TECHNICALIECSPECIFICATIONTS 62351-6

First edition 2007-06

Power systems management and associated information exchange – Data and communications security –

Part 6: i Security for IEC 61850 REVIEW (standards.iteh.ai)

<u>IEC TS 62351-6:2007</u> https://standards.iteh.ai/catalog/standards/sist/24a7b2ee-c5af-4636-be9d-1b48c725f0c9/iec-ts-62351-6-2007



Reference number IEC/TS 62351-6:2007(E)



THIS PUBLICATION IS COPYRIGHT PROTECTED Copyright © 2007 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 Varembé CH-1211 Geneva 20 Switzerland Email: inmail@iec.ch Web: 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 corrigenda or an amendment might have been published.

Catalogue of IEC publications: www.iec.ch/searchpub The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

• IEC Just Published: www.iec.ch/online news/justpub ros.iteh.ai) Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

Customer Service Centre: www.iec.ch/webstore/custserv2351-6:2007

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us: 1b48c725f0c9/iec-ts-62351-6-2007

Email: csc@iec.ch Tel.: +41 22 919 02 11 Fax: +41 22 919 03 00

TECHNICALIECSPECIFICATIONTS 62351-6

First edition 2007-06

Power systems management and associated information exchange – Data and communications security –

Part 6: i Security for IEC 61850 REVIEW (standards.iteh.ai)

<u>IEC TS 62351-6:2007</u> https://standards.iteh.ai/catalog/standards/sist/24a7b2ee-c5af-4636-be9d-1b48c725f0c9/iec-ts-62351-6-2007



Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

CONTENTS

1 Scope and object. 5 1.1 Scope 5 1.2 Object 5 2 Normative references 5 3 Definitions 6 4 Security issues addressed by this specification 6 4.1 Operational issues affecting choice of security options 6 4.2 Security threats countered 7 4.3 Attack methods countered 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.1.3 Substation communications 7 5.1.4 General format of profiles using VLAN IDs 8 6 IEC 61850 security for profiles using VLAN IDs 8 7.1 Deereit format of extended PDU 8 7.2 IEC 61850 security for profiles using VLAN IDs 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU 8 7.2.2 Format of extended	FOI	REWC	DRD	3		
1.1 Scope	1	Scop	e and object	5		
1.2 Object 5 Normative references 5 3 Definitions 6 4 Security issues addressed by this specification 6 4 Security threats countered 7 4.1 Operational issues affecting choice of security options 6 4.2 Security threats countered 7 5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDs 8 6 IEC 61850 security for profiles using VLAN IDs 8 7 S.1.3 Substation communications 7 7.2 IEC 61850 security for profiles using VLAN IDs 8 7 7 Z Extended PDU 8 7.1 Overview of VLAN usage and IEC 61850 (informative) 8 7.2.2 Format of extension poletic security informative) 8 7.2.2 1 6 7.2.1 General format of extended PDU 8 7.2.2		1.1	Scope	5		
2 Normative references 5 3 Definitions 6 4 Security issues addressed by this specification 6 4.1 Operational issues affecting choice of security options 6 4.1 Operational issues affecting choice of security options 6 4.1 Operational issues affecting choice of security options 6 4.2 Security threats countered 7 4.3 Attack methods countered 7 5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.1.4 Centrol resonance 8 7 IEC 61850 security for profiles using VLAN IDS 8 6 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (momative) 8 7.2.1 General format of extended PDU 8 7.2.2 Format of extended PDU 8 7.2.3 Substation configuration language 12 </td <td></td> <td>1.2</td> <td>Object</td> <td>5</td>		1.2	Object	5		
3 Definitions 6 4 Security issues addressed by this specification 6 4.1 Operational issues affecting choice of security options 6 4.2 Security threats countered 7 4.3 Attack methods countered 7 5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDS 8 6 IEC 61850 security for SNTP T. AND A DEPENTEW 8 7 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2.2 Format of extended PDU 8 7.2.3 Substation configuration language 12 8.1 General conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming VLAN profile security 14 <	2	Norm	ative references	5		
4 Security issues addressed by this specification 6 4.1 Operational issues affecting choice of security options 6 4.2 Security threats countered 7 4.3 Attack methods countered 7 5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDs 8 6 IEC 61850 security for profiles using VLAN technologies, 8 7.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU 8 7.2.2 Format of extended PDU 8 7.2.3 Substation configuration language 12 8.1 General conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14	3	Defin	itions	6		
4.1 Operational issues affecting choice of security options 6 4.2 Security threats countered 7 4.3 Attack methods countered 7 5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDs 8 6 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU ^{-2.007} 8 7.2.1 General format of extended PDU ^{-2.007} 8 7.2.2 Format of extended PDU ^{-2.007} 8 7.2.3 Substation configuration language 12 8 7.2.1 General formation extended PDU ^{-2.007} 9 7.2.3 Substation configuration language 12 12 8 Conformance 13	4	Secu	rity issues addressed by this specification	6		
4.2 Security threats countered 7 4.3 Attack methods countered 7 5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDs 8 6 IEC 61850 security for profiles using VLAN IDs 8 7 IEC 61850 security for profiles using VLAN Icbchologies 8 7.1 Overview of VLAN usage and IEC 61859 (Informative) 8 7.2.2 Extended PDU 8 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.1 General conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming SNTP profile security 14 8.4 <td></td> <td>4.1</td> <td>Operational issues affecting choice of security options</td> <td>6</td>		4.1	Operational issues affecting choice of security options	6		
4.3 Attack methods countered 7 5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDS 8 6 IEC 61850 security for SNTP TABLE ADD PREVIEW 8 7 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2.2 Extended PDU 8 7.2.1 7.2.3 Substation configuration language 8 7.2.2 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming SNTP profile security 14 8.3 Conformance for implementations claiming SNTP profile security 15		4.2	Security threats countered	7		
5 Correlation of IEC 61850 parts and IEC 62351 parts 7 5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.1.3 Substation communications 7 5.1.4 Control centre to substation 7 5.1.5 Substation communications 7 5.1.6 Control centre to substation 7 5.1.7 Substation communications 7 5.1.8 Substation communications 7 5.1.1 Control centre to substation 7 5.1.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU- 8 7.2.2 Format of extended PDU- 8 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 <		4.3	Attack methods countered	7		
5.1 IEC 61850 security for profiles using ISO 9506 (MMS) 7 5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDS 8 6 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU 8 7.2.2 Format of extended PDU 8 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations cl	5	Corre	elation of IEC 61850 parts and IEC 62351 parts	7		
5.1.1 General 7 5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDS 8 6 IEC 61850 security for SNEP AND ARD PREVIEW 8 7 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU ^{C2007} 7 7.2.2 Format of extended PDU ^{C2007} 8 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography </td <td></td> <td>5.1</td> <td>IEC 61850 security for profiles using ISO 9506 (MMS)</td> <td>7</td>		5.1	IEC 61850 security for profiles using ISO 9506 (MMS)	7		
5.1.2 Control centre to substation 7 5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDs 8 6 IEC 61850 security for profiles using VLAN technologies 8 7 IEC 61850 security for profiles using VLAN technologies 8 7 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDUccoor 8 7.2.2 Format of extended PDUccoor 9 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for certificates 12 8 Figure 1 – General format of extended PDU 8 9 Figure 2 – SCL extensions for certificates 12 9 Figure 3 – Extension to A			5.1.1 General	7		
5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN IDs 8 6 IEC 61850 security for SNTP T. A. N.D.A. R.D. P.P.F.V.H.W. 8 7 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU 62007 7.2.1 7.2.2 Format of extended PDU 0515 (2007) 9 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for certificates 12 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 13 Table 1 – Scope of application			5.1.2 Control centre to substation	7		
5.2 IEC 61850 security for profiles using VLAN IDs			5.1.3 Substation communications	7		
6 IEC 61850 security for SNTP CANDARD PREVIEW. 8 7 IEC 61850 security for profiles using VLAN technologies. 8 7.1 Overview of VLAN usage and IEC 61850 (informative) 8 7.2 Extended PDU. 8 7.2.1 General format of extended PDU 62007 8 7.2.2 Format of extension octets is 100 sectors 100 sect		5.2	IEC 61850 security for profiles using VLAN IDs	8		
7 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 (informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU 50007 8 7.2.2 Format of extended PDU 50007 9 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 15 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards 5 Table 2 – Extract from IEC 61850-9-2 (informative)	6	IEC 6	1850 security for SNTP	8		
7.1 Overview of VLAN usage and IEC 61850 (Informative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PDU 02007 8 7.2.2 Format of extension octets receive 62051-62007 9 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 12 Figure 3 – Extension to AccessPoint SCL definition 13 13 Table 1 – Scope of application to standards 5 5 Table 2 – E	7	IEC 6	1850 security for profiles using VLAN technologies	8		
7.2 Extended PDU 8 7.2.1 General format of extended PDU ⁶²⁰⁰⁷ 8 7.2.2 Format of extended PDU ⁶²⁰⁰⁷ 9 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 12 Figure 3 – Extension to AccessPoint SCL definition 13 13 Table 1 – Scope of application to standards 5 5 Table 2 – Extr		7.1	Overview of VLAN usage and IEC 61850 (informative)	8		
7.2.1 General format of extended PDU ²⁰⁰⁰ 8 7.2.2 Format of extension oxtels current assize 247b2ce-c5aF4636-be94 9 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards 5 Table 2 – Extract from IEC 61850-9-2 (informative) 11 Table 3 – Conformance table 14 Table 4 – PICS for ISO 9506 profile 14 Table 5 – PICS for VLAN profiles 14 Table 6 – PICS for SNTP profiles 15		7.2	Extended PDU	8		
7.2.2 Format of extension octets 9 7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards 5 Table 2 – Extract from IEC 61850-9-2 (informative) 11 Table 3 – Conformance table 14 Table 4 – PICS for ISO 9506 profile 14 Table 5 – PICS for VLAN profiles 14 Table 6 – PICS for SNTP profiles 15			7.2.1 General format of extended PDU0:2007	8		
7.2.3 Substation configuration language 12 8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards 5 Table 2 – Extract from IEC 61850-9-2 (informative) 11 Table 3 – Conformance table 14 Table 4 – PICS for ISO 9506 profile 14 Table 5 – PICS for VLAN profiles 14 Table 6 – PICS for SNTP profiles 14			7.2.2 Format of extension octets/ icc -is-62351-6-2007	9		
8 Conformance 13 8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards 5 Table 2 – Extract from IEC 61850-9-2 (informative) 11 Table 3 – Conformance table 14 Table 4 – PICS for ISO 9506 profile 14 Table 5 – PICS for VLAN profiles 14 Table 6 – PICS for SNTP profiles 14			7.2.3 Substation configuration language	. 12		
8.1 General conformance 13 8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards 5 Table 2 – Extract from IEC 61850-9-2 (informative) 11 Table 3 – Conformance table 14 Table 4 – PICS for ISO 9506 profile 14 Table 5 – PICS for VLAN profiles 14 Table 6 – PICS for SNTP profiles 14	8	Confo	ormance	.13		
8.2 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming VLAN profile security 14 8.4 Conformance for implementations claiming SNTP profile security 15 Bibliography 16 Figure 1 – General format of extended PDU 8 Figure 2 – SCL extensions for certificates 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards 5 Table 2 – Extract from IEC 61850-9-2 (informative) 11 Table 3 – Conformance table 14 Table 4 – PICS for ISO 9506 profile 14 Table 5 – PICS for VLAN profiles 14 Table 6 – PICS for SNTP profiles 15		8.1	General conformance	.13		
8.3 Conformance for implementations claiming VLAN profile security. 14 8.4 Conformance for implementations claiming SNTP profile security. 15 Bibliography. 16 Figure 1 – General format of extended PDU. 8 Figure 2 – SCL extensions for certificates. 12 Figure 3 – Extension to AccessPoint SCL definition 13 Table 1 – Scope of application to standards. 5 Table 2 – Extract from IEC 61850-9-2 (informative) 11 Table 3 – Conformance table 14 Table 4 – PICS for ISO 9506 profile 14 Table 5 – PICS for VLAN profiles 14 Table 6 – PICS for SNTP profiles 15		8.2	Conformance for implementations claiming ISO 9506 profile security	. 14		
8.4 Conformance for implementations claiming SNTP profile security		8.3	Conformance for implementations claiming VLAN profile security	. 14		
Bibliography16Figure 1 – General format of extended PDU8Figure 2 – SCL extensions for certificates12Figure 3 – Extension to AccessPoint SCL definition13Table 1 – Scope of application to standards5Table 2 – Extract from IEC 61850-9-2 (informative)11Table 3 – Conformance table14Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15		8.4	Conformance for implementations claiming SNTP profile security	. 15		
Figure 1 – General format of extended PDU. .8 Figure 2 – SCL extensions for certificates .12 Figure 3 – Extension to AccessPoint SCL definition .13 Table 1 – Scope of application to standards .5 Table 2 – Extract from IEC 61850-9-2 (informative) .11 Table 3 – Conformance table .14 Table 4 – PICS for ISO 9506 profile .14 Table 5 – PICS for VLAN profiles .14 Table 6 – PICS for SNTP profiles .15	Bib	liograi	ohv	. 16		
Figure 1 – General format of extended PDU.8Figure 2 – SCL extensions for certificates12Figure 3 – Extension to AccessPoint SCL definition13Table 1 – Scope of application to standards5Table 2 – Extract from IEC 61850-9-2 (informative)11Table 3 – Conformance table14Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15		0 1				
Figure 2 – SCL extensions for certificates12Figure 3 – Extension to AccessPoint SCL definition13Table 1 – Scope of application to standards5Table 2 – Extract from IEC 61850-9-2 (informative)11Table 3 – Conformance table14Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15	Fig	ure 1 -	- General format of extended PDU	8		
Figure 3 – Extension to AccessPoint SCL definition13Table 1 – Scope of application to standards5Table 2 – Extract from IEC 61850-9-2 (informative)11Table 3 – Conformance table14Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15	Fig	ure 2 -	- SCL extensions for certificates	.12		
Table 1 – Scope of application to standards.5Table 2 – Extract from IEC 61850-9-2 (informative).11Table 3 – Conformance table.14Table 4 – PICS for ISO 9506 profile.14Table 5 – PICS for VLAN profiles.14Table 6 – PICS for SNTP profiles.15	Fia	ure 3 -	- Extension to AccessPoint SCL definition	.13		
Table 1 – Scope of application to standards.5Table 2 – Extract from IEC 61850-9-2 (informative).11Table 3 – Conformance table.14Table 4 – PICS for ISO 9506 profile.14Table 5 – PICS for VLAN profiles.14Table 6 – PICS for SNTP profiles.15	9					
Table 2 – Extract from IEC 61850-9-2 (informative)11Table 3 – Conformance table14Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15	Tab	ole 1 –	Scope of application to standards	5		
Table 3 – Conformance table14Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15	Tab	Table 2 – Extract from IEC 61850-9-2 (informative)1				
Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15	Tab	le 3 –	Conformance table	. 14		
Table 5 – PICS for VLAN profiles14Table 6 – PICS for SNTP profiles15	Tab	Table 4 – PICS for ISO 9506 profile1				
Table 6 – PICS for SNTP profiles	Tab	le 5 –	PICS for VLAN profiles	.14		
	Tab	. 15				

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

Part 6: Security for IEC 61850

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.
- 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 the international and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter. 1b48c725f0c9/iec-ts-62351-6-2007
- 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 62351-6, 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
57/805/DTS	57/859/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.

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

A list of all parts of the IEC 62351 series, published 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, ٠
- replaced by a revised edition, or amended.
- •

A bilingual version of this publication may be issued at a later date.

IEC TS 62351-6:2007 https://standards.iteh.ai/catalog/standards/sist/24a7b2ee-c5af-4636-be9d-1b48c725f0c9/iec-ts-62351-6-2007

Part 6: Security for IEC 61850

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the standard IEC 61850. This specification applies to at least those protocols listed in Table 1.

Table 1 – Scope of application to standards

Number	Name
IEC 61850-8-1	Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
IEC 61850-9-2	Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC 61850-6	Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs
	IEC TS 62351 6:2007

<u>IEC 1S 62351-6:2007</u> https://standards.iteh.ai/catalog/standards/sist/24a7b2ee-c5af-4636-be9d-1b48c725f0c9/iec-ts-62351-6-2007

1.2 Object

The initial audience for this specification is intended to be the members of the working groups developing or making use of the protocols listed in Table 1. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process.

The subsequent audience for this specification is intended to be the developers of products that implement these protocols.

Portions of this specification may also be of use to managers and executives in order to understand the purpose and requirements of the work.

2 Normative references

The following referenced documents are indispensable for the application 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 61850 (all parts), Communication networks and systems in substations

IEC 61850-6, Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs

IEC 61850-8-1, Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

IEC 61850-9-1, Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link

IEC 61850-9-2, Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3

IEC 62351-1, Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues

IEC 62351-2, Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms

IEC 62351-4, Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS

ISO 9506 (all parts), Industrial automation systems – Manufacturing Message Specification

ISO/IEC 8802-3, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications

iTeh STANDARD PREVIEW ISO/IEC 13239, Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures

IEEE Std. 802.1Q-2003, Virtual Bridged Local Area Networks https://standards.iteh.ai/catalog/standards/sist/24a7b2ee-c5af-4636-be9d-

RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

RFC 2313, PKCS #1: RSA Encryption Version 1.5

RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

RFC 4634, US Secure Hash Algorithms (SHA and HMAC-SHA)

3 Definitions

For the purposes of this document, the terms and definitions contained in IEC 62351-2 apply.

4 Security issues addressed by this specification

4.1 Operational issues affecting choice of security options

For applications using GOOSE and IEC 61850-9-2 and requiring 4 ms response times, multicast configurations and low CPU overhead, encryption is not recommended. Instead, the communication path selection process (e.g. the fact that GOOSE and SMV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges. However, this specification does define a mechanism for allowing confidentiality for applications where the 4 ms delivery criterion is not a concern.

NOTE The actual performance characteristics of an implementation claiming conformance to this technical specification is outside the scope of this specification.

TS 62351-6 © IEC:2007(E)

- 7 -

With the exception of confidentiality, this specification sets forth a mechanism that allows coexistence of secure and non-secure PDUs.

4.2 Security threats countered

See IEC 62351-1 for a discussion of security threats and attack methods.

If encryption is not employed, then the specific threats countered in this part include:

• unauthorized modification of information through message level authentication of the messages.

If encryption is employed, then the specific threats countered in this part include:

- unauthorized access to information through message level authentication and encryption of the messages;
- unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

4.3 Attack methods countered

The following security attack methods are intended to be countered through the appropriate implementation of the specification/recommendations found within this document:

- man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism specified within this document;
- tamper detection/message integrity; These threats will be countered through the algorithm used to create the authentication mechanism as specified within this document;
- replay: this threat will be countered through the use of specialized processing state machines specified within IEC 62351-4 and this document.

5 Correlation of IEC 61850 parts and IEC 62351 parts

5.1 IEC 61850 security for profiles using ISO 9506 (MMS)

5.1.1 General

IEC 61850 implementations claiming conformance to this specification and declaring support for the IEC 61850-8-1 profile utilizing TCP/IP and ISO 9506 (MMS) shall implement Clauses 5 and 6 of IEC 62351-4. In addition to the IEC 62351-4 specification, extensions to IEC 61850-6 (the Substation Configuration Language) shall be supported as prescribed in 7.2.3.

IEC 61850-8-1 specifies the use of MMS within a substation. However, the scope of this specification provides security specifications for use within the substation and external to the substation (e.g. Control Centre to Substation).

5.1.2 Control centre to substation

The IEC 62351-4 standard shall be used without any other additions.

5.1.3 Substation communications

The following cipher suite shall be supported in addition to those specified in IEC 62351-4.

TLS_DH_RSA_WITH_AES_128_SHA

NOTE This additional cipher suite is suggested in order to allow less CPU utilization when the communication environment is within a substation.

5.2 IEC 61850 security for profiles using VLAN IDs

For the IEC 61850 profiles specified that make use of VLAN IDs (e.g. IEC 61850-8-1 GOOSE, IEC 61850-9-1, and IEC 61850-9-2) profile security shall be provided as specified in Clause 7.

6 IEC 61850 security for SNTP

RFC 2030, including mandatory use of the authentication algorithms, shall be used.

7 IEC 61850 security for profiles using VLAN technologies

7.1 Overview of VLAN usage and IEC 61850 (informative)

This specification extends the normal IEC 61850 GOOSE and SMV PDUs. The outline of a PDU for GSE Management and GOOSE is given in Annex C of IEC 61850-8-1.

7.2 Extended PDU

7.2.1 General format of extended PDU



Figure 1 – General format of extended PDU

Figure 1 depicts the fact that the Reserved1 and Reserved2 fields are to be used for implementations claiming conformance to this specification in regards to GOOSE and SMV. This specification specifies that the:

• **Reserved1 field** shall be used to specify the number of octets conveyed by the extension octets. This value shall be contained in the first octet of the Reserved1 field. The valid range of values is zero(0) through 255. A value of zero(0) shall indicate that no extension octets are present.

The second octet of the Reserved1 field shall be reserved for future use;

 Reserved2 field shall contain a 16-bit CRC, as calculated per ISO/IEC 13239 (ISO HDLC). The CRC shall be calculated over Octets 1-8 of the VLAN information of the Extended PDU.

The CRC shall be present if the Extension Length has a non-zero value.

7.2.2 Format of extension octets

The format of the extension octet area shall be:

```
Extension::= {
    [0] IMPLICIT SEQUENCE {
        [1] IMPLICIT SEQUENCE Reserved OPTIONAL,
        [2] IMPLICIT OCTETSTRING Private OPTIONAL,
        [3] IMPLICIT AuthenticationValue OPTIONAL,
        ...
        }
}
```

Extension shall be encoded per ASN.1 Basic Encoding Rules.

The Reserved SEQUENCE is used to reserve future standardized extension per this specification. If no extension, besides Authentication and Encryption is defined in this specification, this SEQUENCE shall not be present.

Therefore a SEQUENCE of NULA length shall be considered non-conformant to this specification. (standards.iteh.ai)

The Private SEQUENCE is provided to allow vendors to convey Private information. The scope of the semantics and syntax of the contents of this SEQUENCE is out-of-scope of this specification and shall only be interoperable via prior agreement. This SEQUENCE shall only be present if there are actual contents being conveyed. 6-2007

7.2.2.1 &AuthenticationValue Algorithm

The algorithm for AuthenticationValue generation is based upon the generation of a reproducible Message Authentication Code (MAC).

The MAC shall be generated through the computation of a SHA256 hash per RFC 4634. The hash shall contain all octets of the Extended PDU with the exception of the Tag, Length, Value of the

AuthenticationValue.

The value of the hash shall then be digitally signed.

The definition for digital signature is found in RFC 2313:

"For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then an octet string containing the message digest is encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS #7 to yield a digital signature."

NOTE The reference to MD5, in the definition, is not normative. It is an example given in the RFC 2313 quoted text.

RFC 3447 (specification for PKCS#1 Version 2.1) specifies RSASA-PSS. This is the algorithm that shall be used by implementations claiming conformance to this specification. The use of RFC 3447 shall be restricted to those abilities/capabilities that are compatible with PKCS Version 1.5 (RFC 2313). The Hash algorithm shall be SHA256