

Contents

1 Introduction

1.1	Purpose and Scope of This GR	1-1
1.1.1	Reasons for GR-3103-CORE, Issue 4	1-1
1.1.2	Reasons for GR-3103-CORE, Issue 3	1-2
1.1.3	Reasons for GR-3103-CORE, Issue 2	1-2
1.2	Document Organization	1-4
1.3	Relationship to Other Documents	1-4
1.4	Requirements Terminology	1-5
1.4.1	Terminology	1-5
1.4.2	Numbering of Requirement and Related Objects	1-5
1.4.3	Requirement, Conditional Requirement, and Objective Identification. . .	1-6

2 Background

2.1	General Assumptions	2-2
2.2	Specific Terminology	2-2
2.3	Next Steps	2-3

3 LIDB LDAP Gateway Security Interface (GSI)

3.1	Terminology	3-1
3.2	Security Assumptions	3-4
3.3	LIDB LDAP GSI Objectives	3-5
3.4	What the GSI Does.	3-6
3.5	What the GSI Does “Not” Do	3-6
3.6	GSI Overview.	3-6
3.7	Primary GSI Concepts.	3-7
3.8	Network Architecture	3-8
3.9	LIDB Owner’s Network	3-9
3.9.1	LIDB Owner’s Network Setup Requirements.	3-9
3.10	Security Infrastructure Components.	3-16
3.10.1	LIDB LDAP Security Interface Component Requirements	3-16
3.10.2	Authorized Client Table (ACT)	3-16
3.10.3	ACT Contents	3-17
3.10.3.1	Anticipated ACT Fields	3-19
3.10.4	LIDB LDAP Interface Registration Requirements	3-20
3.10.4.1	Client ID	3-24
3.11	LIDB Client’s Network	3-27
3.11.1	LIDB Client’s Network Setup Requirements	3-27
3.11.2	Non-Repudiation Requirements	3-29
3.12	Connection Establishment and Authentication Processes.	3-32
3.12.1	Client Authentication and Session Setup Using SSLv3	3-32
3.12.1.1	Server Certificate Authentication Process	3-35
3.12.1.2	Setting Up an Encrypted Communications Channel Using SSLv3	3-37

- 3.12.2 Authenticating the Connection Requester’s Access Control Rights 3-41
- 3.12.3 Testing the LIDB Client’s Certificate Validity 3-41
 - 3.12.3.1 Certificate Structure 3-44
- 3.12.4 Connection Request Access Control Process 3-44
- 3.12.5 Authenticating the Connection Requester 3-45
- 3.13 Message Authentication Process 3-47
 - 3.13.1 Message Protection and Authentication Requirements. 3-47
 - 3.13.2 Message Confidentiality 3-48
 - 3.13.3 Message Origin and Data Integrity Authentication 3-49
 - 3.13.3.1 Non-Repudiation Concerns 3-50
 - 3.13.4 Operations Request Access Control 3-51
 - 3.13.4.1 Single Entity Access Control. 3-55
 - 3.13.4.2 Multiple Entity Access Control 3-57
- 3.14 Interconnection Agreements (IAs) 3-58
 - 3.14.1 LIDB LDAP Interconnection Agreement Requirements 3-59
- 3.15 Gateway Screening Overview and Requirements 3-59
 - 3.15.1 LIDB Gateway Screening History 3-60
 - 3.15.2 Gateway Screening Process 3-60
 - 3.15.3 Destination Address Authentication Function Requirements 3-62
 - 3.15.4 Source Address Authentication Function Requirements 3-63
- 3.16 Security Services for LIDB LDAP Applications 3-65
 - 3.16.1 Intent of LIDB LDAP Security Services. 3-65
 - 3.16.2 Flexibility of Security Services and Requirements 3-65
- 3.17 Establishing a Secure Connection Between “Proxy” and Actual LIDB LDAP Servers 3-66
- 3.18 Non-Repudiation 3-67
 - 3.18.1 Non-Repudiation of Message Origin 3-69
 - 3.18.1.1 Whole Message Hashing 3-69
 - 3.18.2 Non-Repudiation of Message Delivery 3-70
- 3.19 Guidelines for a PKI. 3-71
 - 3.19.1 Trust Model 3-72
 - 3.19.2 Cryptographic Aspects. 3-73
- 3.20 Guidelines for Certificate Authority (CA). 3-73
 - 3.20.1 Certification Practice Statement (CPS) 3-73
 - 3.20.2 User Management 3-74
 - 3.20.3 Confirmation of Proof of Rights. 3-75
 - 3.20.4 CA Configuration, Backup, and Recovery 3-75
 - 3.20.5 CA Operations 3-75
 - 3.20.6 Protecting the CA’s Signing Key. 3-76
 - 3.20.7 Recommendations for LIDB LDAP Certificate Authority. 3-77
- 3.21 Guidelines for Digital Certificates 3-77
 - 3.21.1 Rationale for Digital Certificates 3-78
 - 3.21.2 Structure of LIDB LDAP Digital Certificates. 3-78
 - 3.21.3 Certificate Revocation 3-80
 - 3.21.3.1 LIDB LDAP Interface CRL Process 3-80
- 3.22 Guidelines for Key Management. 3-81
 - 3.22.1 Protecting Private Keys 3-82

- 3.22.2 Recovery of Keys and Stored Data 3-82
- 3.23 Guidelines for Secure System and Network Management. 3-83
- 3.24 Network Element/Network System (NE/NS) Threats 3-83
 - 3.24.1 Internet Security Concerns. 3-85
 - 3.24.2 Attacks on Systems and Networks Attached to the Internet 3-86
 - 3.24.3 Attacks on the Internet and Its Protocols. 3-88
 - 3.24.4 Insider Concern 3-88
- 3.25 Guidelines for Firewalls. 3-89
- 3.26 SSL Overview. 3-90
 - 3.26.1 Establishing an SSL Session 3-91
 - 3.26.2 Selection of SSL Session Security Mechanisms 3-91
 - 3.26.3 Client SSL Initiation. 3-92
- 3.27 Follow-On Work: Next Steps 3-93

4 LDAP Interface Directory and Data Schema

- 4.1 LDAP Directory Overview 4-1
 - 4.1.1 LDAP Directory Elements 4-1
 - 4.1.2 LDAP Directory Model 4-3
 - 4.1.2.1 Defining an LDAP Interface Information Tree for LIDB. 4-4
 - 4.1.2.2 Defining an LDAP DIT Entry 4-5
 - 4.1.2.3 LDAP Object Classes 4-6
 - 4.1.2.4 Attribute Types 4-7
 - 4.1.2.5 Attribute Values 4-8
- 4.2 LDAP Schema Overview 4-8
- 4.3 LIDB LDAP Interface Requirements 4-9
 - 4.3.1 Creating an LDAP Interface Directory Tree 4-10
- 4.4 LDAP Interface Schema Requirements 4-12
- 4.5 Defining a LDAP Interface Directory Namespace 4-13
 - 4.5.1 Designing the LDAP Directory Namespace. 4-13
 - 4.5.1.1 Choosing an LDAP Directory Suffix. 4-13
 - 4.5.1.2 Namespace Considerations. 4-14
- 4.6 LDAP Interface Support for Multiple Data Owners (DOs). 4-14

5 LIDB LDAP Interface Authentication and Interrogation Operations

- 5.1 Introduction 5-1
 - 5.1.1 LIDB LDAP Interface Architecture 5-2
 - 5.1.2 Protocols. 5-3
 - 5.1.3 LDAP Messaging 5-3
 - 5.1.3.1 LDAPMessage Envelope 5-3
- 5.2 Overview of LDAP Authentication and Interrogation Operations. 5-5
 - 5.2.1 Client/Server Interaction 5-5
 - 5.2.2 Bind Request and Response 5-6
 - 5.2.3 Unbind Operation 5-9
 - 5.2.4 Abandon Operation 5-9
 - 5.2.5 Search Operations 5-10
 - 5.2.5.1 LDAP SearchRequest 5-10

- 5.2.5.2 SearchRequest Filters 5-16
- 5.2.5.3 Compound and Complex Search Filters 5-17
- 5.2.6 LDAPResult/Response Message. 5-18
- 6 LDAP Interface Update Operations**
- 6.1 LDAP Update Operation Overview 6-1
 - 6.1.1 Add, Delete, and Rename Operations 6-2
 - 6.1.2 Modify Operation. 6-2
 - 6.1.3 LDAP Interface Non-Standard Update (NSU) 6-4
- 6.2 LDAP Interface Update Requirements 6-4
 - 6.2.1 LDAP Interface Modify Request Requirements 6-5
 - 6.2.2 Updates in Redundant Platforms 6-8
 - 6.2.2.1 Text Error Messages 6-9
 - 6.2.3 Update Logs. 6-9
 - 6.2.4 LDAP NSU Requirements 6-9
- 6.3 Indicate LDAP Update (REPT-ILU) 6-10
- 6.4 AS Support for the LDAP Interface 6-32
- 7 LDAP CompareRequest**
- 7.1 Compare Request 7-1
 - 7.1.1 Entry. 7-1
 - 7.1.2 Attribute Value Assertion 7-1
 - 7.1.2.1 Matching Rules 7-2
- 7.2 Compare Response 7-2
- 7.3 Verification Applications 7-3
- 8 Measurements**
- 8.1 LDAP Operations Measurements 8-1
 - 8.1.1 Data Types 8-2
 - 8.1.1.1 Generated Data 8-2
 - 8.1.1.2 Parametric Data. 8-4
- 8.2 Data Presentation 8-5
 - 8.2.1 Data Generation 8-5
 - 8.2.2 Data Retention (on-occurrence, polled, logs, etc.) 8-7
 - 8.2.3 Data Distribution 8-9
 - 8.2.4 Measurement Report Structure 8-10
- 8.3 Generated and Parametric Measurement Collection 8-11
- 8.4 Message Detail Recording 8-11
 - 8.4.1 Successful Operations 8-12
 - 8.4.2 Failed Operations. 8-13
 - 8.4.2.1 LDAP Bind Problem 8-14
 - 8.4.2.2 Search Errors 8-14
 - 8.4.2.3 Attribute Problem. 8-15
 - 8.4.2.4 Name Problem 8-16
 - 8.4.2.5 Security Problem 8-16
 - 8.4.2.6 Service Problem. 8-17

- 8.4.2.7 Update Problem 8–18
- 8.4.2.8 Other Problem 8–18
- 8.4.2.9 Abandons. 8–18
- 8.5 Performance Management Measurements 8–18
 - 8.5.1 Processor Performance Data 8–18
 - 8.5.2 LIDB LDAP Interface 8–20

9 Performance

- 9.1 Reliability 9–1
- 9.2 Availability 9–4
- 9.3 Throughput and Scalability 9–4
- 9.4 Response Time by the Interface 9–5
- 9.5 Application Level Timers 9–7
- 9.6 Overload Protection 9–7
 - 9.6.1 LDAP Server Overload or Congestion Measurements. 9–8

10 Usage Measurements

- 10.1 General 10–1
- 10.2 Detailed AMA Recording 10–3
 - 10.2.1 Basic Detailed AMA. 10–3
 - 10.2.2 Additional Detailed Element-Specific AMA 10–9
- 10.3 Aggregate AMA Recording 10–16
 - 10.3.1 Basic Aggregate AMA. 10–16
 - 10.3.2 Additional Aggregate Element-Specific AMA. 10–23

Appendix A: LIDB/LDAP Interface Data Catalog Abbreviations

- A.1 Introduction A–1
- A.2 LIDB Line Record Data Elements Abbreviations A–1
- A.3 LIDB Line Record Data Elements Restricted to Compare Operation. A–4

Appendix B: LIDB LDAP Interface Error Codes

- B.1 Introduction B–1
- B.2 LIDB LDAP Interface Error Code Definitions. B–1

Appendix C: References

Appendix D: Glossary

Requirement-Object Index

List of Figures

Figure 3-1	Data Requester/Service Broker/Proxy Architecture	3-3
Figure 3-2	GSI Architecture	3-7
Figure 3-3	LIDB LDAP Security Architecture	3-9
Figure 3-4	Connection Request Access Control	3-46
Figure 3-5	Operation Request Access Control	3-52
Figure 4-1	LDAP Directory Information Tree (DIT)	4-3
Figure 4-2	Sample LIDB Tree	4-4
Figure 5-1	Illustration of the LDAP Categories and Supported Operations . . .	5-1
Figure 5-2	Typical Session Between the Client and a Server	5-6
Figure 6-1	Supported Functionality	6-1
Figure 9-1	Sample Architecture With Points of Congestion	9-2
Figure 9-2	Another Sample Architecture With Points of Congestion	9-3
Figure 9-3	Response Time	9-6

List of Tables

Table 6-1	REPT-ILU Message Format	6-12
Table 6-2	REPT-ILU Message Parameters	6-15
Table 8-1	Traffic Data Schedules	8-2
Table 9-1	Examples of Objective Criteria to Measure in Laboratory Testing Environment (Beta Trial)	9-5
Table 10-1	BAF Data Structures for LDAP AMA	10-3
Table 10-2	Population of LIDB Processing Result (BAF Table 452) for LDAP SearchRequest	10-6
Table 10-3	Population of LIDB Processing Result (BAF Table 452) for LDAP ModifyRequest	10-7
Table A-1	LIDB Data Elements	A-1
Table B-1	LIDB LDAP Interface Error Code Definitions	B-1