Security for OSI-Based TMN Interfaces

Contents

List of Figures xv

List of Tables xvii

Preface Preface–1
Bellcore's Interactive GR Process Preface–1
FA-TA-TR to GR Preface–1
Transition Phase Preface–1
Comments and Issues List Report Mechanism Preface–2
GR–1469 Current Maturity Level, Status and Plans Preface–2
Formatting Comments Preface–3
Where and When to Submit Comments Preface–4

1. Introduction 1–1
1.1 scope 1–1
1.2 Layered security architecture 1–3
1.3 Other security considerations 1-5
1.4 Requirements Terminology 1-6
1.5 Requirement Labeling Conventions 1-6
1.5.1 Numbering of Requirement and Related Objects 1-6
1.5.2 Requirement, Conditional Requirement, and Objective Object Identification 1–7

2. Background 2–1
2.1 Operational Environment 2-1
2.2 Communications Environment 2-3

3. Threats to TMN Interfaces 3-1
3.1 Threats to the Integrity and Confidentiality of Information 3-1
3.2 Unauthorized Access to Resources through the Interfaces 3-2
3.3 Repudiation 3-3

4. security Services 4-1
4.1 Security Semites and Security Mechanisms 4-2
4.2 Authentication Service 4-3
4.3 Access Control Service 4-3
4.4 Confidentiality Service 4–4
4.5 Data Integrity Service 4-5
4.6 Non-Repudiation Service 4-5
4.7 Other Security Concerns 4–6
4.7.1 OSI Security Management 4–6

4.7.2 Security Alarm *4-7*
4.7.3 Security Audit Log 4-7
4.8 Security Requirements of Specific Applications 4-8

5. Security Mechanisms 5-1
5.1 One-way Hashing *5-2*
5.2 Encryption *5-3*
5.2.1 Symmetric Encryption *5-3*
5.2.2 Asymmetric Encryption 5-3
5*3 Authentication Mechanisms 5-3
5.3.1 Association Request 5-4
5.3.1.1 Simple Authentication Seal 5-4
5.3.1.2 Strong Authentication Seal 5-5
5.3.1.3 Digital Signature 5-5
5.3.2 Association Response 5-6
5.3.3 Connectionless Authentication. 5-6
5.4 Integrity Mechanisms 5-6
5.5 Access Control Mechanisms 5-7
5.6 External Information 5-8
5.6.1 Security Paths 5-8
5.6.2 Directory Linking 5-9
5.7 Key Management and Distribution 5-9
5.7.1 X.500 Directory 5-10
5.72 Kerberos 5-10
5.7.3 Distribution of Security Information 5-10
5.7.3.1 Distribution of symmetric encryption keys 5-1 1
5.7.3.2 Distribution of public key certificates 5-12
5.8 Authentication Server 5-12

6. OSI Security Work 6-1
6.1 OSI Security Architecture 6-1
6.2 Upper Layers Security 6-2
6.2.1 Upper Layers Security Model 6-2
6.2.2 Infrastructure/Support *Security* *6-2*
6.2.2.1 Association Control Service Element 6-2
6.2.2.2 Generic Upper Layer Security 6-3
6.2.3 Application-Specific Security 6-4
6.2.3.1 Common Management Information Semite Element 64
6.2.3.2 File Transfer, Access, and Management 6-5
6.2.3.3 X.500 Directory 6-5
6.3 Lower Layer Security Services 6-6
6.3.1 Link Layer Security Services 6-6
6.3.2 Network Layer Security Services 6-7
6.3.3 Transport Layer Security Services 6-8

7. Security Requirements for the OSI-Based TMN Interfaces 7-1

7.1 Baseline Requirements 7-1
7.2 Requirements for Encryption 7–2
7.2.1 Requirements for DES 7–2
7.2.2 Requirements for PKCS 7-3
7.3 Requirements for Identification 7-4
7.4 Requirements for Authentication 7-5
7.5 Requirements for Data Integrity 7-7
7.6 Requirements for Access Control 7-8
7.7 Confidentiality 7-10
7.8 Non-Repudiation 7-11
7.8.1 Non-Repudiation of Origin 7–1 1
7.8.2 Non-Repudiation of Delivery 7–1 1
7.9 Key Distribution 7–12
7.10 General Security Mechanisms 7-13
7.11 security Alarm 7–13
7.12 Security Audit 7-13

Appendix A: Requirement-Object List A–1

Appendix B: Encoding of Authentication and Digital Signature Information B–1

Appendix C: Interoperability C-1

References References-1

Glossary Glossary-1

Requirement-Object Index Index-1

List of Figures

Figure 2-1. TMN Physical Architecture 2-1
Figure 2-2. Communication Environment of GR-828-CORE 2-5
Figure 6-1. Location of TLSP in the OSI Model 6-8

List of Tables

Table 1-1. Security Features of ISO Standards 1-4
Table 4-1. Security Services vs. Security Threats 4-1
Table 4-2. Severity of Threats to TMN Applications 4-8
Table 5-1. Security Services vs. Security Mechanisms 5-1
Table 5-2. Digital Signature Algorithms 5-5