

DIN EN 62541-2

ICS 35.200; 35.240.50

Einsprüche bis 2009-02-28

Entwurf**OPC Unified Architecture –
Teil 2: Modell für die IT-Sicherheit (IEC 65E/93/CDV:2008);
Englische Fassung FprEN 62541-2:2008**

OPC Unified Architecture –
Part 2: Security model (IEC 65E/93/CDV:2008);
English version FprEN 62541-2:2008

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2008-12-15 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an dke@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (Hausanschrift: Stresemannallee 15, 60596 Frankfurt am Main).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 33 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Nationales Vorwort

Die englische Fassung des europäischen Dokuments FprEN 62541-2:2008 „OPC Unified Architecture – Teil 2: Modell für die IT-Sicherheit“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument OPC Unified Architecture – Teil 2: Modell für die IT-Sicherheit IEC 65E/93/CDV:2008 „OPC Unified Architecture – Part 2: Security model“ unverändert in den Entwurf FprEN 62541-2:2008 übernommen worden.

Das internationale Dokument wurde vom SC 65E „System: engineering and management“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium K 931 „Systemaspekte“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnitsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

CONTENTS

Page

FOREWORD	5
INTRODUCTION	7
1 Scope	8
2 Reference documents	8
2.1 References	8
3 Terms, definitions, and abbreviations	10
3.1 OPC UA Part 1 terms	10
3.2 OPC UA Security terms	10
3.2.1 Application Instance	10
3.2.2 Application Instance Certificate	10
3.2.3 Asymmetric Cryptography	10
3.2.4 Asymmetric Encryption	10
3.2.5 Asymmetric Signature	11
3.2.6 Auditability	11
3.2.7 Auditing	11
3.2.8 Authentication	11
3.2.9 Authorization	11
3.2.10 Availability	11
3.2.11 Confidentiality	11
3.2.12 Cryptography	11
3.2.13 Cyber Security Management System (CSMS)	11
3.2.14 Digital Certificate	11
3.2.15 Digital Signature	11
3.2.16 Hash Function	12
3.2.17 Hashed Message Authentication Code (HMAC)	12
3.2.18 Integrity	12
3.2.19 Key Exchange Algorithm	12
3.2.20 Message Authentication Code (MAC)	12
3.2.21 Message Signature	12
3.2.22 Non-Repudiation	12
3.2.23 Nonce	12
3.2.24 OPC UA Application	12
3.2.25 Private Key	12
3.2.26 Public Key	13
3.2.27 Public Key Infrastructure (PKI)	13
3.2.28 Rivest-Shamir-Adleman (RSA)	13
3.2.29 Secure Channel	13
3.2.30 Symmetric Cryptography	13
3.2.31 Symmetric Encryption	13
3.2.32 Symmetric Signature	13
3.2.33 X.509 Certificate	13
3.3 Abbreviations and symbols	13
3.4 Conventions	14
3.4.1 Conventions for security model figures	14
4 OPC UA Security architecture	

4.1	OPC UA Security Environment.....	14
4.2	Security Objectives	15
4.2.1	Overview.....	15
4.2.2	Authentication	15
4.2.3	Authorization.....	16
4.2.4	Confidentiality	16
4.2.5	Integrity	16
4.2.6	Auditability	16
4.2.7	Availability	16
4.3	Security Threats to OPC UA Systems	16
4.3.1	Overview.....	16
4.3.2	Message Flooding.....	16
4.3.3	Eavesdropping	17
4.3.4	Message Spoofing	17
4.3.5	Message Alteration	17
4.3.6	Message Replay	17
4.3.7	Malformed Messages	17
4.3.8	Server Profiling	18
4.3.9	Session Hijacking.....	18
4.3.10	Rogue Server.....	18
4.3.11	Compromising User Credentials	18
4.4	OPC UA Relationship to Site Security	19
4.5	OPC UA Security Architecture	20
4.6	Security Policies	21
4.7	Security Profiles	22
4.8	User Authorization	22
4.9	User Authentication	22
4.10	Application Authentication.....	22
4.11	OPC UA Security Related Services	22
4.12	Auditing	23
4.12.1	General.....	23
4.12.2	Single client and server.....	24
4.12.3	Aggregating server.....	25
4.12.4	Aggregation through a non-auditing server.....	26
4.12.5	Aggregating server with service distribution	27
5	Security Reconciliation.....	28
5.1	Reconciliation of Threats with OPC UA Security Mechanisms	28
5.1.1	Overview.....	28
5.1.2	Message Flooding.....	28
5.1.3	Eavesdropping	28
5.1.4	Message Spoofing	29
5.1.5	Message Alteration	29
5.1.6	Message Replay	29
5.1.7	Malformed Messages	29
5.1.8	Server Profiling	29
5.1.9	Session Hijacking.....	29
5.1.10	Rogue Server.....	29
5.1.11	Compromising User Credentials	30
5.2	Reconciliation of Objectives with OPC UA Security Mechanisms.....	30

5.2.1	Overview.....	30
5.2.2	Authentication.....	30
5.2.3	Authorization.....	30
5.2.4	Confidentiality.....	30
5.2.5	Integrity	31
5.2.6	Auditability.....	31
5.2.7	Availability	31
6	Implementation considerations.....	31
6.1	Appropriate Timeouts:.....	31
6.2	Strict Message Processing.....	32
6.3	Random Number Generation.....	32
6.4	Special and Reserved Packets.....	32
6.5	Rate Limiting and Flow Control	32
Figure 1 - OPC UA Network Model		15
Figure 2 – OPC UA Security Architecture		20
Figure 3 – Simple Servers		24
Figure 4 – Aggregating Servers.....		25
Figure 5 – Aggregation with a Non-Auditing Server		26
Figure 6 – Aggregate server with Service Distribution		27

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC Unified Architecture Specification

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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.

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

The text of this standard is based on the following documents:

FDIS	Report on voting
65E/XX/FDIS	65E/XX/RVD

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, 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 maintenance result date¹ 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.

1

The National Committees are requested to note that for this publication the maintenance result date is 2018.

INTRODUCTION

This specification is the specification for developers of OPC UA applications. The specification is a result of an analysis and design process to develop a standard interface to facilitate the development of applications by multiple vendors that shall inter-operate seamlessly together.

OPC Unified Architecture Specification

Part 2: Security Model

1 Scope

This specification 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 multi-part specification. This part of the specification is informative rather than normative. Any seeming ambiguity between this part and one of the normative parts does not remove or reduce the requirement specified in the normative part.

This Part 2 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 Reference documents

2.1 References

Part 1: IEC 62541-1 OPC UA Specification: Part 1 – Overview and Concepts

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

Part 4: IEC 62541-4 OPC UA Specification: Part 4 – Services

Part 5: IEC 62541-5 OPC UA Specification: Part 5 – Information Model

Part 6: IEC 62541-6 OPC UA Specification: Part 6 – Mappings

Part 7: IEC 62541-7 OPC UA Specification: Part 7 – Profiles

Part 12: IEC 62541-12 OPC UA Specification: Part 12 – Discovery

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

<http://www.w3.org/TR/soap12-part1/>

SOAP Part 2: SOAP Version 1.2 Part 2: Adjuncts

<http://www.w3.org/TR/soap12-part2/>

XML Encryption: XML Encryption Syntax and Processing

<http://www.w3.org/TR/xmlenc-core/>

XML Signature:: XML-Signature Syntax and Processing

<http://www.w3.org/TR/xmldsig-core/>

WS Security: SOAP Message Security 1.1

<http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>

WS Addressing: Web Services Addressing (WS-Addressing)

<http://www.w3.org/Submission/ws-addressing/>

WS Trust: Web Services Trust Language (WS-Trust)

<http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf>

WS Secure Conversation: WebServices Secure Conversation Language (WS-SecureConversation)

<http://specs.xmlsoap.org/ws/2005/02/sc/WS-SecureConversation.pdf>

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

<http://www.ietf.org/rfc/rfc2246.txt>

:X509: X.509 Public Key Certificate Infrastructure

<http://www.itu.int/rec/T-REC-X.509-200003-I/e>

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

<http://www.ietf.org/rfc/rfc2616.txt>

HTTPS: RFC 2818: HTTP Over TLS

<http://www.ietf.org/rfc/rfc2818.txt>

IS Glossary: Internet Security Glossary

<http://www.ietf.org/rfc/rfc2828.txt>

NIST 800-12: Introduction to Computer Security

<http://csrc.nist.gov/publications/nistpubs/800-12/>

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

<http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

IEC 62351: Data and Communications Security

http://www.iec.ch/heb/d_md doc-e050507.htm

SPP-ICS: System Protection Profile – Industrial Control System, by Process Control Security Requirements Forum (PCSRF)

<http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf>

SHA-1: Secure Hash Algorithm RFC

<http://tools.ietf.org/html/rfc3174>

PKI: Public Key Infrastructure article in Wikipedia

http://en.wikipedia.org/wiki/Public_key_infrastructure

X509 PKI: Internet X.509 Public Key Infrastructure

<http://www.ietf.org/rfc/rfc3280.txt>