IEC/TR 62541-2

Edition 1.0 2010-02

TECHNICAL REPORT

OPC Unified Architecture – Part 2: Security Model

IEC/TR 62541-2:2010(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TR 62541-2

Edition 1.0 2010-02

TECHNICAL REPORT

OPC Unified Architecture –
Part 2: Security Model

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE V

ICS 25.040.40; 35.100.01

ISBN 978-2-88910-760-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

OPC UNIFIED ARCHITECTURE –

Part 2: Security Model

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62541-2, which is a technical report, has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
65E/93/DTR	65E/155/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62541 series, under the general title *OPC Unified Architecture*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

This technical report introduces security concepts for OPC Unified Architecture as specified by IEC 62541. This technical report and specification are a result of an analysis and design process to develop a standard interface to facilitate the development of applications by multiple vendors that inter-operate seamlessly together.

OPC UNIFIED ARCHITECTURE –

Part 2: Security Model

1 Scope

This part of IEC 62541 describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It gives an overview of the security features that are specified in other parts of the OPC UA specification. It references services, mappings, and profiles that are specified normatively in other parts of this series of standards.

Note that there are many different aspects of security that have to be addressed when developing applications. However since OPC UA specifies a communication protocol, the focus is on securing the data exchanged between applications.

This does not mean that an application developer can ignore the other aspects of security like protecting persistent data against tampering. It is important that the developer look into all aspects of security and decide how they can be addressed in the application.

This part of IEC 62541 is directed to readers who will develop OPC UA client or server applications or implement the OPC UA services layer.

It is assumed that the reader is familiar with Web Services and XML/SOAP. Information on these technologies can be found in SOAP Part 1 and SOAP Part 2.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62541 (all parts), *OPC Unified Architecture*

IEC 62541-1, *OPC Unified Architecture – Part 1: Overview and concepts*

3 Terms, definitions, abbreviations and conventions

3.1 Terms and definitions

For the purposes of this document the following terms and definitions as well as the terms and definitions given in IEC 62541-1 apply.

3.1.1
Application Instance
individual installation of a program running on one computer

NOTE There can be several *Application Instances* of the same application running at the same time on several computers or possibly the same computer.

3.1.2
Application Instance Certificate
Digital Certificate of an individual instance of an application that has been installed in an individual host

NOTE Different installations of one software product would have different *Application Instance Certificates*.

3.1.3
Asymmetric Cryptography
Cryptography method that uses a pair of keys, one that is designated the *Private Key* and kept secret, the other is called the *Public Key* that is generally made available

NOTE *Asymmetric Cryptography*, also known as "public-key cryptography". In an asymmetric encryption algorithm when an entity A wants to ensure *Confidentiality* for data it sends to another entity B, entity A encrypts the data with a *Public Key* provided by entity B. Only entity B has the matching *Private Key* that is needed to decrypt the data. In an asymmetric digital signature algorithm when an entity A wants to ensure *Integrity* or provide *Authentication* for data it sends to an entity B, entity A uses its *Private Key* to sign the data. To verify the signature, entity B uses the matching *Public Key* that entity A has provided. In an asymmetric key agreement algorithm, entity A and entity B each send their own *Public Key* to the other entity. Then each uses their own *Private Key* and the other's *Public Key* to compute the new key value. See IS Glossary.

3.1.4
Asymmetric Encryption
mechanism used by *Asymmetric Cryptography* for encrypting data with the *Public Key* of an entity and for decrypting data with the associated *Private Key*

NOTE See 3.1.3 for details.

3.1.5
Asymmetric Signature
mechanism used by *Asymmetric Cryptography* for signing data with the *Private Key* of an entity and for verifying the data's signature with the associated *Public Key*

NOTE See 3.1.3 for details.

3.1.6
Auditability
security objective that assures that any actions or activities in a system can be recorded

3.1.7
Auditing
tracking of actions and activities in the system, including security related activities where the Audit records can be used to verify the operation of system security

3.1.8
Authentication
process of verifying the identity of an entity such as a client, server, or user

3.1.9
Authorization
process of granting the right or the permission to a system entity to access a system resource

3.1.10
Availability
running of the system with unimpeded capacity

3.1.11
Confidentiality
protection of data from being read by unintended parties

3.1.12
Cryptography
transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key

3.1.13
Cyber Security Management System
CSMS
program designed by an organization to maintain the security of the entire organization's assets to an established level of *Confidentiality*, *Integrity*, and *Availability*, whether they are on the business side or the industrial automation and control systems side of the organization

3.1.14
Digital Certificate
structure that associates an identity with an entity such as a user, a product or an *Application Instance* where the certificate has an associated asymmetric key pair which can be used to authenticate that the entity does, indeed, possess the *Private Key*

3.1.15
Digital Signature
value computed with a cryptographic algorithm and appended to data in such a way that any recipient of the data can use the signature to verify the data's origin and integrity

3.1.16
Hash Function
algorithm such as SHA-1 for which it is computationally infeasible to find either a data object that maps to a given hash result (the "one-way" property) or two data objects that map to the same hash result (the "collision-free" property), see IS Glossary

3.1.17
Hashed Message Authentication Code
HMAC
MAC that has been generated using an iterative *Hash Function*

3.1.18
Integrity
security goal that assures that information has not been modified or destroyed in a unauthorized manner

NOTE definition from IS Glossary.

3.1.19
Key Exchange Algorithm
protocol used for establishing a secure communication path between two entities in an unsecured environment whereby both entities apply a specific algorithm to securely exchange secret keys that are used for securing the communication between them

NOTE A typical example of a *Key Exchange Algorithm* is the SSL Handshake Protocol specified in SSL/TLS.

3.1.20
Message Authentication Code
MAC
short piece of data that results from an algorithm that uses a secret key (see *Symmetric Cryptography*) to hash a message whereby the receiver of the message can check against alteration of the message by computing a *MAC* that should be identical using the same message and secret key

3.1.21
Message Signature
Digital Signature used to ensure the *Integrity* of messages sent between two entities

NOTE There are several ways to generate and verify *Message Signature*s, however, they can be categorized as symmetric (see 3.1.32) and asymmetric (see 3.1.5) approaches.

3.1.22
Non-Repudiation
strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the original submission or delivery of the message and the integrity of its contents

3.1.23
Nonce
random number that is used once, typically by algorithms that generate security keys

3.1.24
OPC UA Application
OPC UA *Client*, which calls OPC UA services, or an OPC UA *Server*, which performs those services

3.1.25
Private Key
secret component of a pair of cryptographic keys used for *Asymmetric Cryptography*

3.1.26
Public Key
publicly-disclosed component of a pair of cryptographic keys used for *Asymmetric Cryptography, see* IS Glossary

3.1.27
Public Key Infrastructure
PKI
set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke *Digital Certificates* based on *Asymmetric Cryptography*

NOTE The core *PKI* functions are to register users and issue their public-key certificates, to revoke certificates when required, and to archive data needed to validate certificates at a much later time. Key pairs for data *Confidentiality* may be generated by a certificate authority (CA), but requiring a *Private Key* owner to generate its own key pair improves security because the *Private Key* would never be transmitted, see IS Glossary. See PKI and X509 PKI for more details on *Public Key Infrastructures*.

3.1.28
Rivest-Shamir-Adleman
RSA
algorithm for *Asymmetric Cryptography*, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, see IS Glossary

3.1.29
Secure Channel
in OPC UA, a communication path established between an OPC UA client and server that have authenticated each other using certain OPC UA services and for which security parameters have been negotiated and applied

3.1.30
Symmetric Cryptography
branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification), see IS Glossary