



A11103 928980

NIST
PUBLICATIONS

NISTIR 4983

A Study of OSI Key Management

Roberto Zamparo

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems Laboratory
Computer Security Division
Gaithersburg, MD 20899

QC
100
.U56
4983
1992

NIST

A Study of OSI Key Management

Roberto Zamparo

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems Laboratory
Computer Security Division
Gaithersburg, MD 20899

November 1992



U.S. DEPARTMENT OF COMMERCE
Barbara Hackman Franklin, Secretary

TECHNOLOGY ADMINISTRATION
Robert M. White, Under Secretary for Technology

**NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY**
John W. Lyons, Director

TABLE OF CONTENTS

PREFACE	XI
ACKNOWLEDGMENTS	XIII
1 INTRODUCTION	1
1.1 BACKGROUND	1
1.2 PLACE OF KEY MANAGEMENT IN THE OSI ARCHITECTURE	3
1.3 KEY MANAGEMENT ACTIVITIES	3
1.3.1 Secure Data Network System (SDNS)	4
1.3.2 ANSI X9.17	4
1.3.3 ANSI X9.28	4
1.3.4 ISO/CD 11166	4
1.3.5 Standards for Interoperable LAN Security (SILS)	5
1.3.6 ISO SC 27	5
1.3.7 Network Layer Security Protocol (NLSP)	5
2 CRITERIA FOR OSI KEY MANAGEMENT	7
2.1 GENERAL CRITERIA FOR OSI KEY MANAGEMENT	7
2.1.1 Algorithm independence	7
2.1.2 Operations across security domains	7
2.1.3 Support of a variety of security protocols	7
2.1.4 Support across a range of networking environments	8
2.2 GENERAL REQUIREMENTS	8
3 KEY MANAGEMENT MODEL	9
3.1 TOP LEVEL VIEW	9
3.2 DECOMPOSITION OF THE KEY MANAGEMENT SERVICE	9
3.3 DECOMPOSITION OF THE KEY CENTER	10
4 PHASES IN TRAFFIC ENCRYPTION KEY MANAGEMENT	13
5 ISSUES IN KEY MANAGEMENT	15
5.1 HOLDER OF THE CERTIFICATE	15
5.2 ORGANIZATION OF THE CERTIFICATION AUTHORITIES	16
5.2.1 Organization of certification authorities in SDNS	16
5.2.2 Organization of certification authorities in the Directory standards	16
5.2.3 Organization of certification authorities in RFC 1114	21
5.2.4 Section summary	29
5.3 ORGANIZATION OF KEY DISTRIBUTION AND KEY TRANSLATION CENTERS	29
5.3.1 Organization of Key Distribution and Key Translation Centers in X9.17	30
5.3.2 Organization of Key Distribution and Key Translation Centers in X9.28	34
5.3.2.1 X9.28 key exchange transaction	37
5.3.2.2 Diversion from the key management model	39
5.3.3 Section summary	40
5.4 PASSIVE OR ACTIVE CERTIFICATION AUTHORITY	40
5.5 GENERATION OF THE PRIVATE AND PUBLIC KEY PAIR	41
5.5.1 Generation of public key pair in SDNS	41
5.5.2 Generation of public key pair in ISO/CD 11166	41
5.5.3 Generation of public key pair in the Directory standards	42
5.5.4 Generation of public key pair in RFC 1114	42

TABLE OF CONTENTS (continued)

5.6 REKEY HANDLING	42
5.6.1 Rekey handling in an asymmetric form of key management.....	42
5.6.1.1 Rekey handling in SDNS.....	48
5.6.1.2 Rekey handling in the Directory standards.....	49
5.6.1.2.1 Rekeying as part of the Directory standards	50
5.6.1.2.2 Rekeying performed outside the Directory	52
5.6.1.3 Rekey handling in ISO/CD 11166	53
5.6.1.4 Section summary.....	54
5.6.2 Rekey handling in a symmetric form of key management.....	54
5.6.2.1 Rekey handling in X9.17	54
5.6.2.2 Rekey handling in X9.28	55
5.7 REVOCATION LIST HANDLING	55
5.7.1 Revocation list handling in SDNS.....	56
5.7.2 Revocation list handling in the Directory standards	56
5.7.3 Revocation list handling in RFC 1114.....	57
5.7.4 Revocation list handling in ISO/CD 11166.....	58
5.7.5 Section summary	58
5.8 CONVERSION PROBLEMS	59
5.9 PROTECTION OF GROUP AND BROADCAST KEYS	59
5.10 ALGORITHM INDEPENDENCE	61
5.10.1 Algorithm independence by using Object Identifiers.....	61
5.10.2 Algorithm independence by altering presentation context.....	62
5.10.3 Algorithm independence in SDNS.....	64
5.10.4 Section summary.....	64
5.11 ASN.1 ABSTRACT VERSUS TRANSFER SYNTAX PROBLEMS.....	64
5.12 TRIGGERING OF KEY MANAGER.....	65
5.13 ESTABLISHMENT OF SECURITY SERVICES	68
5.14 KEY MANAGEMENT AS PART OF THE SECURITY PROTOCOL.....	73
5.15 KEY MANAGEMENT AS PART OF A LAYER PROTOCOL.....	77
5.16 ADDING A NEW COMPONENT TO THE NETWORK.....	78
5.16.1 Adding a new component in SDNS	78
5.16.2 Public key registration.....	78
5.17 COMMON KEY MANAGEMENT PROTOCOL	80
5.18 THE CONCEPT OF SECURITY ASSOCIATION	80
5.19 SUBSTITUTION OF TRAFFIC ENCRYPTION KEYS	83
5.20 KNOWN PLAIN TEXT ATTACK.....	85
5.21 ADDRESSING PROBLEMS	86
5.21.1 Addressing problems in SDNS	86
5.21.2 Addressing problems in SILS.....	88
5.21.3 Can key management entities be trusted?.....	91
5.22 ASPECTS OF KEY MANAGEMENT OUTSIDE OSI.....	92
5.22.1 Key Archiving	92
5.22.2 Key Generation	92
5.22.3 Key Destruction	92
5.22.4 Key Storage.....	93
5.22.5 Compromised Key Recovery.....	93
6 REALIZATION OF THE MODEL	95
7 GENERALITY OF THE KEY MANAGEMENT MODEL	99
7.1 IMPROVEMENTS OF THE MODEL.....	99
8 LEVEL OF CENTRALIZATION.....	101

TABLE OF CONTENTS (continued)

9 KEY MANAGEMENT PROTOCOL SPECIFICATIONS	103
9.1 TYPES OF PROTOCOLS.....	103
9.2 ASN.1 MODULE DISPOSITION.....	104
9.3 SECURITY REGISTER.....	105
9.3.1 Registration of key exchange algorithms/methods.....	106
9.3.1.1 Approach one.....	108
9.3.1.2 Approach two	110
9.3.2 Registration of rekeying methods	112
9.4 PROTOCOL OVERVIEW	115
9.5 INTEGRITY PROCEDURE.....	117
9.6 ENCRYPTION PROCEDURE	118
9.7 KEY EXCHANGE.....	118
9.8 KMSA TO KMSA PROTOCOL.....	120
9.8.1 Algorithm choice	120
9.8.1.1 A priori agreements.....	121
9.8.1.2 Need to initialize cryptographic variables.....	122
9.8.1.3 Algorithm negotiation.....	123
9.8.2 Update of traffic encryption keys	125
9.8.3 Support of different kinds of security protocols	125
9.8.4 Security association identification.....	127
9.8.5 Separation of confidentiality and integrity keys	127
9.9 KMSA TO KCA PROTOCOL.....	127
9.9.1 Algorithm choice	128
9.9.2 Rekeying.....	128
9.10 KCA TO KCA PROTOCOL.....	129
9.11 SECURITY PROTOCOL DEFINITIONS	129
9.11.1 TLSP definitions.....	130
9.12 ERROR HANDLING	131
9.13 BROADCAST AND GROUP KEYS.....	131
9.14 FINDING THE REMOTE ADDRESS DYNAMICALLY.....	131
9.15 TIMERS	131
9.16 POSSIBILITY TO ENHANCE SECURITY.....	131
9.17 GENERALITY OF THE KEY MANAGEMENT PROTOCOL	132
10 COMPARISONS APPLICATION LAYER VERSUS SECURITY PROTOCOL LAYER..	135
10.1 APPLICATION LAYER ADVANTAGES.....	135
10.2 SECURITY PROTOCOL ADVANTAGES	135
11 AREAS NOT COVERED	137
11.1 SYMMETRIC FORM OF KEY MANAGEMENT	137
11.2 REKEY HANDLING.....	137
11.3 DISTRIBUTED ASPECTS.....	137
11.4 ACCESS CONTROL.....	137
11.5 ORANGE BOOK ASPECTS	138
11.6 ZERO KNOWLEDGE TECHNIQUES.....	138
11.7 SECURITY MANAGEMENT.....	138
11.8 KERBEROS	138
ANNEX A KEY MANAGEMENT APPROACHES.....	139
A1 SYMMETRIC FORM OF KEY MANAGEMENT	139
A2 ASYMMETRIC FORM OF KEY MANAGEMENT	144
A3 COMPARISONS.....	147

TABLE OF CONTENTS (continued)

ANNEX B PROTOCOL AND SERVICE DEFINITIONS	149
B1 PROTOCOL DEFINITIONS	149
B1.1 SECURITY DEFINITIONS MODULE.....	149
B1.2 SECURITY REGISTER MODULES.....	151
B1.2.1 Confidentiality Algorithms.....	152
B1.2.1.1 Symmetric algorithms.....	153
B1.2.1.2 Asymmetric algorithms.....	154
B1.2.2 Key Exchange Methods.....	155
B1.2.3 Integrity Mechanisms.....	159
B1.2.4 Security Levels.....	160
B1.2.5 Security Labels.....	161
B1.2.6 Signature Algorithms.....	162
B1.2.7 Rekeying Methods.....	163
B1.3 KEY MANAGEMENT PROTOCOL MODULES.....	165
B1.3.1 KMSA TO KMSA.....	167
B1.3.1.1 ASN.1 declarations.....	167
B1.3.1.2 Protocol Machine.....	170
B1.3.2 KMSA TO KCA.....	172
B1.3.2.1 ASN.1 definitions.....	172
B1.3.2.2 Protocol Machine.....	175
B1.3.3 KCA TO KCA.....	177
B1.4 MAPPING OF PDUs.....	178
B1.4.1 KMSA TO KMSA.....	178
B1.4.2 KMSA TO KCA.....	179
B1.4.3 KCA TO KCA.....	181
B1.5 SECURITY PROTOCOL MODULE.....	182
B1.5.1 TLSP.....	182
B1.5.2 NLSP.....	183
B1.5.3 SDE.....	184
B2 SERVICE SPECIFICATIONS	185
B2.1 KMSA TO KMSA SERVICE SPECIFICATION.....	185
B2.1.1 Available service primitives.....	185
B2.1.1.1 Key Management Initialization service primitive.....	185
B2.1.1.2 New Key service primitive.....	187
B2.1.1.3 Security Service service primitive.....	188
B2.1.1.4 Key Update service primitive.....	189
B2.1.1.5 KM-Release service primitive.....	189
B2.1.1.6 KM-Abort service primitive.....	189
B2.1.2 Security protocol parameters.....	190
B2.1.2.1 TLSP parameters.....	190
B2.2 KMSA TO KCA service primitives.....	192
B2.2.1 Available service primitives.....	192
B2.2.1.1 Key Management Initialization service primitive.....	192
B2.2.1.2 New Key service primitive.....	192
B2.2.1.3 Rekey service primitive.....	192
B2.2.1.4 Rekey Delivery service primitive.....	193
B2.2.1.5 KM-Release service primitive.....	193
B2.2.1.6 KM-Abort service primitive.....	193
B2.3 KCA TO KCA service primitives.....	194

TABLE OF CONTENTS (continued)

B2.4 GENERIC AND ALGORITHM DEPENDENT PARAMETERS.....195

 B2.4.1 Key Exchange Methods195

 B2.4.1.1 Diffie-Hellman195

 B2.4.1.2 RSA196

 B2.4.2 Rekey Methods.....197

 B2.4.2.1 rekMeth1197

 B2.4.3 Diagnostics.....197

B2.5 ALTERNATIVE SERVICE SPECIFICATION199

ANNEX C SUGGESTED READING.....201

ANNEX D ASN.1 EXTENSIONS203

GLOSSARY205

 OSI TERMS AND ABBREVIATIONS205

 SECURITY GLOSSARY.....207

 ANSI X9 SECURITY TERMS AND ABBREVIATIONS209

REFERENCES213

