



TECHNICAL SPECIFICATION

**Power systems management and associated information exchange – Data and communications security –
Part 2: Glossary of terms**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

CONTENTS

FOREWORD.....	9
1 Scope and object.....	11
2 Terms and definitions.....	11
2.1 Glossary references and permissions.....	11
2.2 Glossary of security and related communication terms.....	13
2.2.1 Abstract Communication Service Interface (ACSI).....	13
2.2.2 Access.....	13
2.2.3 Access Authority.....	13
2.2.4 Access Control.....	13
2.2.5 Access Control List (ACL).....	13
2.2.6 Accountability.....	13
2.2.7 Adequate Security.....	13
2.2.8 Advanced Encryption Standard (AES).....	14
2.2.9 Alarm.....	14
2.2.10 Application Layer.....	14
2.2.11 Association.....	14
2.2.12 Assurance.....	14
2.2.13 Asymmetric Cipher.....	14
2.2.14 Asymmetric Cryptography.....	14
2.2.15 Asymmetric Key Pair.....	14
2.2.16 Attack.....	14
2.2.17 Audit.....	15
2.2.18 Audit Log.....	15
2.2.19 Audit Record Field.....	15
2.2.20 Audit Trail.....	15
2.2.21 Authentic Signature.....	15
2.2.22 Authentication.....	15
2.2.23 Authorization.....	15
2.2.24 Authorization Process.....	15
2.2.25 Authorized User.....	16
2.2.26 Availability.....	16
2.2.27 Back Door.....	16
2.2.28 Bandwidth.....	16
2.2.29 Biometric.....	16
2.2.30 Block Cipher.....	16
2.2.31 Boundary Protection.....	16
2.2.32 Buffer Overflow.....	16
2.2.33 Bump-in-the-Stack.....	17
2.2.34 Bump-in-the-Wire.....	17
2.2.35 Call Back.....	17
2.2.36 Certificate.....	17
2.2.37 Certificate Management.....	17
2.2.38 Certificate Revocation List (CRL).....	17
2.2.39 Certification.....	17
2.2.40 Certification Authority (CA).....	18

2.2.41	Chain of Custody	18
2.2.42	Challenge Handshake Authentication Protocol (CHAP)	18
2.2.43	Challenge-Response, Challenge-Response Protocol.....	18
2.2.44	Checksum	18
2.2.45	Cipher	18
2.2.46	Ciphertext	19
2.2.47	Cleartext	19
2.2.48	Client	19
2.2.49	Compromise.....	19
2.2.50	Computer Emergency Response Team (CERT).....	19
2.2.51	Computer Virus	19
2.2.52	Confidentiality	19
2.2.53	Conformance Test.....	19
2.2.54	Control Network	20
2.2.55	Control System	20
2.2.56	Control System Operations	20
2.2.57	Cookie	20
2.2.58	Countermeasure	20
2.2.59	Cracker	20
2.2.60	Credential	21
2.2.61	Critical System Resource	21
2.2.62	Crypto-algorithm	21
2.2.63	Cryptographic Hash	21
2.2.64	Cryptographic Key	21
2.2.65	Cryptography	21
2.2.66	Cyber	21
2.2.67	Cyber Attack	21
2.2.68	Cyber Security	22
2.2.69	Cyclic Redundancy Check (CRC).....	22
2.2.70	Data Authentication.....	22
2.2.71	Data Corruption	22
2.2.72	Data Encryption Standard (DES).....	22
2.2.73	Data Integrity	22
2.2.74	Data Object (DO)	22
2.2.75	Data Security	22
2.2.76	Datagram	22
2.2.77	Decode	23
2.2.78	Decrypt	23
2.2.79	Decryption	23
2.2.80	De-Facto Standard.....	23
2.2.81	Defence in Depth	23
2.2.82	Denial of Service (DoS).....	23
2.2.83	Designated Approving Authority (DAA).....	24
2.2.84	Device	24
2.2.85	Diffie-Hellman Key Exchange	24
2.2.86	Digital Certificate	24
2.2.87	Digital Data	24
2.2.88	Digital Signature	24
2.2.89	Digital Signature Standard (DSS).....	25

2.2.90	Distributed Control System (DCS)	25
2.2.91	Dongle	25
2.2.92	Eavesdropping	25
2.2.93	Electronic Deception	25
2.2.94	Elliptic Curve Cryptography	25
2.2.95	Encrypt	25
2.2.96	Encryption	25
2.2.97	Firewall	26
2.2.98	Flooding	26
2.2.99	Flow Control	26
2.2.100	Functions	26
2.2.101	Gateway	26
2.2.102	Generic Upper Layer Security (GULS)	26
2.2.103	Hacker	26
2.2.104	Hash Function	27
2.2.105	Honey Pot	27
2.2.106	Identification	27
2.2.107	IEEE 802.11i	27
2.2.108	Information Security	27
2.2.109	Instrumentation, Systems, and Automation Society (ISA)	27
2.2.110	Integrity	27
2.2.111	Intelligent Electronic Device (IED)	28
2.2.112	Intercept	28
2.2.113	Interchangeability	28
2.2.114	Interface	28
2.2.115	Internet Protocol security (IPsec)	28
2.2.116	Interoperability	28
2.2.117	Intruder	28
2.2.118	Intrusion Detection System (IDS)	29
2.2.119	Key	29
2.2.120	Key Distribution	29
2.2.121	Key Logger	29
2.2.122	Key Pair	29
2.2.123	Key Update	29
2.2.124	Latency	29
2.2.125	Local Area Network (LAN)	29
2.2.126	Malicious Code	29
2.2.127	Malware	30
2.2.128	Management Information Base (MIB)	30
2.2.129	Man-in-the-Middle Attack	30
2.2.130	Manufacturing Message Specification (MMS)	30
2.2.131	Masquerade	30
2.2.132	Mockingbird	31
2.2.133	Multicast	31
2.2.134	Network Layer Protocol	31
2.2.135	Network Management	31
2.2.136	Non-repudiation	31
2.2.137	Object Identifier (OID)	31
2.2.138	Open Protocol	31

2.2.139	Open System	31
2.2.140	Open Systems Architecture	32
2.2.141	Open Systems Interconnection – Reference Model (OSI-RM).....	32
2.2.142	Password.....	32
2.2.143	Personal Identification Number (PIN)	32
2.2.144	Phishing.....	32
2.2.145	Physical Layer Protocol.....	32
2.2.146	Plaintext.....	32
2.2.147	Point-to-Point Protocol (PPP).....	33
2.2.148	Port Scanning	33
2.2.149	Pretty Good Privacy (PGP)	33
2.2.150	Private Key	33
2.2.151	Protection Profile	33
2.2.152	Proxy, Proxy Server	33
2.2.153	Pseudorandom Number Generator (PRNG).....	34
2.2.154	Public Key.....	34
2.2.155	Public Key Asymmetric Cryptographic Algorithm	34
2.2.156	Public Key Certificate.....	34
2.2.157	Public Key Cryptography.....	34
2.2.158	Public Key Infrastructure (PKI)	35
2.2.159	Replay Attack.....	35
2.2.160	Repudiation	35
2.2.161	Risk	35
2.2.162	Risk Assessment	35
2.2.163	Risk Management	35
2.2.164	Rivest, Shamir and Adleman (RSA).....	36
2.2.165	Role Based Access Control (RBAC).....	36
2.2.166	Secret Key	36
2.2.167	Secret Key Encryption.....	36
2.2.168	Secret Key Symmetric Cryptographic Algorithm	36
2.2.169	Secure Hash Algorithm (SHA).....	36
2.2.170	Secure Shell (SSH).....	36
2.2.171	Secure Sockets Layer (SSL)	36
2.2.172	Secure/ Multipurpose Internet Mail Extensions (S/MIME)	37
2.2.173	Security	37
2.2.174	Security Domain.....	37
2.2.175	Security Guidelines	37
2.2.176	Security Management	37
2.2.177	Security Performance.....	37
2.2.178	Security Perimeter	37
2.2.179	Security Policy	38
2.2.180	Security Risk Assessment.....	38
2.2.181	Security Services	38
2.2.182	Server.....	38
2.2.183	Session Key.....	38
2.2.184	Shoulder Surfing	38
2.2.185	Signature Certificate	38
2.2.186	Simple Network Management Protocol (SNMP).....	38
2.2.187	Smart Card	39

2.2.188	Smurf.....	39
2.2.189	Sniffing	39
2.2.190	Social Engineering.....	39
2.2.191	Spoof.....	39
2.2.192	Spyware.....	39
2.2.193	Strong Authentication.....	39
2.2.194	Strong Secret.....	39
2.2.195	Supervisory Control and Data Acquisition (SCADA)	39
2.2.196	Symmetric Cryptography	40
2.2.197	Symmetric Key.....	40
2.2.198	Symmetric Key Algorithm	40
2.2.199	SYN Flood	40
2.2.200	Tamper Detection	40
2.2.201	Tampering.....	40
2.2.202	TASE.2	40
2.2.203	Threat.....	40
2.2.204	Throughput	40
2.2.205	Traffic Analysis	41
2.2.206	Transport Level Security (TLS)	41
2.2.207	Trap Door	41
2.2.208	Triple DES	41
2.2.209	Trojan Horse.....	41
2.2.210	Trust.....	41
2.2.211	Tunnel	42
2.2.212	Unforgeable	42
2.2.213	Update Key.....	42
2.2.214	Virtual Private Network (VPN).....	42
2.2.215	Virus	43
2.2.216	Vulnerability.....	43
2.2.217	Vulnerability Assessment.....	43
2.2.218	Wide Area Network (WAN).....	43
2.2.219	WiFi	43
2.2.220	Wired Equivalent Privacy (WEP).....	43
2.2.221	Wireless Application Protocol (WAP).....	44
2.2.222	Wireless LAN (WLAN).....	44
2.2.223	Worm.....	44
2.2.224	X.509	44
3	Abbreviations	45
3.1.1	3DES	45
3.1.2	ACL	45
3.1.3	ACSI.....	45
3.1.4	AES	45
3.1.5	AGA.....	45
3.1.6	ANSI.....	45
3.1.7	BIS	45
3.1.8	BSI	45
3.1.9	BTW	45
3.1.10	CA	45
3.1.11	CERT.....	45

3.1.12	CHAP.....	45
3.1.13	CIP.....	45
3.1.14	CRC.....	45
3.1.15	CRL.....	45
3.1.16	DAA.....	45
3.1.17	DCS.....	45
3.1.18	DES.....	45
3.1.19	DO.....	45
3.1.20	DoS.....	45
3.1.21	DSS.....	45
3.1.22	ECC.....	45
3.1.23	EM/RF.....	45
3.1.24	EMS.....	45
3.1.25	FIPS.....	45
3.1.26	GULS.....	45
3.1.27	ICCP.....	45
3.1.28	IDS.....	46
3.1.29	IED.....	46
3.1.30	IEEE.....	46
3.1.31	IETF.....	46
3.1.32	IPS.....	46
3.1.33	IPsec.....	46
3.1.34	ISA.....	46
3.1.35	ISO.....	46
3.1.36	IT.....	46
3.1.37	LAN.....	46
3.1.38	MIB.....	46
3.1.39	MMS.....	46
3.1.40	NERC.....	46
3.1.41	NIST.....	46
3.1.42	OID.....	46
3.1.43	OSI-RM.....	46
3.1.44	PGP.....	46
3.1.45	PICS.....	46
3.1.46	PIN.....	46
3.1.47	PIXIT.....	46
3.1.48	PKI.....	46
3.1.49	PLC.....	46
3.1.50	PLC.....	47
3.1.51	PPP.....	47
3.1.52	PRNG.....	47
3.1.53	RA.....	47
3.1.54	RBAC.....	47
3.1.55	RSA.....	47
3.1.56	RTU.....	47
3.1.57	SCADA.....	47
3.1.58	SHA.....	47
3.1.59	SNMP.....	47
3.1.60	SSH.....	47

3.1.61	SSL.....	47
3.1.62	TASE.2	47
3.1.63	TDEA	47
3.1.64	TDES	47
3.1.65	TLS.....	47
3.1.66	VPN	47
3.1.67	WAN	47
3.1.68	WEP	47
3.1.69	WiFi	47
3.1.70	WLAN	47
3.1.71	WPA	47
BIBLIOGRAPHY		48

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 2: Glossary of terms

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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- The subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62351-2, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

Enquiry draft	Report on voting
57/853/DTS	57/922/RVC

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

A list of all parts of the IEC 62351 series, under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual edition of this document may be issued at a later date.

**POWER SYSTEMS MANAGEMENT AND
ASSOCIATED INFORMATION EXCHANGE –
DATA AND COMMUNICATIONS SECURITY –**

Part 2: Glossary of terms

1 Scope and object

This part of IEC 62351 covers the key terms used in the IEC 62351 series, and is not meant to be a definitive list. Most terms used for cyber security are formally defined by other standards organizations, and so are included here with references to where they were originally defined.