Industrial Ethernet Security Harmonization Group

_____

FAQ ON INDUSTRIAL ETHERNET SECURITY CONCEPTS

Version 1.0 | September 19, 2022

Disclaimer

Prepared by Industrial Ethernet Security Harmonization Group, consisting of the Standards Developing Organizations (SDOs):

- PI (PROFIBUS&PROFINET International)
- ODVA, Inc.
- OPC Foundation
- FCG (FieldComm Group)

Core group members contributing (alphabetic order):

Andreas Walz (PI)
Dave Berndt (FCG)
Jack Visoky (ODVA)
Joachim Koppers (PI)
Joakim Wiberg (ODVA)
Randy Armstrong (OPC Foundation)
Sean Vincent (FCG)
Simon Merklin (PI)

Comments to be submitted to working group editor: simon.merklin@endress.com

Content

Preamble

This document was created to shed light on different topics of the security concepts of industrial automation environments.

Please be aware that this is a living document which will be updated and is not meant to be exhaustive. Over time, when this working group works on further topics, more content will be added.

Basic knowledge of Industrial Ethernet Security concepts is assumed.

1 Introduction and scope

This FAQ is intended to answer frequently asked questions regarding Industrial Ethernet security concepts.

Question:

Who is the Industrial Ethernet Security Harmonization Group (IESHG)?

Answer:

The Industrial Ethernet Security Harmonization Group meets on a regular basis to discuss security topics in the industrial automation context. The goal of this group is the alignment of Industrial Ethernet security concepts, so that end users of the protocols have less complexity when using security in their automation systems.

The group consists of representatives of the following four standards developing organizations (SDOs):

- OPC Foundation
- ODVA, Inc.
- Profibus & Profinet International
- FieldComm Group

Question:

Who is the intended audience for this FAQ?

Answer:

End users of Industrial Ethernet protocols, such as plant operators, who want to gain knowledge concerning Industrial Ethernet security concepts.

System integrators and product suppliers who want to know which concepts will help their customers to improve Industrial Ethernet security.

2 General concepts and terms

2.1 Evolution of security in industrial automation plants

Question:

Why do I need to care about security in my industrial plant?

Answer:

Due to the convergence of IT and OT levels in industrial plants, the expectations concerning security have changed. Production plants are not air-gapped anymore due to digitalization and leveraging of field data. Plant networks can't be assumed anymore to be trusted by default. Therefore, plant operators need to have new concepts and approaches for plant security.

2.2 Public-key cryptography and digital certificates

Question:

Why do I need public-key cryptography and digital certificates in my industrial environment?

Answer:
Ensuring secure industrial communications requires the distribution of cryptographic keys to all relevant entities (see Table 1 for a list). Public-key cryptography provides the most cost-effective mechanism to do this. Public-key cryptography makes use of "key pairs" (one public and one private). The public-key is packaged in an electronic document called a "Certificate" that identifies the owner of the key pair. The private key is securely stored on the application's machine and is only accessible to the owner.

2.3 Public-key infrastructure (PKI)

Question:

What is a PKI and why do I need it in the industrial environment?

Answer:
To communicate with a peer, an application needs the certificate of the peer. Secure communication protocols include a mechanism to exchange these certificates. However, communication is not secure until both sides verify the certificate provided by their peer. The infrastructure used to create, distribute, and verify certificates and their private keys is called public-key infrastructure (PKI). A PKI has three logical functions: the Certificate Authority (CA), the Registration Authority (RA) and the Certificate Revocation List (CRL) issuing point.

2.4 Certificate Authority (CA)

Question:

What is a Certificate Authority?

Answer:

PKI defines Certificate Authorities which are responsible to sign so-called certificate signing requests forwarded from a Registration Authority. Certificate Authorities have one or more “Certificate Authority Certificates” which represent the certificate hierarchy in the plant.

2.5 Registration Authority (RA)

Question:

What is the function of a Registration Authority?

Answer:

A Registration Authority provides the decision function of whether a certificate is to be issued to a given requestor. A Certificate Authority and Registration Authority may be embedded within one application but are logically distinct functions. A policy might support making automated decisions. An example is a network service that has received a request for a new certificate could send a notification to the administrator’s cell phone.

2.6 Certificate Revocation Mechanism and Certificate Revocation Lists (CRL)

Question:

Why do Certificates need to be revoked?

Answer:

Public-key certificates are forward-looking claims, which in the course of time might become false (e.g., because of key compromise). Certificate issuers, therefore, need a way to revoke certificates.

Question:

How does the Certificate Revocation Mechanism work?

Answer

Certificate Authorities maintain “Certificate Revocation Lists” (CRL) which contain the identifiers of Certificates signed by the Certificate Authority that are no longer valid. For this reason, a certificate revocation mechanism must be in place. This mechanism provides the ability to verify if a certificate is still valid or has been revoked by the authority that issued it.

Question:

What is the difference between an offline and an online CRL?

Answer:

There are two strategies for doing this Certificate Revocation check:

1) Rely on an offline file, called offline CRL, which contains a list of revoked certificates. The devices reject communication from peers that are in that list.
2) Rely on an online service, that will check the identity of the certificate of the peer online and will return a flag indicating whether the certificate is valid. If the flag is not valid, communication from that peer is rejected.

The online service is easier to maintain as one does not need to have a mechanism to distribute and update these files. However, in industrial environments, it is highly undesirable to have a device depending on some external source. Devices must be able to function even if the Certificate Manager (see chapter 0) is not available. For this reason, in industrial environments, the offline CRL is often a preferrable choice.

Note that the use of offline CRLs has implications on the PKI hierarchy in order to keep the potential number of CRL entries low. Offline CRLs can get very large if there is a large number of revoked certificates. Therefore, it is necessary to have a strategy to minimize the potential size of the CRLs.
One proposed strategy is to have shorter lifetimes of your subordinate CAs because once the subordinate CA expires one reissues certificates and therefore clears the CRL. Subordinate CAs also allow the factory owner to limit the number of certificates issued by that CA and therefore limit the size of the CRLs.

2.7 Certificate Chains

Question:

What is a Certificate Chain?

Answer:

In order to properly validate a certificate, it is necessary to validate the issuing Certificate Authority. These issuing Certificate Authorities can have their own issuer Certificate Authorities. This chain can go on until the root Certificate Authority.
Therefore, the term Certificate Chain refers to the complete set of certificates that are needed to validate a certificate back to the root Certificate Authority.

2.8 Certificate hierarchies in an industrial environment

Question:

Why are certificate hierarchies useful in an industrial environment?

Answer:

In many environments no more than one issuer of certificates is necessary. However, there are use cases where having an intermediate Certificate Authority is useful for managing certificates. In particular, enterprises could find it useful to have an enterprise-wide Certificate Authority that issues certificates to different entities, such as a specific factory or even a specific production line in a factory.

The advantage of this approach is that the enterprise Certificate Authority could have a private key that is carefully protected by the IT department and ensures that it is very difficult to compromise whereas the private key for the production line would be not that strictly protected. If this private key is compromised, only the certificates within this production line will be compromised.
With this approach, the potential damage if the private key for the production line is compromised is restricted. When a compromise occurs, the enterprise Certificate Authority can be used to revoke the Certificate Authority that was used for the production line.

2.9 Trust Lists

Question:

What are Trust Lists?

Answer:

Once applications verify the certificate provided by their peer, they must decide if the peer is “trusted”. A “Trust List” is a list of certificates (sometimes called “trust anchors”) which the application is configured to trust. A peer certificate is only trusted if the certificate or one of the Certificate Authorities in the Certificate Chain is in the Trust List. This also allows new peers to be automatically trusted as soon as a trusted CA signs the new peer’s certificate.

2.10 Why are different types of Certificates needed?

Each public-key certificate underlies an identity model that becomes manifest in the attributes used to describe the certificate subject. Identity information that is necessary for one purpose is often not useful or insufficient for other purposes.

In addition, a Certificate is issued by a Registration Authority (RA) that is only able to determine if the holder is allowed to have a Certificate for the specific purpose for which the RA was established.

A good analogy is passports and driver’s licenses: they both identify a person, but they are issued by different authorities and contain different identifying information.

2.11 Different types of certificates

Question:

What kind of certificate types exist in the industrial environment and which SDO specified which certificate types?

Answer:

Table 1: Different types of certificates

Certificate types	Issuer	Use cases	Naming in SDOs specifications
Device Identity Certificate (long lived)	By manufacturer	Certificates issued by the manufacturer/ vendor of a device to prove the originality of a device with cryptographical measures.	OPC UA: device certificate PROFINET: Manufacturer certificate EtherNet/IP: Vendor certificate FCG: Secure device identity (In all cases it is a 802.1 AR IDevID)
Device Identity Certificate	By any organization in the supply chain, such as a value-added reseller or machine builder	Certificates issued by an intermediary that assert that the device is authentic.	OPC UA: LDevID EtherNet/IP and PROFINET: No use case specified
Device Identity Certificate	By factory owner	A certificate that identifies that a device is trustful and can be used inside of a dedicated plant. This will be used e.g., for automated certificate enrolment.	PROFINET: LDevID generic
Application Instance Certificate	By factory owner	A certificate that identifies a specific application of a device – many devices will have exactly one application.	PROFINET: LDevID PN EtherNet/IP: LDevID OPC UA: Application Instance Certificate.

2.11.1 Device certificates need business level trust relationship

Question:

What kind of device certificates are described in an industrial environment?

Answer:

In the industrial environment, a device certificate is an IDevID or an LDevID as described by IEEE 802.1 AR.

These device certificates are used to authenticate a device. However, this is only possible if the owner of the device has a business reason to trust the organization that signed the certificates.

In many cases the owner will be able to trust the original manufacturer and will be able to verify the IDevID of the manufacturer directly. In other cases, if no direct relationship with the manufacturer exists (or the manufacturer has gone out of business), the owner will have to trust the LDevID of intermediary.
In order to authenticate a device, only one of the certificates is needed.

Note: The owner can always assume that the device in possession is trustworthy. In this case, there is no need to use the device certificates or authenticate the device at all. If the owner uses the device certificates for any other sort of validation of device identity, then the device certificates should always be verified.

Phases of the component lifecycle in which certificates are affected in the device:

- Manufacturing
- Distribution/ Supply Chain
- Integration and commissioning
- Decommissioning

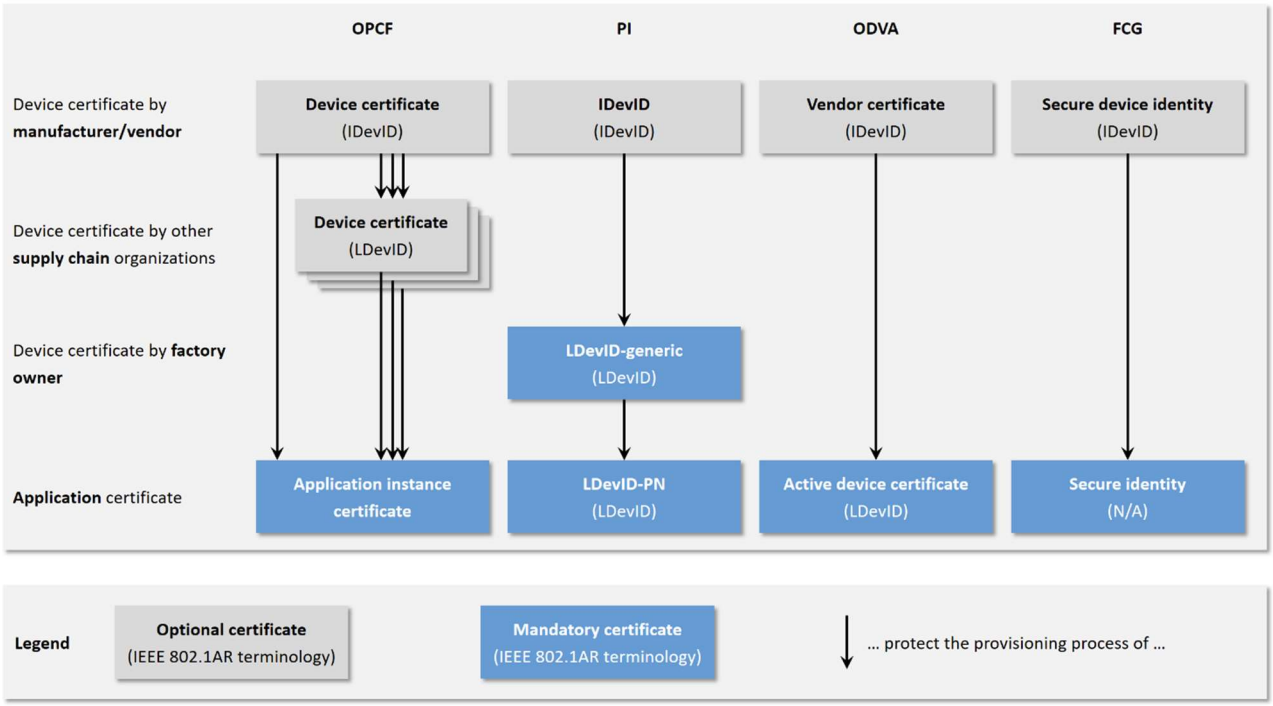

Figure 2-1 SDO certificate types overview

Figure 2-1 provides a mapping of the harmonized categories to the actual terms used by the individual specifications
(The figure might be subject to change as specifications are still being developed)

3 Certificate Management Tool

3.1 General

Question: Why do I need a tool for certificate management and what kind of capabilities does it have?

Answer:

In secure industrial communications, participants rely on a certificate management tool to provide the PKI needed to manage the Certificates and their private keys. For example, in the OPC Foundation this tool is called “Certificate Manager” or in PI it is called “Security Infrastructure Handler”. For simplicity, this document will refer to this as a “Certificate Manager”. A Certificate Manager is a central service available in the OT environment that provides access to features which include:

- Register/Unregister Devices and/ or Applications
- Issue and revoke certificates
- Get Trust Lists
- Checking Revocation Status

A Certificate Manager controls access to the Certificate Authorities (CA) and Registration Authorities (RA) used in the factory. These CA/RAs may be part of the Certificate Manager, or they may be an external service. The Certificate Manager hides the details of CA/RA implementation which allows integration with a variety of existing solutions.
The Application Programming Interfaces (API) exposed by the Certificate Manager give application standard interfaces that are independent of the particular Certificate Authority.

The Certificate Manager has two modes of operation intended to support different types of applications.

The Pull Management is used by applications that act as clients and initiate communication with the Certificate Manager.

The Push Management is used by applications that act as servers and require Certificate Manager to initiate communication.

3.2 Workflows of a Certificate Manager

The following workflows used in standard IT are necessary for a proper operation of a Certificate Manager in an OT environment.

In general, the participants of the following workflows need to pass authentication and authorization checks as appropriate.

3.2.1 Register/Unregister devices and applications

Register device and application workflow allows the PKI to be made aware of about a given device or application.
The Administrator provides a unique identifier for the application which is unique within the context of the system managed by the Certificate Manager.
The Unregister device and application workflow removes the device or application from the system and revokes all Certificates.

3.2.2 Request Certificate

The RequestCertificate workflow is called by a registered application to request a new certificate.

3.2.3 GetTrustList

The GetTrustList workflow delivers the current Trust List for the given applications.

3.2.4 Check Revocation Status

The CheckRevocationStatus workflow checks the revocation status of a certificate.

4 Miscellaneous

4.1 Glossary

Peer: Communication partner of an industrial automation device

4.2 Abbreviations

Abbreviation	Description
API	Application programming interfaces
CA	Certificate authority
CRL	Certificate revocation list
FAQ	Frequently asked questions
IESHG	Industrial Ethernet Security Harmonization Group
OT	Operation Technology
PKI	Public-key infrastructure
RA	Registration authority
SDO	Standards developing organization

4.3 Version History

Version	Date	Changes
Version 1	19.09.2022	Release of first version of the FAQ.

FieldComm Group

http://go.fieldcommgroup.org

ODVA

www.odva.org

OPC Foundation

www.opcfoundation.org

Profibus and Profinet International (PI)

www.profibus.com