

# TECHNICAL REPORT



**OPC unified architecture –  
Part 2: Security Model**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

ICS 25.040.40; 35.100.01

ISBN 978-2-8322-3641-3

**Warning! Make sure that you obtained this publication from an authorized distributor.**

## CONTENTS

FOREWORD.....	4
1 Scope.....	6
2 Normative references.....	6
3 Terms, definitions and abbreviations .....	8
3.1 Terms and definitions .....	8
3.2 Abbreviations .....	12
3.3 Conventions for security model figures .....	12
4 OPC UA security architecture.....	12
4.1 OPC UA security environment .....	12
4.2 Security objectives .....	13
4.2.1 Overview.....	13
4.2.2 Authentication .....	13
4.2.3 Authorization.....	13
4.2.4 Confidentiality .....	14
4.2.5 Integrity .....	14
4.2.6 Auditability .....	14
4.2.7 Availability .....	14
4.3 Security threats to OPC UA systems.....	14
4.3.1 Overview.....	14
4.3.2 Message flooding .....	14
4.3.3 Eavesdropping .....	15
4.3.4 Message spoofing .....	15
4.3.5 Message alteration.....	15
4.3.6 Message replay.....	15
4.3.7 Malformed Messages .....	15
4.3.8 Server profiling.....	16
4.3.9 Session hijacking .....	16
4.3.10 Rogue Server.....	16
4.3.11 Compromising user credentials.....	16
4.4 OPC UA relationship to site security .....	17
4.5 OPC UA security architecture .....	17
4.6 Security Policies .....	19
4.7 Security Profiles.....	20
4.8 User Authorization .....	20
4.9 User Authentication.....	20
4.10 Application Authentication .....	20
4.11 OPC UA security related Services .....	21
4.12 Auditing .....	21
4.12.1 General.....	21
4.12.2 Single Client and Server.....	22
4.12.3 Aggregating Server .....	23
4.12.4 Aggregation through a non-auditing Server .....	23
4.12.5 Aggregating Server with service distribution.....	24
5 Security reconciliation.....	25
5.1 Reconciliation of threats with OPC UA security mechanisms .....	25
5.1.1 Overview.....	25

5.1.2	Message flooding .....	25
5.1.3	Eavesdropping .....	26
5.1.4	Message spoofing .....	26
5.1.5	Message alteration .....	26
5.1.6	Message replay .....	26
5.1.7	Malformed Messages .....	27
5.1.8	Server profiling.....	27
5.1.9	Session hijacking .....	27
5.1.10	Rogue Server.....	27
5.1.11	Compromising user credentials.....	27
5.2	Reconciliation of objectives with OPC UA security mechanisms.....	27
5.2.1	Overview.....	27
5.2.2	Application Authentication .....	28
5.2.3	User Authentication.....	28
5.2.4	Authorization.....	28
5.2.5	Confidentiality .....	28
5.2.6	Integrity .....	28
5.2.7	Auditability .....	28
5.2.8	Availability .....	29
6	Implementation and deployment considerations.....	29
6.1	Overview.....	29
6.2	Appropriate timeouts .....	29
6.3	Strict Message processing.....	29
6.4	Random number generation .....	29
6.5	Special and reserved packets.....	30
6.6	Rate limiting and flow control.....	30
6.7	Administrative access.....	30
6.8	Alarm related guidance.....	30
6.9	Program access .....	30
6.10	Audit event management.....	31
6.11	Certificate management .....	31
	Bibliography .....	36
	Figure 1 – OPC UA network model.....	13
	Figure 2 – OPC UA security architecture .....	18
	Figure 3 – Simple Servers.....	22
	Figure 4 – Aggregating Servers.....	23
	Figure 5 – Aggregation with a non-auditing Server.....	24
	Figure 6 – Aggregate Server with service distribution.....	25
	Figure 7 – Manual Certificate handling .....	32
	Figure 8 – CA Certificate handling.....	33
	Figure 9 – Certificate handling .....	34

## 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 is 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 *Profiles* 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 Applications* 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)

:X.509: 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](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](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)