Contents

List of Figures ix
Preface xi
The Telcordia Technologies GR Process xi
About GR-1253-CORE xi
To Submit Comments xii
1. Introduction 1–1
1.1 Purpose and Scope 1–3
1.2 Target Audience 1–5
1.3 Structure and Use of This Document 1–6
1.4 Requirements Terminology 1–7
1.5 Requirement Labeling Conventions 1–8
1.5.1 Numbering of Requirement and Related Objects 1–8
1.5.2 Requirement, Conditional Requirement, and Objective Object Identification 1–8
2. Background 2–1
2.1 Operational Environment 2–2
2.2 Communications Environment 2–5
3. Security Administration Functions 3–1
3.1 Login Management 3–2
3.2 Notification Management 3–3
3.3 Access Control Management 3–4
3.4 Management of Encryption Keys 3–5
4. Information Model 4–1
4.1 Login Management 4–2
4.1.1 Pre and Post Login Messages 4–2
4.1.2 User Management 4–2
4.1.3 Password Management 4–3
4.1.4 Channel Management 4–3
4.1.5 Security MOs management 4–3
4.2 Notification Management 4–5
4.3 Access Control 4–9
4.3.1 Targets 4–9
4.3.2 Rules 4–10
4.3.3 Initiators 4–10
4.3.3.1 Access Control Lists 4–10
4.3.3.2 Capabilities 4–10
4.3.3.3 Security Labels 4–10
4.3.4 Authentication for Access Control 4–11
4.3.5 MOs for Access Control 4–12
4.4 Key Management 4–17
5. Definition of Management Information 5–1
5.1 Login management 5–2

5.1.1 Login management object classes 5–2
5.1.1.1 Security channel 5–2
5.1.1.2 Security system 5–3
5.1.1.3 Security system initial values 5–4
5.1.1.4 Security user 5–5
5.1.1.5 System password authentication 5–7
5.1.1.6 User password authentication 5–8
5.1.1.7 User session 5–9
5.1.2 Name Bindings 5–11
5.1.2.1 Security channel – security system 5–11
5.1.2.2 Security system initial values – security system 5–11
5.1.2.3 security user – security system 5–12
5.1.2.4 System password authentication – security system 5–12
5.1.2.5 User password authentication – security user 5–13
5.1.2.6 User session – security user 5–14
5.1.3 Login management attributes 5–15
5.1.3.1 Channel ID 5–15
5.1.3.2 Channel lockout period 5–15
5.1.3.3 Idle time out period 5–16
5.1.3.4 Last login location ID 5–16
5.1.3.5 Last login time 5–16
5.1.3.6 Last logout time 5–17
5.1.3.7 Last password change 5–17
5.1.3.8 Last password changed by 5–18
5.1.3.9 Last user ID disabled 5–18
5.1.3.10 Non used period 5–18
5.1.3.11 Number last unsuccessful login 5–19
5.1.3.12 Password aging interval 5–19
5.1.3.13 Password complexity algorithm 5–20
5.1.3.14 Password expiration notification 5–20
5.1.3.15 Password reuse number 5–21
5.1.3.16 Password reuse period 5–21
5.1.3.17 Post login message 5–22
5.1.3.18 Pre login message 5–22
5.1.3.19 Privilege level 5–23
5.1.3.20 Process ID list 5–23
5.1.3.21 Security event list 5–23
5.1.3.22 Security system ID 5–24
5.1.3.23 Security system initial values ID 5–24
5.1.3.24 Session idle time 5–24
5.1.3.25 Session location ID 5–25
5.1.3.26 Session start time 5–25
5.1.3.27 System Password Authentication ID 5–26
5.1.3.28 Unsuccess login attempt 5–26
5.1.3.29 User ID 5–26
5.1.3.30 User ID status 5–27
5.1.3.31 User password 5–27

5.1.3.32 User password authentication ID . . . 5–28
5.1.3.33 User session ID . . . 5–28
5.1.4 Login management parameters . . . 5–28
5.1.4.1 Delete error parameter . . . 5–28
5.1.4.2 Specific error parameter . . . 5–29
5.1.5 Login management actions . . . 5–30
5.1.5.1 User login request . . . 5–30
5.1.5.2 User logout request . . . 5–31
5.1.6 Login management notifications . . . 5–31
5.1.6.1 Session idle time out . . . 5–31
5.1.7 Login management packages . . . 5–31
5.1.7.1 System access control . . . 5–31
5.1.7.2 Password complexity algorithm . . . 5–32
5.1.7.3 Password expiration notification . . . 5–32
5.1.8 Login management supporting productions . . . 5–33
5.2 Key management . . . 5–41
5.2.1 Key management object classes . . . 5–41
5.2.1.1 Key list . . . 5–41
5.2.2 Key management attributes . . . 5–44
5.2.2.1 List ID . . . 5–44
5.2.2.2 List size . . . 5–44
5.2.2.3 Other users . . . 5–44
5.2.2.4 List of keys . . . 5–44
5.2.2.5 Key status . . . 5–45
5.2.2.6 List creation date . . . 5–45
5.2.2.7 List validity period . . . 5–45
5.2.2.8 List creator . . . 5–46
5.2.2.9 List encryption method . . . 5–46
5.2.2.10 Encryption keys . . . 5–46
5.2.3 Key management supporting productions . . . 5–47
6. Summary . . . 6–1
Appendix A: References . . . A–1
NOTE . . . A–5
Appendix B: Acronyms . . . B–1
Requirement-Object Index . . . ROI–1

List of Figures

Figure 1-1 Example of Security Manager and Managed Systems 1–1
Figure 2-1 Example of a TMN Physical Architecture 2–2
Figure 2-2 Communication Environment of GR-828-CORE 2–7
Figure 4-1 Possible Name Bindings for Login Management MOs 4–2
Figure 4-2 Inheritance of Notification Management MO Classes 4–5
Figure 4-3 Possible Name Binding for Notification Management MOs 4–6
Figure 4-4 Notification Management Interactions 4–7
Figure 4-5 Access Control MO Class Inheritance Hierarchy 4–13
Figure 4-6 Relationship of Access Control MOs 4–14