Practical Security Recommendations for building OPC UA Applications

Whitepaper

Security Working Group

Editorial

The increasing networking and digitization of industrial systems entails new security challenges that need to be tackled systematically. A trustworthy, secure handling of sensitive data such as product and production knowledge is just as necessary as the protection against attacks on the networked systems. In order to counteract potential damage, Information Technology (IT) security should be ensured throughout the development process of a system and its software, from the requirements phase all the way to the decommissioning of the system.

The M2M Alliance and the OPC Foundation, the two largest professional Machine-to-Machine communication associations in Europe, are working together to help members build secure, connected products. At the end of 2016, members of both associations started a joint security user group. The objective of this group is to enhance the use of IT security mechanisms in the context of Operational Technology (OT) through practical examples.

The group members develop best practices and guidelines for typical use cases under the management of the Fraunhofer IEM and the Hochschule Offenburg. The security expertise is based on the extensive industry knowledge and the latest research in this area. The group took the requirements of device and machine builders as well as those of industrial operators into account. The implementation of the presented solutions within self-run projects and customer projects underlined the need for security. The steady increase in attacks on critical infrastructure and industrial automation solutions, the economic and social threats, and the lack of understanding in security principles make it necessary to build a community to share requirements, use cases, and best practices. An open mind-set and a thorough examination of the present situation, including defining the threats and risks, is a good starting point for improving protection of assets.

The group focuses on the communication standard OPC UA. As a starting point, the group developed the guideline “Practical Security Recommendations for building OPC UA Applications”. The guideline gives an overview of the OPC UA security concept and how to use it.

As the chairmen of the group, we thank all participants for sharing their knowledge and the contributions to the user group. Finally, we would like to invite you to read this brochure and to contact us for participation and further information.

Uwe Pohlmann, Fraunhofer IEM

Prof. Dr.-Ing. Axel Sikora, Hochschule Offenburg

The members of the group are:

- Ascolab
- Beckhoff Automation
- DS Interoperability
- exceet Secure Solutions
- Fraunhofer IEM
- Hochschule Offenburg
- Microsoft Corporation
- Software AG
- Sparhawk Software Inc
- TE Connectivity

Introduction

Today's devices and machines produce high-value data. For example, a production machine logs at which time it is used. However, the available data only becomes viable if it can be processed and used to improve a product, to offer a service, or to reduce the costs. For example, knowing the utilization of production systems can be used for offering overcapacity of the production system to other parties. Currently, the value of the available data is lost as the data is locked within its machine.

Communication enables remote access to and processing of the data. Internet-based smart services enable new business cases, like production as a service, which mine the value of the available data. A prerequisite for smart services is that devices, machines, and smart services exchange data in a secure way. Otherwise, data, machines, and devices might be compromised or the value of the data might be monetarized by external parties. Figure 1 shows a typical use case for a connected factory. OPC UA is the best solution that realizes the use case in a secure way.

Device and machine builders must ensure the data integrity and the data confidentially. Furthermore, they must guarantee that the sovereignty of the data remains with the data owner. Currently, many devices and machine builders are struggling with these security challenges. Thereby, they give away the ability to use the data securely to improve or extend their own products and services or to reduce their operational costs in a secure way.

For this reason and based on their expertise, the M2M Alliance & OPC Foundation security user group was founded. Its goal is to document and inform about best practices for secure communication solutions and smart services based on device and machine data.

This document shall give a condensed overview of the recommended security measures, which are used in "best practice" installations.

Please note that this short description

- → Gives an overview of the possible countermeasures being available in the OPC UA specification
- → Reports on typical installations, though without claim to be complete
- → Shows a snapshot of the situation at the time of compilation of this white paper. For obvious reasons, the security solutions need a regular review to current developments in the area.

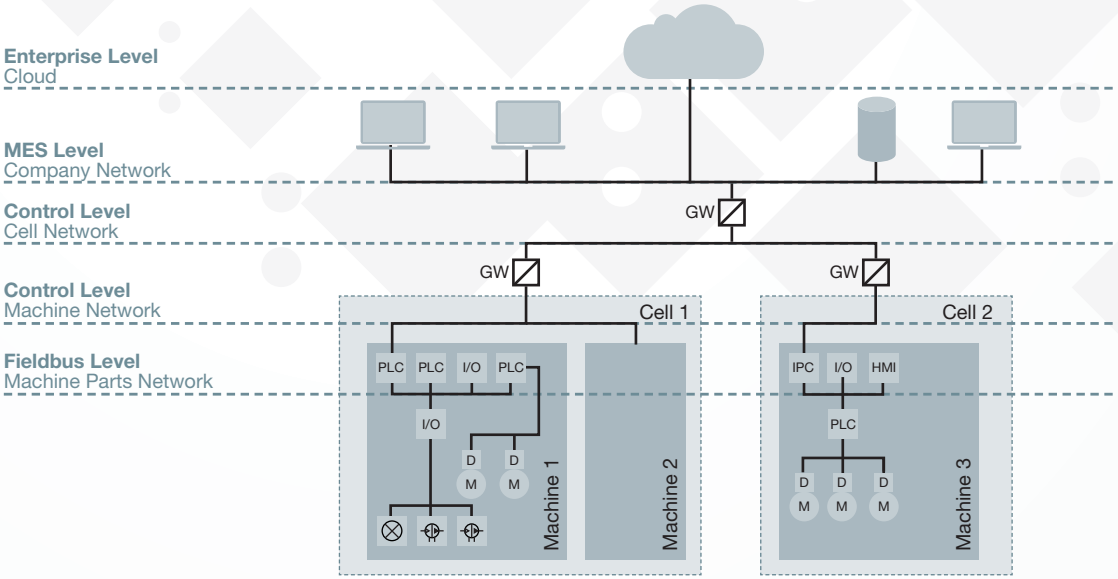
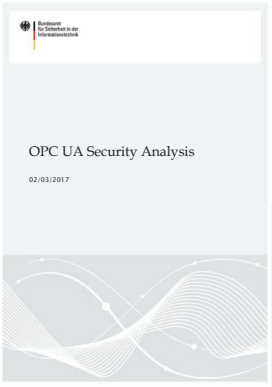


Figure 1: Connected Factory

Secure By Design

The Federal Office for Information Security (BSI) performed under the consortium leadership of the TÜV SÜD Rail the OPC UA security analysis study during the year 2015. The BSI is the first and foremost the central IT security service provider and national cyber security authority for the federal government in Germany. It shapes information security in digitization through prevention, detection and reaction for government, business and society. The OPC UA communication was analyzed systematically with regard to the Secure-Channel, Session and Discovery services according to the specification. The specification analysis has shown that OPC UA, in contrast to many other industrial protocols, provides a high level of security, as the BSI detected no systematic errors. On the basis of the analysis results, the OPC Foundation improved the OPC UA specification and provided an annotated edition of the OPC UA security analysis. [1]



https://opcfoundation.org/security/

Figure 2: Building of the German Federal Office for Information Security in Bonn, Germany
Source: Bundesamt für Sicherheit in der Informationstechnik

Scope of the Security Model

The OPC UA security architecture addresses the following concepts [2]:

Trusted Information (CIA triad)

→ Confidentiality by encrypting messages on the transport layer
→ Integrity by signing messages on the transport layer
→ Availability by restricting the message size and returning no security related codes

Access Control (AAA Framework)

→ Authentication by username and password or X.509 certificate on the application layer
→ Authorization to read, write values of a node or to browse the information model based on the access rights of the information model, access rights of the user or of the user's role
→ Accounting by generating audit events for security related operations

The following concepts are outside the scope of the OPC UA security architecture [2]:

→ Organizational Issues, like security training of personnel, security lifecycles and policies or how to handle physical access. OPC UA does not replace the information security management system (ISM) that the ISO 27001 defines. OPC UA security aspects should be used to implement defense/security in depth.
→ User and Role Authentication and Authorization Management

Nevertheless, UA can be integrated with existing concepts, like Kerberos, OAuth2, or JSON Web Token by using claims-based authorization.

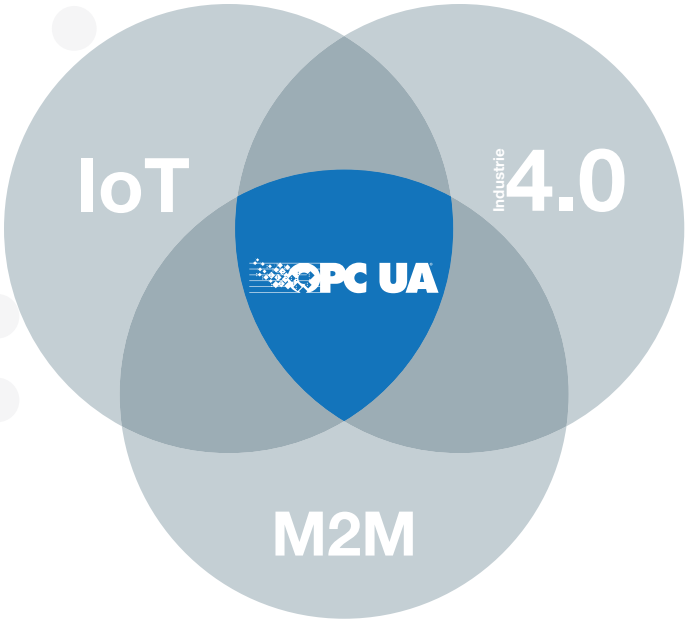


Figure 3: OPC UA serves as the common data connectivity and collaboration standard for local and remote device access in IoT, M2M, and Industrie4.0 settings.

Security Model

Security is a fundamental requirement for OPC UA and it is therefore tightly integrated into the architecture. UA security mechanisms are based on a detailed analysis of security threats. UA security deals with authentication of users and UA applications, integrity and confidentiality of the exchanged messages and the validation of function profiles.

UA Security complements the preexisting security infrastructure within a company. Figure 3 shows the scalable UA security concept. It consists of three levels: user security, application security, and transport security.

The mechanisms of UA user level security grant access for a specific user and its role while setting up a new session.

UA application level security is also part of the communication session and includes the exchange of digitally signed **X.509 certificates**. Application instance certificates that are exchanged during Secure Channel establishment are used to authenticate an application. The supported UA security profile that can be certified by the OPC Foundation defines, which security mechanisms a UA application supports.

Transport level security can be used to sign and encrypt each message during a communication session. Signing ensures the message integrity and encryption prevents eavesdropping.

The UA security mechanisms are implemented in the UA stack, i.e. they are included in the software package distributed by UA stack vendors, so UA applications just have to make use of it. It is however the responsibility of the UA application developer (i.e. the machine builder, etc.) to configure the UA server, according to the requirements that he has to adhere to. Refer to [3] for further reading.

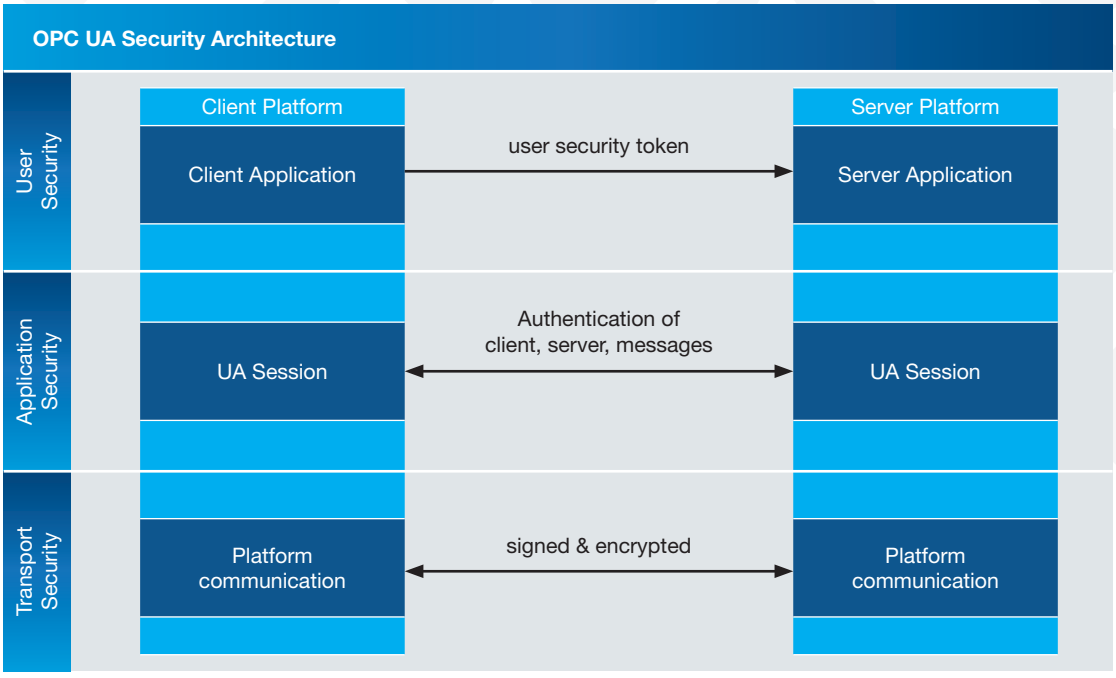


Figure 3: Scalable Security Concept

X.509 Certificate Management

Self-signed certificates
A certificate created and signed by users themselves using a tool like OpenSSL is called a self-signed certificate. The format of the certificate is defined by the X.509 standard. A certificate contains a Public Key and identity information of the owner. Furthermore, a certificate is only valid for a defined period. The public key contained within the certificate can be used to sign and encrypt communication with a remote party. Accepting self-signed certificates can be dangerous if the operator currently in charge of making the trust decision is not well trained in X.509 certificate management because it is not clear from the information provided whether you can trust the properties of the certificate as no trusted 3rd-party approved the correctness of the properties. A self-signed certificate is an inexpensive solution because you do not have to pay or go through additional effort for being trusted. In contrast, using a trusted certification authority (CA) can build a chain of trust from the remote party all the way to a trusted root (i.e. a root you trust already).

CA-signed certificates in a PKI
A ceritifcation authority (CA) is an entity that issues digital certificates [20]. It must be a trusted party, which is trusted by the owner of certificates and by the users that should accept the certificate. In a Public Key Infrastructure (PKI) there is at least one CA or there are even more hierarchical organized CAs that build a chain of trust (cf. Figure 4). A CA can revoke the trust of a certificate or of another CA that is at a lower level by providing a certificate revocation list. A CA must meet high-security requirements and the private key used to create the public key contained within the certificate must be kept in a safe place. By using multiple issuing CAs, it is possible to revoke the trust of one issuing CA without harming the other issuing CAs. A CA can distribute issued certificates by the following distribution channels [4]:

- → Manuel Distribution Mechanism: The certificates are transported on a storage medium or secure email communication. The certificates are installed manually. This requires a large amount of manual labor, especially for large deployments.
- → Custom Distribution Mechanism: The requesting application uses a well-known public repository, where it uses its credentials to authenticate, download and install the certificate from. A custom solution usually has the disadvantage that it can be more easily compromised by a hacker.
- → Automatic Certificate Management: The certificates are distributed via a **Global Discovery Server.** This option is explained in the following section.

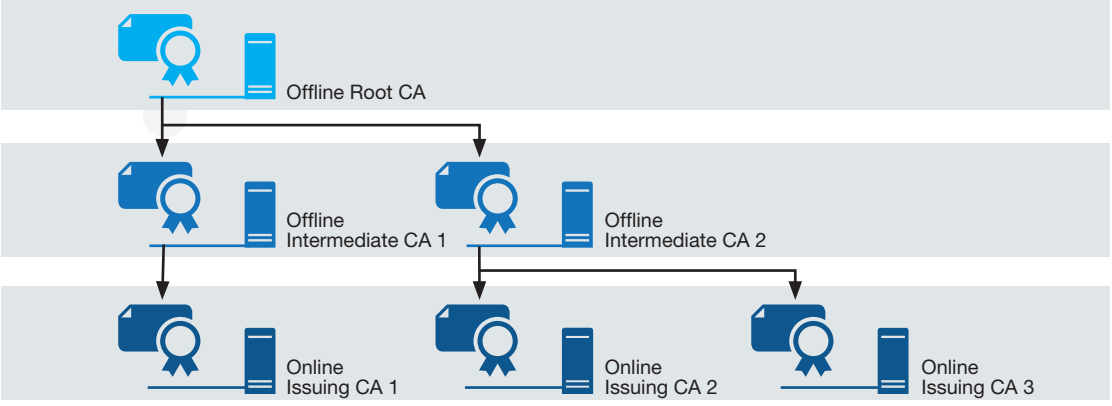


Figure 4: Three-Tier CA Hierarchy; Source: https://technet.microsoft.com/en-us/library/dn786436(v=ws.11).aspx

GDS Security Features

A Global Discovery Server (GDS) is an OPC UA server that provides services allowing Servers to register themselves and also allows Clients to search for Servers to connect to. Furthermore, it provides X.509 security certificate management services for Clients and Servers. Please see this video [19] for a detailed introduction to the GDS.
Figure 5 shows the structure and use cases of a connected factory that uses a GDS.

Roles & Claim-Based Security
A GDS provides the master database including roles, like security admin observer. The role management integrates with existing user and role management systems. Roles have access permission for nodes within the OPC UA Information Model. Users provide credentials to authenticate and to get a granted role and the corresponding access rights for a UA session. The identity information and access rights are handled via a claims-based authorization mechanism, which, e.g., Kerberos or OAuth2 provides.

Automatic Certificate Management
Automatic certificate management means that the OPC UA GDS maintains the X.509 certificate provisioning and renewable for a list of UA applications, which are available in an administrative domain. The GDS provides a certificate manager to request and update certificates and trust and revocation lists. The certificate manager supports pull and push-based distribution models. Either the application acts as a client and uses methods of the certificate manager to pull certificates and lists or the application acts as a server and provides methods that the certificate manager can use to push new certificates and lists. Managing certificates by using the certificate manager scales better than handling certificates manually.

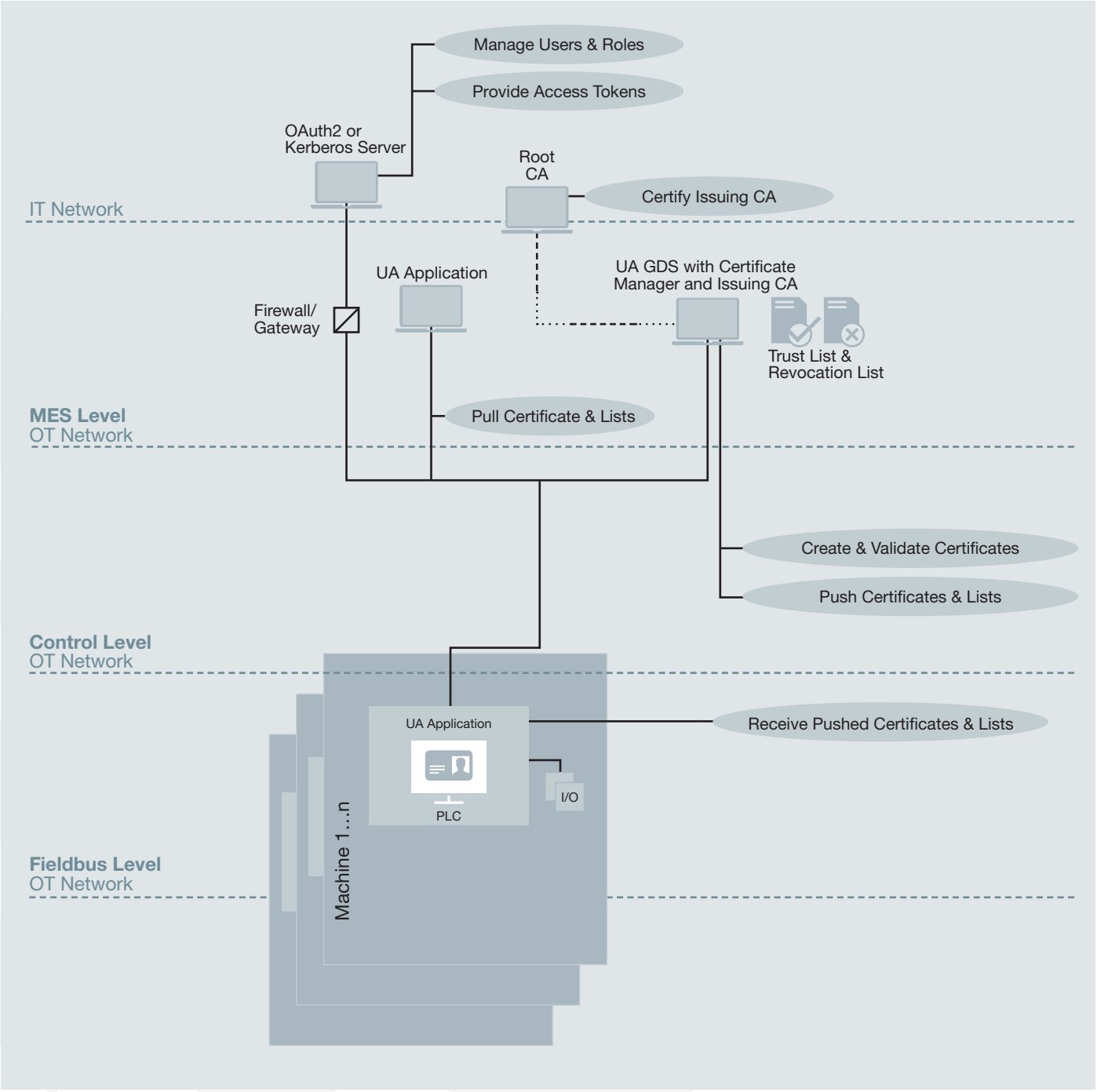


Figure 5: Connected Factory with new UA Features and Use Cases

Defense in Depth

The security concept “defense in depth” realizes the information assurance by using multiple layers. As a result, an attacker must break through several barriers before compromising the whole system. Figure 6 shows the security features that OPC UA offers within the different layers. Within each layer, several requirements can be fullfilled by using the corresponding OPC UA feature to improve the overall security.

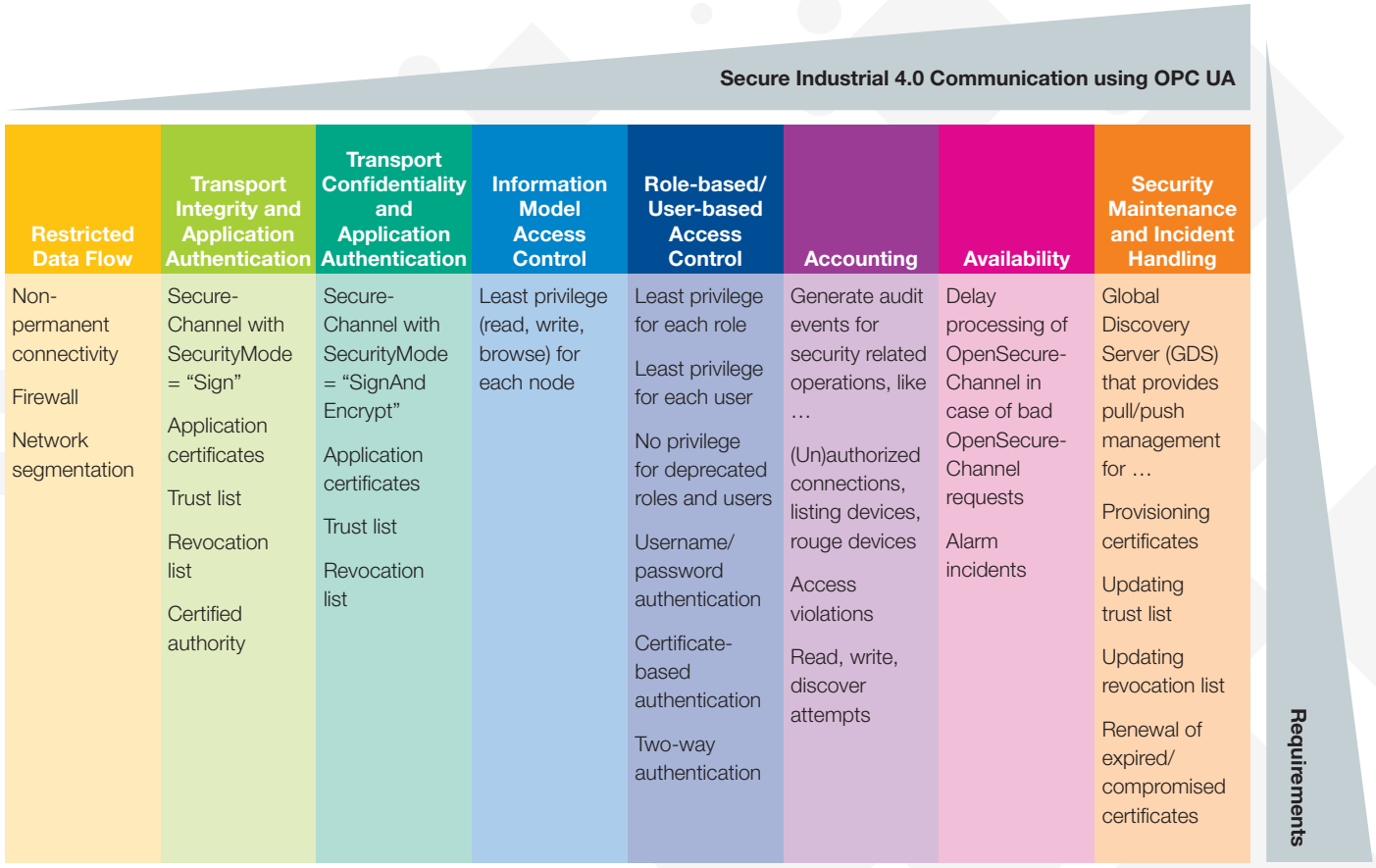


Figure 6: Defense in Depth Using the OPC UA Security Architecture

Recommendations for Using OPC UA in a Secure Way

WHEN SECURING THE COMMUNICATION WITH THE OPC UA PROTOCOL, THE FOLLOWING SETTINGS ARE OF CENTRAL IMPORTANCE:

→ **SecurityMode:** The SecurityMode [5] should be 'Sign' or 'SignAndEncrypt'. This ensures that, among other things, authentication at the application level is forced. The SecurityMode 'None' does not provide any protection! SecurityMode 'SignAndEncrypt' must be used if not only integrity but also confidentiality of data has to be protected. [6]

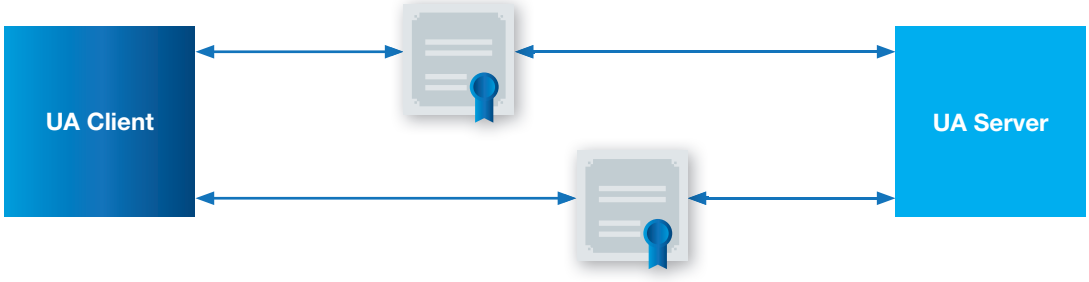
→ **Selection of cryptographic algorithms:** At a minimum, the SecurityPolicy [7] 'Basic256Sha256' should be chosen, provided that this is technically possible, i.e. any existing client the server needs to interact with also supports this policy. Note that a good client connection strategy is to start with the most secure profile, check that this is supported by the server and then try the next best thing until a common profile is found. Weaker security policies use outdated algorithms and should not be used. For example, SHA-1 is no longer secure and should not be used. [6]

→ **User authentication:** The possibility of logging in with the identifier 'anonymous' should be used only for accessing non-critical UA server resources as it does not provide any protection (what data is deemed non-critical is at the discretion of the UA application developer). It is not possible to trace who has changed, for example, the data or configuration on the server side when this generic identifier is used. Also, an attacker could use this identifier to read or write data in an unauthorized manner if no adequate restriction of the rights of the identifier 'anonymous' was configured. [6]

→ **Certificate and private key storage:** Never store private keys or the corresponding certificate files (.pfx/p12) on an unencrypted file system. Use the dedicated certificate stores of your operating system and use operating system capabilities for setting the access rights. TPM modules or external secured hardware, like USB-based authentication tokens to store certificates and/or private keys improve the security level.

→ **Using certificates:** Don't accept connections which do not provide trusted certificates. Especially, self-signed certificates should not be trusted automatically, which means without an additional verification. If the certificates are not self-signed, a Certificate Authority (CA), e.g., for all OPC UA applications of a company is required. The certificates of the Certificate Authority are either self-signed or signed by another Certificate Authority. Certificate Authorities can be multilayered. (cf. [2])

→ **Managing and maintaining certificates:** Use certificate trust lists and certificate revocation lists to manage valid certificates. Only trusted users or processes should be allowed to write these lists. The lists should be updated regularly.



References

[1]	OPC Foundation, „OPC UA Security,“ [Online]. Available: https://opcfoundation.org/security
[2]	OPC Foundation, "OPC Unified Architecture Specification, Part 2: Security Model, Release 1.03," Scottsdale, USA.
[3]	R. Armstrong und P. Hunkar, „The OPC UA Security Model,“ OPC Foundation, Scottsdale, USA, 2010.
[4]	A. Fernbach und W. Kastner, „Certificate Management in OPC UA Applications: An Evaluation of different Trust Models,“ in Proceedings of the 2012 IEEE 17th Conference on Emerging Technologies & Factory Automation (ETFA), 2012.
[5]	OPC Foundation, „OPC Unified Architecture Specification, Part 4: Services, Release Candidate 1.04.11,“ Scottsdale, USA, 2017.
[6]	Fiat, Störtkuhl, Plöb, Zugfil, Gappmeier and Damm, "OPC UA Security Analysis," Federal Office for Information Security, Bonn, Germany, 2017.
[7]	OPC Foundation, „OPC Unified Architecture Specification, Part 7: Profiles, Release 1.03,“ Scottsdale, USA, 2015.
[8]	OPC Foundation, „OPC Unified Architecture Specification, Part 12: Discovery, Release 1.03,“ Scottsdale, USA, 2015.
[9]	[Online]. Available: http://www.vdmashop.de/refs/Leitf_I40_Security_En_LR_neu.pdf
[10]	[Online]. Available: http://www.27000.org/ismsprocess.htm

[11]	[Online]. Available: http://isa99.isa.org/ISA99%20Wiki/Home.aspx
[12]	[Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
[13]	[Online]. Available: https://www.first.org/cvss/
[14]	[Online]. Available: https://www.commoncriteriaportal.org/
[15]	Mano Paul, Official (ISC)^2 GUIDE TO THE CSSLP CBK, Boca Raton, USA: CRC Press, 2014.
[16]	[Online]. Available: https://opcfoundation.org/markets-collaboration/m2m-alliance/
[17]	[Online]. Available: https://www.owasp.org/index.php/Main_Page
[18]	OPC Foundation, „OPC Unified Architecture Specification, Part 14: PubSub, Release Candidate 1.04.24," Scottsdale, USA, 2017.
[19]	[Online]. Available: https://www.youtube.com/watch?v=TCy8JInWIXw
[20]	Wylie Shanks, "Building and Managinga PKI Solution for Small and Medium Size Business", 2013, Online Available: https://www.sans.org/reading-room/whitepapers/certificates/building-managing-pki-solution-small-medium-sizebusiness-34445

Further information

This document gives only a condensed overview of security for OPC UA. Security is a must have in connected systems. An overview of industrial security is given by the VDMA guideline [9]. You need an overall security concept, which is based on accepted security standards.

An information security management as described by the ISO/IEC 2700x [10] series of security standards requires organizational policies, infrastructure policies, and development policies. Furthermore, personnel must be trained regularly and you must be prepared for security incidents. The IEC 62443 [11] series of security standards defines industrial communication networks requirements for the network and system security.

You should also be aware of your threats and risks. STRIDE [12] defines a common security threat classification model. Furthermore, CVSS [13] defines a security threats evaluation model. Additionally, Common Criteria [14] defines a common methodology for information security evaluation. The book [15] gives you a good starting point for becoming a security expert. Being up to date and networking with security professional is also one of the key factors for getting the latest news. You should get into contact with community projects, like our OPCF / M2M security user group [16] or the Open Web Application Security Project (OWASP) [17]. The OWASP publishes the top 10 security risks regularly and publishes security guidelines. If you do not have the resources for building up security expertise by yourself get in touch with external experts from security companies, OPC UA companies, universities, or research societies.

Online Videos

LEARN MORE ABOUT ...

OPC Videos

https://opcfoundation.org/resources/multimedia

What is OPC? UA in a minute

https://www.youtube.com/watch?v=-tDGzwsBokY

OPC UA Technical Introduction by Uwe Steinkrauss

https://youtu.be/nYMbQiRqK74

OPC UA Security by Darek Kominek

https://www.youtube.com/watch?v=NFQfZeU90Kw

HEADQUARTERS / USA
OPC Foundation
16101 N. 82nd Street
Suite 3B
Scottsdale, AZ 85260-1868
Phone: (1) 480 483-6644
office@opcfoundation.org

OPC EUROPE
Huelshorstweg 30
33415 Verl
Germany
opceurope@opcfoundation.org

OPC JAPAN
c/o Microsoft Japan Co., Ltd
2-16-3 Konan Minato-ku, Tokyo
1080075 Japan
opcjapan@microsoft.com

OPC KOREA
c/o KETI
22, Daewangpangyo-ro 712,
Bundang-gu, Seongnam-si, Gyeonggi-do
13488 South Korea
opckorea@opcfoundation.org

OPC CHINA
B-8, Zizhuyuan Road 116,
Jiahao International Center, Haidian District,
Beijing, P.R.C
P.R.China
opcchina@opcfoundation.org

V1

www.opcfoundation.org