

Contents

Preface	ix
1. Introduction	1-1
1.1 Purpose and Scope	1-1
1.2 Target Audience	1-1
1.3 Review/Concurrence Information	1-1
1.4 Structure and Use of This Document	1-1
1.5 Requirements Terminology	1-2
1.6 Requirement Labeling Conventions	1-3
1.6.1 Numbering of Requirement and Related Objects	1-3
1.6.2 Requirement, Conditional Requirement, and Objective Object Identification	1-3
1.7 Technical Terminology	1-4
1.8 Assumptions	1-6
2. General Information	2-1
2.1 Problem/Opportunity	2-1
2.1.1 Telecommunications Network Management Standards Activities	2-1
2.2 Changes to the Telecommunications Industry	2-3
2.3 Approach for SNMP Requirements	2-4
2.4 Strategy for Developing SNMP Security Requirements	2-6
2.5 Why the TMN Requires Cryptography	2-6
2.6 Why the TMN Needs a Public Key Infrastructure (PKI)	2-7
2.7 Baseline Security Requirements for NE/NSs	2-8
2.8 NE/NS Security	2-8
2.9 SNMP Framework Description	2-10
2.10 Assumptions, Dependencies, and Constraints	2-11
2.11 SNMP Version 1 Introduction and Overview	2-11
2.11.1 SNMP Version 1 Architecture	2-12
2.12 SNMP Version 2	2-14
2.13 Basic SNMP Security Overview	2-16
2.14 SNMP Version 3	2-17
2.15 SNMP Version 3 Architecture Components	2-18
2.16 SNMP Popularity Gains in the TMN	2-20
3. Threats and Vulnerabilities	3-1
3.1 Threat Origination	3-2
4. Generic Security Requirements for SNMP	4-1
4.1 Security Services Outline	4-1
4.2 Identification and Authentication (I&A)	4-2
4.2.1 User Identification and Authentication	4-2
4.3 SNMP Protocol Protection Requirements	4-4
4.3.1 Data Integrity	4-5
4.3.2 Message Origin Authentication	4-6
4.3.3 Data Confidentiality	4-7
4.3.4 Message Timeliness and Replay Protection	4-8

- 4.4 Non-Repudiation 4-9
- 4.5 Access Control 4-9
 - 4.5.1 Resource Access Control 4-10
 - 4.5.1.1 SNMPv1/2-Based Application Access Control Requirements 4-10
 - 4.5.1.2 SNMPv3-Based Application Access Control Requirements 4-11
 - 4.5.2 System Access Control 4-12
- 4.6 Security Alarm 4-12
- 4.7 Security Audit 4-13
- 4.8 Internet Gateway Screening SNMP Process 4-14
- 4.9 Trusted Computing Base (TCB) 4-16
- 4.10 TCB and Application Integrity 4-17
- 5. Implementing SNMPv1/2 Using Basic SNMPv1 Security Features 5-1
 - 5.1 Access Control 5-3
- 6. Implementing SNMP Using IPsec Security Features 6-1
 - 6.1 Rationale for Implementing IPsec in the TMN 6-1
 - 6.2 Generic IPsec Implementation Requirements 6-3
 - 6.2.1 Key Management Infrastructure 6-3
 - 6.2.2 Security Policy 6-4
 - 6.2.3 Security Association Database (SAD) 6-4
 - 6.2.4 Security Associations (SAs) 6-4
 - 6.3 IPsec Message Authentication Requirements 6-5
 - 6.3.1 Connectionless Integrity and Data Origin Authentication 6-7
 - 6.3.2 IPsec Message Confidentiality Requirements 6-8
 - 6.4 IPsec Authentication Header (AH) Requirements 6-9
 - 6.4.1 Inbound Processing of AH Packets 6-10
 - 6.5 IPsec Encapsulated Security Payload Requirements 6-10
 - 6.6 Requirements for Internet Key Exchange (IKE) 6-11
 - 6.6.1 IKE Aggressive Mode Requirements 6-11
 - 6.6.2 IKE Main Mode Requirements 6-12
 - 6.6.3 Requirements for ISAKMP Phase One, Message 1 6-12
 - 6.6.3.1 ISAKMP Authentication Method Requirements 6-12
 - 6.6.3.2 ISAKMP Pseudo Random Function Requirements 6-13
 - 6.6.3.3 ISAKMP Encryption Algorithm Requirements 6-13
 - 6.6.3.4 ISAKMP SA Lifetime Requirements 6-14
 - 6.6.3.5 ISAKMP Diffie-Hellman Group Requirements 6-14
 - 6.6.4 Requirements for ISAKMP Phase One, Message 2 6-15
 - 6.6.5 Requirements for ISAKMP Phase One, Message 3 6-15
 - 6.6.6 Requirements for ISAKMP Phase One, Message 4 6-15
 - 6.6.7 Requirements for ISAKMP Phase One, Message 5 6-16
 - 6.6.8 Requirements for ISAKMP Phase One, Message 6 6-16
 - 6.7 IPsec use of Digital Certificates 6-16
- 7. Implementation Requirements for SNMP Version 3 Using TLS Security Services 7-1
 - 7.1 Transactions Security Requirements 7-1
 - 7.2 Access Control Requirements 7-3
 - 7.3 Security Audit Requirements 7-3
 - 7.4 Security Alarm Requirements 7-3

- 8. Implementing SNMP Version 3 Using User-Based Security Model (USM) 8-1
 - 8.1 SNMPv3 USM Identification and Authentication Requirements 8-1
 - 8.2 USM Data Integrity Requirements 8-2
 - 8.3 USM Message Origin Authentication Requirements 8-2
 - 8.4 USM Data Confidentiality Requirements 8-2
 - 8.5 USM Message Replay Protection Requirements 8-2
 - 8.6 USM Access Control Requirements 8-2
 - 8.7 Security Audit Trail Requirements 8-3
 - 8.8 Security Alarm Requirements 8-3
- Appendix A: IPsec Overview A-1
 - A.1 Authentication Header (AH) A-2
 - A.2 Encapsulating Security Payload (ESP) A-3
 - A.3 Security Associations A-3
 - A.4 IPsec Implementation Considerations A-4
 - A.5 Identification Services A-6
 - A.6 Internet Key Exchange (IKE) A-6
- Appendix B: Transport Layer Security (TLS) Overview B-1
 - B.1 Establishing a TLS Session B-1
 - B.2 Selection of TLS Session Security Mechanisms B-2
 - B.3 TLS Initiation B-3
- Appendix C: Cryptographic Technologies C-1
 - C.1 Symmetric Encryption C-1
 - C.2 Hash Functions and Message Authenticators C-3
 - C.3 Public Keys for Digital Signatures and Key Exchange C-4
 - C.4 Digital Signatures Using Public Key Technology C-5
 - C.5 Certificates C-6
 - C.6 Tokens C-6
 - C.7 Cryptographic Protocols C-7
 - C.8 Guidelines for Digital Certificates C-8
 - C.8.1 Rationale for Digital Certificates C-8
 - C.8.2 X.509 Digital Certificates C-8
 - C.8.3 Certificate Revocation C-10
- Appendix D: Acronyms D-1
- Appendix E: References E-1
 - Reference Note E-4
 - To Contact Telcordia Customer Service E-4
 - To Order Documents From Outside Telcordia E-4
 - To Order Documents Within Telcordia E-4
- Requirement-Object Index ROI-1

List of Figures

Figure 2-1	General Relationship of a TMN to a Telecommunication Network (Source: ITU-T Recommendation M.3010)	2-3
Figure 2-2	Generic Manager/Agent Model	2-13
Figure 2-3	SNMPv3 Architecture	2-17
Figure A-1	AH Header Format	A-2