IEC 62541-2

Edition 1.0 2026-02

INTERNATIONAL STANDARD

OPC unified architecture –
Part 2: Security Model

ICS 25.040

ISBN 978-2-8327-1035-7

IEC 62541-2:2026-02(en)

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

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

This edition cancels and replaces the third edition of IEC TR 62541-2, published in 2020.This edition constitutes a technical revision.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65E/1201/FDIS	65E/1206/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

Throughout this document and the 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 definitions" 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 in 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 document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

– reconfirmed,
– withdrawn, or
– revised.

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 provides definition of common security terms that are used in this and other parts of the IEC 62541 series. It gives an overview and concept of the security features that are specified in other parts of the series. It references services, mappings, and *Profile*s that are specified normatively in other parts of the 62541 series. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this document and one of the other normative parts does not remove or reduce the requirement specified in the other normative part.

There are many different aspects of security that are 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. Common security features for industrial Controls are defined in IEC 62443-4-2 and OPC UA defined a relationship to them in Annex A.

This document is directed to readers who will develop OPC UA applications. It is also for end Users that wish to understand the various security features and functionality provided by OPC UA. It also offers some recommendations that can be applied when deploying systems. These recommendations 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.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 62541-1, *OPC Unified Architecture - Part 1: Overview and Concepts*

Bibliography

IEC 62541-3, *OPC UA Specification - Part 3: Address Space Model*

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*

IEC 62541-12, *OPC Unified Architecture - Part 12: Discovery and Global Services*

IEC 62541-14, *OPC Unified Architecture - Part 14: PubSub*

IEC 62541-18, *OPC Unified Architecture - Part 18: Role-Based Security*

IEC 62541-21, *OPC Unified Architecture - Part 21: Device Onboarding*

IEC 62351, *Power systems management and associated information exchange - Data and communications security*

IEC 62443-4-2, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*

Recommendation ITU-T X.509v3 │ ISO/IEC 9594-8, *Information technology - Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

IETF RFC 2246, Dierks T. and Allen C., “The TLS Protocol Version 1.0”, January 1999, available at https://www.ietf.org/rfc/rfc2246.txt

IETF RFC 2616, Fielding R., Gettys J., Mogul J., Frystyk H., Masinter L., Leach P. and Berners-Lee T., “Hypertext Transfer Protocol - HTTP/1.1”, June 1999, available at https://www.ietf.org/rfc/rfc2616.txt

IETF RFC 2818, Rescorla E., “HTTP Over TLS”, May 2000, available at https://www.ietf.org/rfc/rfc2818.txt

IETF RFC 2986, Nystrom M., Kaliski B., “PKCS #10: Certification Request Syntax Specification Version 1.7”, November 2000, available at https://tools.ietf.org/html/rfc2986

IETF RFC 4949, Shirey R., “Internet Security Glossary, Version 2”, August 2007, available at https://www.ietf.org/rfc/rfc4949.txt

IETF RFC 5958, Turner S., “Asymmetric Key Packages”, August 2010, available at https://datatracker.ietf.org/doc/html/rfc5958

IETF RFC 6234, Eastlake D., Hansen T., “SHA-1: US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)”, May 2011, available at https://www.ietf.org/rfc/rfc6234.txt

IETF RFC 6749, Hardt D., “OAuth2: The OAuth 2.0 Authorization Framework”, October 2012, available at https://tools.ietf.org/html/rfc6749

IETF RFC 7519, Jones M., Bradley J. and Sakimura N., “JWT: JSON Web Token (JWT)”, May 2015, available at https://tools.ietf.org/html/rfc7519

IETF RFC 9549, Housley R., “Internationalization Updates to RFC 5280”, March 2024, available at https://tools.ietf.org/html/rfc9549

NIST 800-12, Introduction to Computer Security
https://csrc.nist.gov/publications/nistpubs/800-12/

NIST 800-57, Part 3: Application-Specific Key Management Guidance
https://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf

NERC CIP: CIP 002-1 through CIP 009-1, by North-American Electric Reliability Council
https://www.nerc.com/page.php?cid=2|20

SPP-ICS: Guide to Operational Technology (OT)) Security
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

PKI: Design and build a privately hosted Public Key Infrastructure
https://www.ncsc.gov.uk/collection/in-house-public-key-infrastructure/introduction-to-public-key-infrastructure/components-of-a-pki

OpenID: OpenID Connect Discovery 1.0
https://openid.net/specs/openid-connect-discovery-1_0.html

O-PAS™ Standard, Version 2.1, Copyright © 2021 The Open Group

Profile Database
https://profiles.opcfoundation.org

_____