouds from unauthorized devices
- OEMs can control the number of devices that are built per batch, thus protecting against overbuilding by the manufacturer
- OEMs can centralize their security focus on 1 supplier (Arrow Electronics), instead of managing security processes at multiple contract manufacturers

Solution

The OPTIGA™ Trust X comes with 4 Elliptic-curve cryptography (ECC) based key slots. During production at Infineon fab, unique asymmetric keys (private and public) are generated. The private key is securely stored in the first key slot. The public key is signed by the Infineon Certificate Authority (CA) and the resulting X.509 certificate (Endorsement Certificate) issued is securely stored in the first certificate slot.

As the chip is shipped to Arrow Electronics, the origin of the chip can be proven by validating the certificate inside of OPTIGA™ Trust X against the Infineon CA (also called chip authenticity). As a next step the public key is taken from this certificate and a new customer specific certificate is generated during the provisioning service provider (Arrow Electronics).
This closes the Chain of Trust between Infineon and Arrow.



The remaining 3 keys can be provisioned upon customer request and can be used for multiple crypto functions, depending on the use case.

The 2nd certificate slot (Device Certificate) is typically used to securely store the certificate of the public key, belonging to the first private key, but now signed by the customer's specific CA (also called "Signing CA" or "Intermediate CA"). This Device Certificate can be provided with a customer specified unique serial number.

The Authentication Trust Anchor serves multiple use-cases. One typical provisioning example is the CA Certificate for Data Transport Layer Security (DTLS).

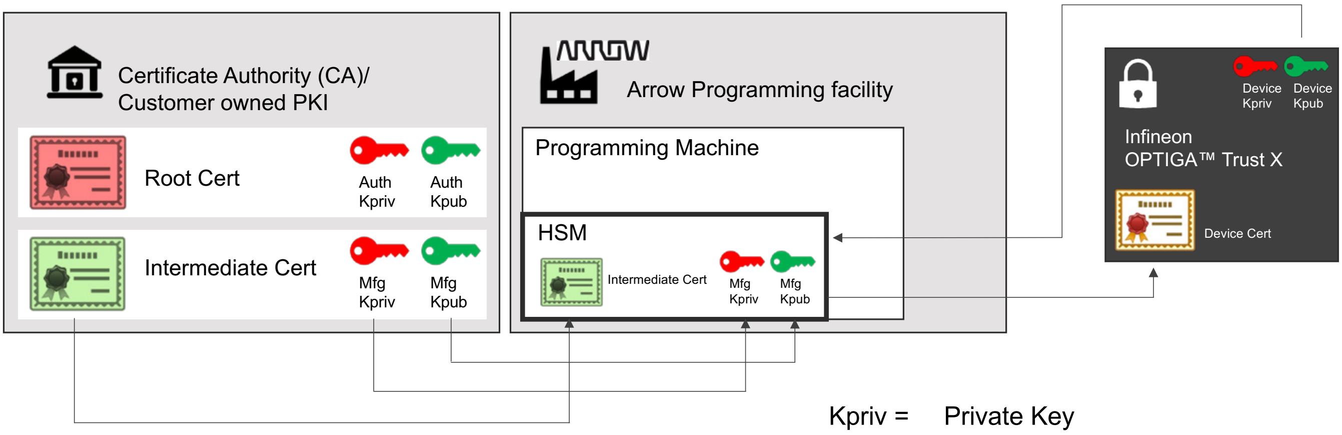
OPTIGA™ Trust X also provides a Firmware Update Anchor (Secured Update CA Certificate), where the certificate can be provisioned for Secured Update purposes.

Finally, the OPTIGA™ Trust X provides 2 additional certificate slots, 16 Arbitrary Data Object slots of 100 Bytes each and 2 Arbitrary Data Object slots of 1,500 Bytes each.

Solution

Certificate Authority

The customer's specific CA is used to sign the device public key, creating a X.509 certificate that is linked to the customer's chain of trust.



Kpriv	=	Private Key
Kpub	=	Public Key
Auth	=	(Certificate) Authority
Mfg	=	Manufacturer (provisioning the devices)
HSM	=	Hardware Security Module

This customer specific CA comes from either the customer or an external Certificate Authority.

Not all customers have an own Public Key Infrastructure (PKI). Arrow Electronics has partnered up with a leading global Certificate Authority that can provide the Chain of Trust to the customer.

The Global Certificate Authority maintains a highly secured PKI, in which the customer specific Root CA and Intermediate CA can be created, protected and maintained. Arrow Electronics takes care of management, coordination and stays the single point of contact for the customer.

Secured transfer of credentials

The intermediate CA needs to be securely transferred and installed in the Hardware Security Module (HSM) that is cryptographically integrated in the state of the art, highly secured programming machine.

For this process of secured transfer, a private-public key pair is created inside the HSM of the programming machine. The public key is being provided to the customer, along with a secret wrapping tool. The secret wrapping tool and the public key are used to securely wrap the Intermediate CA. Next, the encrypted Intermediate CA will be securely transferred to Arrow Electronics. Finally the encrypted Intermediate CA is securely installed inside the HSM, where it is decrypted only during the provisioning process.

The secured transfer from public key, wrapping tool and encrypted Intermediate CA, happens through Arrow's Secured FileShare Service, based on Advanced Encryption Standard (AES) and Transport Layer Security (TLS) encryption.

Infineon Security Partner Preferred

Solution

Provisioning Process

The provisioning of customer credentials and data takes place on a state of the art, highly secured programming platform. Within Arrow Global Programming Services, Arrow has installed multiple systems in multiple regions and can serve customers globally.

Arrow's facility and secured provisioning processes have been validated by Infineon and approved to provision the OPTIGA™ Trust E and X Secure Elements.

Certificate Lifecycle Management Services

Through the partnership with the External Certificate Authority, Arrow Electronics offers optionally Certificate Lifecycle Management Services, consisting out of Reporting Services, Online Certificate Status Services (OCSP) and Revocation Services.

The customer will get access to a web portal where these services can be managed and/or monitored.

Support and enable Just-In-Time registration at Cloud

Arrow's infrastructure, processes and services support and enable customers with connection to multiple cloud service providers.

Using the OPTIGA™ Trust X, securely provisioned by Arrow Electronics, a highly secured application and connection to the cloud can be realized.

A two-way authentication process takes place between the edge device and the cloud infrastructure using standard TLS handshaking protocol.

An end-to-end crypto binding is established that provides integrity and confidentiality. Once this process takes place, the cloud provides authorization for the device to join the network and starts providing the service.

Main benefits of the Infineon product

The best-fit security solution for IoT devices, to protect your business as well as your customers' data and Intellectual Property (IP). The OPTIGA™ Trust X is easy to integrate and work with, reducing your design effort for faster time-to-market. This product enables new features and business models that empower you to differentiate your offering, stay ahead of the competition and grow.

The OPTIGA™ Trust X is available in two temperature ranges. Standard for most commercial implementations, and extended to meet the requirements of harsh industrial environments.

Infineon Security Partner Preferred

Partner

ARROW

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

Arrow

Arrow Electronics is a global provider of products, services and solutions to industrial and commercial users of electronic components and enterprise computing solutions. Arrow serves as a supply channel partner for more than 150,000 original equipment manufacturers, value-added resellers, contract manufacturers, and commercial customers through a global network. The company maintains over 300 sales facilities and 45 distribution and value-added centers, serving over 80 countries.

For more information, please visit: www.arrow.com.

Arrow's contribution to the Infineon Security Partner Network

Arrow Electronics offers Secured Provisioning Services for hardware based security devices, such as the OPTIGA™ Trust X. These Services enable customers of all sales and demand profiles to take full advantage of silicon based security features. This programming and provisioning technology is based on a highly secured and reliable chain of trust, consisting out of:

- Partnership with leading global Certificate Authority
- Secured transfer of customer Intellectual Property and security credentials to secured equipment
- State of the art, highly secured programming platform
- Optional certificate lifecycle management services
- Support and enable just-in-time registration at cloud

Solutions for every step of IoT: Arrow Electronics is uniquely positioned to offer complete end-to-end security solutions, including cybersecurity. These Secured Provisioning Services are just one building block out of Arrow's comprehensive portfolio of technology from sensors, wireless connectivity, gateways to cloud platforms, data ingestion, aggregation and visualization, analytics, and security. Service capabilities span ideation, design, integration, manufacturing, logistics, financing, wireless connectivity with billing services, marketing, monitoring and managed services, and sustainable and secured end of life cycle disposition.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 12 / 2018

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!

THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.