

TECHNICAL REPORT



OPC unified architecture –
Part 2: Security Model

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC TR 62541-2:2020](https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020)

<https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020>



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2020 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 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 TR 62541-2:2020](https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020)

<https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020>



TECHNICAL REPORT



OPC unified architecture –
Part 2: Security Model

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC TR 62541-2:2020](https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020)

<https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.01

ISBN 978-2-8322-9089-7

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

CONTENTS

FOREWORD	5
1 Scope	8
2 Normative references	8
3 Terms, definitions, and abbreviated terms	10
3.1 Terms and definitions.....	10
3.2 Abbreviated terms.....	15
4 OPC UA security architecture	16
4.1 OPC UA security environment.....	16
4.2 Security objectives.....	17
4.2.1 Overview	17
4.2.2 Authentication.....	17
4.2.3 Authorization	18
4.2.4 Confidentiality.....	18
4.2.5 Integrity	18
4.2.6 Non-Repudiation.....	18
4.2.7 Auditability.....	18
4.2.8 Availability	18
4.3 Security threats to OPC UA systems.....	18
4.3.1 Overview	18
4.3.2 Denial of Service	19
4.3.3 Eavesdropping.....	20
4.3.4 Message spoofing.....	20
4.3.5 Message alteration	20
4.3.6 Message replay	20
4.3.7 Malformed Messages.....	21
4.3.8 Server profiling	21
4.3.9 Session hijacking.....	21
4.3.10 Rogue Server	21
4.3.11 Rogue Publisher	22
4.3.12 Compromising user credentials.....	22
4.3.13 Repudiation	22
4.4 OPC UA relationship to site security	22
4.5 OPC UA security architecture	23
4.5.1 Overview	23
4.5.2 Client / Server	24
4.5.3 Publish-Subscribe.....	25
4.6 SecurityPolicies	26
4.7 Security Profiles.....	27
4.8 Security Mode Settings	27
4.9 User Authentication	28
4.10 Application Authentication.....	28
4.11 User Authorization	28
4.12 Roles	28
4.13 OPC UA security related Services.....	29
4.14 Auditing	30
4.14.1 General	30

4.14.2	Single Client and Server	31
4.14.3	Aggregating Server	31
4.14.4	Aggregation through a non-auditing Server	32
4.14.5	Aggregating Server with service distribution	33
5	Security reconciliation	34
5.1	Reconciliation of threats with OPC UA security mechanisms	34
5.1.1	Overview	34
5.1.2	Denial of Service	35
5.1.3	Eavesdropping	36
5.1.4	Message spoofing	36
5.1.5	Message alteration	37
5.1.6	Message replay	37
5.1.7	Malformed Messages	37
5.1.8	Server profiling	37
5.1.9	Session hijacking	37
5.1.10	Rogue Server or Publisher	38
5.1.11	Compromising user credentials	38
5.1.12	Repudiation	38
5.2	Reconciliation of objectives with OPC UA security mechanisms	38
5.2.1	Overview	38
5.2.2	Application Authentication	38
5.2.3	User Authentication	39
5.2.4	Authorization	39
5.2.5	Confidentiality	39
5.2.6	Integrity	39
5.2.7	Auditability	39
5.2.8	Availability	40
6	Implementation and deployment considerations	40
6.1	Overview	40
6.2	Appropriate timeouts	40
6.3	Strict Message processing	40
6.4	Random number generation	41
6.5	Special and reserved packets	41
6.6	Rate limiting and flow control	41
6.7	Administrative access	41
6.8	Cryptographic Keys	42
6.9	Alarm related guidance	42
6.10	Program access	42
6.11	Audit event management	43
6.12	OAuth2, JWT and User roles	43
6.13	HTTPs, SSL/TLS & Websockets	43
6.14	Reverse Connect	43
7	Unsecured Services	44
7.1	Overview	44
7.2	Multicast Discovery	44
7.3	Global Discovery Server Security	44
7.3.1	Overview	44
7.3.2	Rogue GDS	44
7.3.3	Threats against a GDS	45

7.3.4	Certificate management threats	45
8	Certificate management.....	46
8.1.1	Overview	46
8.1.2	Self-signed certificate management	46
8.1.3	CA Signed Certificate management	47
8.1.4	GDS Certificate Management	48
	Bibliography.....	52
	Figure 1 – OPC UA network model example	17
	Figure 2 – OPC UA security architecture – Client / Server	23
	Figure 3 – OPC UA security architecture – Publisher-Subscriber	24
	Figure 4 – Role overview	29
	Figure 5 – Simple Servers.....	31
	Figure 6 – Aggregating Servers	32
	Figure 7 – Aggregation with a non-auditing Server.....	33
	Figure 8 – Aggregate Server with service distribution.....	34
	Figure 9 – Manual Certificate handling.....	47
	Figure 10 – CA Certificate handling	48
	Figure 11 – Certificate handling.....	49
	Table 1 – Security Reconciliation Threats Summary	35

iTech Standards
 (https://standards.itih.ai)
 Document Preview

[IEC TR 62541-2:2020](https://standards.itih.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020)

<https://standards.itih.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020>

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.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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.

This third edition cancels and replaces the second edition of IEC TR 62541-2, published in 2016. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) protection-targets definition change;
- b) threat type clarifications;
- c) expanded best practices;
- d) added Websockets;
- e) added Pub/Sub.

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

Enquiry draft	Report on voting
65E/679/DTR	65E/703/RVDR

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

<https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020>

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 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.

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.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[IEC TR 62541-2:2020](https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020)

<https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020>

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 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~~ the OPC UA Specification. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this part and one of the *other* normative parts does not remove or reduce the requirement specified in the *other* normative part.

Note It is important to understand 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 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 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 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*

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

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

IEC 62351 (all parts), *Power systems management and associated information exchange*

~~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/xmlsig-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 abbreviated terms

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1.1

Access Restriction

limit on the circumstances where an operation, such as a read, write or a call, can be performed on a *Node*

Note 1 to entry: Operations can only be performed on a *Node* if the *Client* has the necessary *Permissions* and has satisfied all of the *Access Restrictions*.

3.1.2

Access Token

digitally signed document that asserts that the subject is entitled to access a *Resource*

Note 1 to entry: The document includes the name of the subject and the *Resource* being accessed.

3.1.3

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.

3.1.4

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. The use of an *Application Instance Certificate* for uses outside of what is described in the specification could greatly reduce the security provided by the *Application Instance Certificate* and should be discouraged.

3.1.5

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~~ requires *Confidentiality* for data ~~it sends~~ sent to ~~another~~ entity "B", then 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~~ requires message Integrity or to provide *Authentication* for data ~~it sends~~ sent 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~~ its own Private Key and the other's Public Key to compute the new key value.' according to IS Glossary.

3.1.6

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*

3.1.7

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*

3.1.8

Auditability

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

3.1.9

Auditing

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

3.1.10

Authentication

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

3.1.11

Authorization

ability to grant access to a system resource

Note 1 to entry: Authorization of access to resources should be based on the need-to-know principle. It is important that access is restricted in a system.

3.1.12

AuthorizationService

Server which validates a request to access a *Resource* and can return an *Access Token* that grants access to the *Resource*

Note 1 to entry: The *AuthorizationService* is also called STS (Security Token Service) in other standards.

3.1.13

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

3.1.14

Certificate Authority

entity that can issue ~~Digital~~ *Certificates*, 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

3.1.15

CertificateStore

persistent location where *Certificates* 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.

3.1.16

Claim

statement in an *Access Token* that asserts information about the subject which the *Authorization Service* knows to be true

Note 1 to entry: Claims can include username, email, and *Roles* granted to the subject.

3.1.17

Confidentiality

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

3.1.18

Cryptography

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

3.1.19

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*~~

3.1.20

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*

<https://standards.iteh.ai/catalog/standards/iec/7845ac6f-7811-47dd-bec9-074fd1b5e53f/iec-tr-62541-2-2020>

3.1.21

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)

Note 1 to entry: See IS Glossary.

3.1.22

Hashed Message Authentication Code

HMAC

MAC that has been generated using an iterative *Hash Function*

3.1.23

Integrity

security objective that assures that information has not been modified or destroyed in an unauthorized manner

Note 1 to entry: See IS Glossary.

3.1.24

Identity Provider

Server which verifies credentials provided by a *Security Principal* and returns a token which can be passed to an associated *Authorization Service*