TECHNICAL SPECIFICATION

IEC TS 62351-6

First edition 2007-06

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

Part 6:

Security for IEC 61850



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 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 IEC 61850 security for profiles using VLAN technologies 8 6 IEC 61850 security for profiles using VLAN technologies 8 7.1 Overview of VLAN usage and IEC 61850 kinformative) 8 7.2 Extended PDU 8 7.2.1 General format of extended PBU 8 7.2.2 Format of extension process 9 7.2.3 Substation configuration language 12 8 Conformance 15 August 16 August 17 8.1 General conformance 13 8.1 General conformance 13 8.1 General conformance 14 8.3 Conformance for implementations claiming ISO 9506 profile security 14 8.3 Conformance for implementations claiming ISO 9506 profile security 14 8.4 Conformance for implementations claiming SNTP profile security 14 8.5 Conformance for implementations claiming SNTP profile security 15 8 Ibibliography 16 8 Ibibliography 17 8 Extension to AccessPoint SCL definition 13 8 Table 1 – Scope of application to standards 5 8 Table 2 – Extract from IEC 61850-9-2 (informative) 11 8 Table 4 – PICS for ISO 9506 profile 14 8 Table 6 – PICS for SNTP profiles 15	FO	REW	ORD	3	
1.2 Object 55 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 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 6 IEC 61850 security for profiles using VLAN VBS 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 PBU 8 7.2.2 Format of extension potets 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 <td< th=""><th>1</th><th>Scor</th><th>pe and object</th><th>5</th></td<>	1	Scor	pe and 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 4.1 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 5.1.3 Substation communications 7 5.1.3 Substation communications 7 6 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 7.2.1 General conformation extended PBU 8		1.1	Scope	5	
3 Definitions		1.2	Object	5	
4 Security issues addressed by this specification	2	Norr	native references	5	
4.1 Operational issues affecting choice of security options	3	Defi	nitions	6	
4.2 Security threats countered	4	Seci	urity issues addressed by this specification	6	
4.2 Security threats countered		4.1	Operational issues affecting choice of security options	6	
5 Correlation of IEC 61850 parts and IEC 62351 parts		4.2	Security threats 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 5.2 IEC 61850 security for profiles using VLAN USS 8 6 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 formation fextended PBU 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 15 Bibliography 16 Figure 1 – General format of extended PDU 8 <t< td=""><td></td><td></td><td></td><td>.7</td></t<>				. 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 by 8 6 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 formatiof 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 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 </td <td>5</td> <td colspan="4">Correlation of IEC 61850 parts and IEC 62351 parts</td>	5	Correlation of IEC 61850 parts and IEC 62351 parts			
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 by 8 6 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 formatiof 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 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 </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	
5.1.3 Substation communications 7 5.2 IEC 61850 security for profiles using VLAN DS 8 6 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 PBU 8 7.2.2 Format of extension cotets 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 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 – E			5.1.1 General	7	
5.2 IEC 61850 security for profiles using VLAN Ds 8 6 IEC 61850 security for SNTP 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 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 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					
6 IEC 61850 security for SNTP 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 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 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			5.1.3 Substation communications	7	
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 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 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		5.2	IEC 61850 security for profiles using VLANVDs	8	
7.1 Overview of VLAN usage and IEC 61850 (informative) 8.7.2 Extended PDU		IEC	61850 security for SNTP	8	
7.2 Extended PDU. 8 7.2.1 General format of 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 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	7	IEC			
7.2.1 General format of extended PBU. 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 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					
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 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		7.2	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 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					
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 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					
8.1 General 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	0	0			
8.2 Conformance for implementations claiming ISO 9506 profile security 8.3 Conformance for implementations claiming VLAN profile security 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	8				
8.3 Conformance for implementations claiming VLAN profile security					
8.4 Conformance for implementations claiming SNTP profile security		_			
Bibliography					
Figure 1 – General format of extended PDU		0.4	Conformance for implementations claiming SNTP profile security	15	
Figure 1 – General format of extended PDU	D:h	liaana		10	
Figure 2 – SCL extensions for certificates	טוט	llogra	priy	16	
Figure 2 – SCL extensions for certificates	- :	1	Compared former of automoted DDU	0	
Figure 3 – Extension to AccessPoint SCL definition					
Table 1 – Scope of application to standards	_				
Table 2 – Extract from IEC 61850-9-2 (informative)	Fig	ure 3	Extension to AccessPoint SCL definition	13	
Table 3 – Conformance table14Table 4 – PICS for ISO 9506 profile14Table 5 – PICS for VLAN profiles14	Tal	ole 1 -	- Scope of application to standards	5	
Table 4 – PICS for ISO 9506 profile	Tal	ole 2 -	- Extract from IEC 61850-9-2 (informative)	11	
Table 5 – PICS for VLAN profiles	Tal	ole 3 -	- Conformance table	14	
Table 5 – PICS for VLAN profiles	Tal	ole 4 -	- PICS for ISO 9506 profile	14	
·					
			·		

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.
- 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 EC 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,
- replaced by a revised edition, or
- amended.

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

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

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

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

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

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)