IEC TR 62541-2

Edition 2.0 2016-10

TECHNICAL REPORT

colour inside

OPC unified architecture – Part 2: Security Model

IEC TR 62541-2:2016-10(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

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.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC TR 62541-2

Edition 2.0 2016-10

TECHNICAL REPORT

colour inside

OPC unified architecture –
Part 2: Security Model

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.01

ISBN 978-2-8322-3641-3

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 TR 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/413/DTR	65E/464/RVC

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

This second edition cancels and replaces the first edition of IEC TR 62541-2, published in 2010.

This second edition includes no technical changes with respect to the first edition but a number of clarifications and additional text for completeness.

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

Throughout this document and the referenced other parts of the series, certain document conventions are used:

– Italics are used to denote a defined term or definition that appears in the “Terms and definition” clause in one of the parts of the series.
– Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.
– The italicized terms and names are also often written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example the defined term is AddressSpace instead of Address Space. This makes it easier to understand that there is a single definition for AddressSpace, not separate definitions for Address and Space.

A list of all parts of the IEC 62541 series, published 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 website 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.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

OPC UNIFIED ARCHITECTURE –

Part 2: Security Model

1 Scope

This part of IEC 62541, which a Technical Report, 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 provides definition of common security terms that are used in this and other parts of the OPC UA specification. It gives an overview of the security features that are specified in other parts of the OPC UA specification. It references services, mappings, and *Profile*s that are specified normatively in other parts of this multi-part specification. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this part of IEC 62541 and one of the normative parts of IEC 62541 does not remove or reduce the requirement specified in the normative part.

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 developers 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 also for end users that wish to understand the various security features and functionality provided by OPC UA. It also offers some suggestions that can be applied when deploying systems. These suggestions are generic in nature since the details would depend on the actual implementation of the *OPC UA Application*s and the choices made for the site security.

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 documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62351 (all parts), *Power systems management and associated information exchange – Data and communications security*

IEC TR 62541-1, *OPC unified architecture – Part 1: Overview and concepts*

IEC 62541-4, *OPC unified architecture – Part 4: Services*

IEC 62541-5, *OPC unified architecture – Part 5: Information Model*

IEC 62541-6, *OPC unified architecture – Part 6: Mappings*

IEC 62541-7, *OPC unified architecture – Part 7: Profiles*

SOAP Part 1: SOAP Version 1.2 Part 1: Messaging Framework

Available from Internet: http://www.w3.org/TR/soap12-part1/ (website checked 2016-04-05)

SOAP Part 2: SOAP Version 1.2 Part 2: Adjuncts

Available from Internet: http://www.w3.org/TR/soap12-part2/ (website checked 2016-04-05)

XML Encryption: XML Encryption Syntax and Processing

Available from Internet: http://www.w3.org/TR/xmlenc-core/ (website checked 2016-04-05)

XML Signature:: XML-Signature Syntax and Processing

Available from Internet: http://www.w3.org/TR/xmldsig-core/ (website checked 2016-04-05)

WS Security: SOAP Message Security 1.1

Available from Internet: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf (website checked 2016-04-05)

WS Secure Conversation: Web Services Secure Conversation Language (WS-SecureConversation)

Available from Internet:http://specs.xmlsoap.org/ws/2005/02/sc/WS-SecureConversation.pdf (website checked 2016-04-05)

SSL/TLS: RFC 2246: The TLS Protocol Version 1.0

Available from Internet: http://www.ietf.org/rfc/rfc2246.txt (website checked 2016-04-05)

:X509: X.509 Public Key Certificate Infrastructure

Available from Internet: https://www.ietf.org/rfc/rfc2459 (website checked 2016-04-05)

HTTP: RFC 2616: Hypertext Transfer Protocol - HTTP/1.1

Available from Internet: http://www.ietf.org/rfc/rfc2616.txt (website checked 2016-04-05)

HTTPS: RFC 2818: HTTP Over TLS

Available from Internet: http://www.ietf.org/rfc/rfc2818.txt (website checked 2016-04-05)

IS Glossary: Internet Security Glossary

Available from Internet: http://www.ietf.org/rfc/rfc2828.txt (website checked 2016-04-05)

NIST 800-57: Part 3: Application-Specific Key Management Guidance

Available from Internet:http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf (website checked 2016-04-05)

NERC CIP: CIP 002-1 through CIP 009-1, by North-American Electric Reliability Council

Available from Internet: http:// www.nerc.com/files/cip-002-1.pdf (website checked 2016-04-05)

SHA-1: Secure Hash Algorithm RFC

Available from Internet: http://tools.ietf.org/html/rfc3174 (website checked 2016-04-05)

PKI: Public Key Infrastructure article in Wikipedia

Available from Internet: http://en.wikipedia.org/wiki/Public_key_infrastructure (website checked 2016-04-05)

X509 PKI: Internet X.509 Public Key Infrastructure

Available from Internet: http://www.ietf.org/rfc/rfc3280.txt (website checked 2016-04-05)

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

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

Note 1 to entry: 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 *Application Instance* that has been installed in an individual host

Note 1 to entry: 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 called the *Public Key* that is generally made available

Note 1 to entry: Asymmetric Cryptography is 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 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 according to IS Glossary.

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

3.1.5
Asymmetric Signature
the 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*

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

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

3.1.8
Authentication
security objective that assures that the identity of an entity such as a *Client*, *Server*, or user can be verified

3.1.9
Authorization
the ability to grant access to a system resource

3.1.10
Availability
security objective that assures that the system is running normally; that is, no services have been compromised in such a way to become unavailable or severely degraded

3.1.11
CertificateAuthority
entity that can issue *Digital Certificate*s, also known as a CA

Note 1 to entry: The *Digital Certificate* certifies the ownership of a Public Key by the named subject of the *Certificate*. This allows others (relying parties) to rely upon signatures or assertions made by the Private Key that corresponds to the *Public Key* that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the *Certificate* and the party relying upon the *Certificate*. CAs are characteristic of many Public Key infrastructure (PKI) schemes.

3.1.12
CertificateStore
persistent location where *Certificate*s and *Certificate* revocation lists (CRLs) are stored

Note 1 to entry: It may be a disk resident file structure or on Windows platforms, it may be a Windows registry location.

3.1.13
Confidentiality
security objective that assures the protection of data from being read by unintended parties

3.1.14
Cryptography
transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key

3.1.15
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

3.1.16
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*

3.1.17
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*

3.1.18
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

3.1.19
Hashed Message Authentication Code
HMAC
MAC that has been generated using an iterative *Hash Function*

3.1.20
Integrity
security objective that assures that information has not been modified or destroyed in an unauthorized manner, see IS Glossary

3.1.21
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 1 to entry: A typical example of a Key Exchange Algorithm is the SSL Handshake Protocol specified in SSL/TLS.

3.1.22
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

3.1.23
Message Signature
Digital Signature used to ensure the *Integrity* of *Messages* that are sent between two entities

Note 1 to entry: There are several ways to generate and verify Message Signatures however they can be categorized as symmetric (See 3.1.34) and asymmetric (See 3.1.5) approaches.

3.1.24
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

3.1.25
Nonce
random number that is used once, typically by algorithms that generate security keys

3.1.26
OPC UA Application
OPC UA *Client*, which calls OPC UA services, or an OPC UA *Server*, which performs those services

3.1.27
Private Key
the secret component of a pair of cryptographic keys used for *Asymmetric Cryptography*

3.1.28
Public Key
the publicly-disclosed component of a pair of cryptographic keys used for *Asymmetric Cryptography*, see IS Glossary

3.1.29
Public Key Infrastructure
PKI
the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke *Digital Certificates* based on *Asymmetric Cryptography*

Note 1 to entry: 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 according to IS Glossary. See PKI and X509 PKI for more details on Public Key Infrastructures.

3.1.30
Rivest-Shamir-Adleman
RSA
algorithm for *Asymmetric Cryptography*, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, see IS Glossary

3.1.31
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

3.1.32
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

3.1.33
Symmetric Encryption
the mechanism used by *Symmetric Cryptography* for encrypting and decrypting data with a cryptographic key shared by two entities

3.1.34
Symmetric Signature
the mechanism used by *Symmetric Cryptography* for signing data with a *cryptographic key* shared by two entities

Note 1 to entry: The signature is then validated by generating the signature for the data again and comparing these two signatures. If they are the same then the signature is valid, otherwise either the key or the data is different from the two entities. Definition 3.1.19 defines a typical example for an algorithm that generates Symmetric Signatures.

3.1.35
TrustList
list of *Certificate*s that an application has been configured to trust

3.1.36
Transport Layer Security
TLS
standard protocol for creating *Secure Channel*s over IP based networks

3.1.37
X.509 Certificate
Digital Certificate in one of the formats defined by X.509 v1, 2, or 3

Note 1 to entry: An X.509 Certificate contains a sequence of data items and has a Digital Signature computed on that sequence.