APPENDIX A

STRAWMAN EXTENDED GSS API

(This appendix will be supplied in the next draft.)

APPENDIX B

DETAILED EXAMPLE OF SECURITY ASSOCIATION ESTABLISHMENT

(This appendix will be supplied in the next draft.)

REFERENCES

American National Standards Institute (ANSI), 1985, *Financial Institution Key Management (Wholesale)*, X9.17

Abrams, Marshall D. and Michael V. Joyce, January 1993, *On TCB Subsets and Trusted Object Management*, MITRE Technical Report 92W0000248, McLean, VA

Center for Information Management (CIM), 1992, *Technical Architecture Framework for Information Management*, Defense Information Systems Agency, Washington, DC

Case, Jeff, Mark Fedor, Martin Schoffstall and James Davin, 1989, *Simple Network Management Protocol (SNMP)*, Internet Request for Comments 1098

Case, Jeff, 1991, *SNMP Version 2*, Internet Request for Comments 1441

International Telegraph and Telephone Consultative Committee (CCITT), 1988, *Recommendations X.400-X.420: Data Communications Networks, Message Handling Systems*

_____, 1992, *Recommendations X.500-X.521 Data Communications Networks, Directory*

Department of Defense, 1985, *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Washington, DC

Institute of Electrical and Electronic Engineers (IEEE), *Standard for Interoperable LAN/MAN Security, Part 2--Secure Data Exchange Protocol Specification*, IEEE 802.10b

_____, 1993, *Standard for Interoperable LAN/MAN Security, Part 3-Key Management Protocol Specification (Draft)*, IEEE 802.10c

International Organization for Standardization (ISO), 1984, Information Processing Systems, *Open Systems Interconnection Reference Model: Basic Reference Model*, ISO 7498

_____, 1987, Information Processing Systems, *Common Management Information Protocol*, ISO 9596

_____, 1988a, Information Processing Systems, *Open Systems Interconnection - Connectionless Network Protocol*, ISO 8473

_____, 1988b, Information Processing Systems, *FTAM - File Transfer, Access, and Management*, ISO 8571-1

_____, 1988c, Information Processing Systems, *ACSE - Association Control Service Element*, IS 8649/8650

_____, 1988d, Information Processing Systems, *Abstract Syntax Notation Number 1 (ASN.1)*, ISO 8824

_____, 1989a, Information Processing Systems, *Open Systems Interconnection Reference Model, Part 2: Security Architecture*, ISO 7498-2

_____, 1989b, Information Processing Systems, *Open Systems Interconnection Reference Model, Part 4: Management Framework*, ISO 7498-4

_____, 29 July 1992a, Information Technology, Network Layer Security Protocol, ISO DIS 11577

_____, 7 December 1992b, Information Technology, Transport Layer Security Protocol, ISO 10736

_____, 1992c, Information Technology - *Open Systems Interconnection - Security Frameworks in Open Systems - Part 3: Access Control*, ISO CD 10181-3

_____, 1993a, Information Technology - *Open Systems Interconnection - Security Frameworks in Open Systems - Part 1: Overview*, ISO CD 10181-1

_____, 1993b, Information Technology - *General Upper Layers Security (GULS) - Part 3: Security Exchange Service Element Protocol (SESEP) Specification*, ISO DIS 11586-3

Linn, John, 1992, *General Security Services - Application Program Interface*, Draft Internet Request for Comments

National Institute of Standards and Technology (NIST), 1992a, *U.S.*

Government OSI Profile, United States Federal Information Processing Publication 146-2

_____, 1992b, *Government Network Management Profile*
National Security Agency (NSA), 1992, *Message Security Protocol*, SDN.701 Revision 2.0

_____,22 February 1993, *Department of Defense Information Systems Security Policy*, DISSP-SP.1

Powell, General Colin L., 1992, as quoted in *C4I for the Warrior*, Joint Staff (J6)

Rivest, R. L., A. Shamir and L. Adelman, 1978, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM, Volume 21, Number 2, pp. 120-126

Rushby, J., September, 1984, "A Trusted Computing Base for Embedded Systems", Proceedings of the 7th DOD/NBS Computer Security Symposium, pp. 294-311

LIST OF ACRONYMS

ACCS	Army Command and Control System
ACSE	Association Control Service Element
ADF	Access Control Decision Function
AEF	Access Control Enforcement Function
API	Application Program Interface
ASSR	Agreed Set of Security Rules
ATM	Asynchronous Transfer Mode
BISDN	Broadband ISDN
BRI	Basic Rate Interface
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
C4IFTW	C4I for the Warrior
CCITT	International Telegraph and Telephone Consultative Committee
CIM	Center for Information Management
CISS	Center for Information System Security
CLNP	Connectionless Network Layer Protocol
CMIP	Common Management Information Protocol
CMW	Compartmented Mode Workstation
CN	Communications Network
COMSEC	Communications Security
COTS	Commercial off-the-shelf
DCI	Director of Central Intelligence
DEA	Drug Enforcement Agency
DGSA	DoD Goal Security Agency
DI	Drug Interdiction
DIS	Defense Information System
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DISSP	Defense Information Systems Security Program
DMS	Defense Message System
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DOJ	Department of Justice
DOS	Department of State

EEI	External Environment Interfaces
EKMS	Electronic Key Management System
ES	End System
FBI	Federal Bureau of Investigation
FDDI	Fiber Distributed Data Interface
FTAM	File Transfer, Access, and Management
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
GOTS	Government off-the-shelf
GSS	General Security Service
GULS	General Upper Layer Security
HDTV	High Definition Television
HIPPI	High Performance Parallel Interface
I&A	Identification and Authentication
IAW	Intelligence Analyst Workstation
IM	Information Management
IPC	Interprocess Communication
ISO	International Organization for Standardization
ITSDN	Integrated Tactical/Strategic Data Network
JCALS	Joint Computer Automated Logistics System
JSAN	Joint Staff Architecture of the Nineties
LAN	Local Area Network
LCS	Local Communications System
LMD	Local Management Device
LSE	Local Subscriber Environment
MAP	Management Application Process
MIB	Management Information Base
MISSI	Multilevel Information System Security Initiative
MG	Military Grade
MLS	Multilevel Security
MSP	Message Security Protocol
MTA	Message Transfer Agent
NLSP	Network Layer Security Protocol
NSA	National Security Agency

OMB	Office of Management and Budget
OSE	Open System Environment
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
PABX	
PCS	Personal Communications Services
PIN	Personal Identification Number
POTS	Plain Old Telephone System
PSTN	Public Switched Telephone Network
RCAS	Reserve Component Automated System
RM	Reference Model
RS	Relay System
RSA	Rivest-Shamir-Adelman
RVM	Reference Validation Mechanism
SAID	Security Association Identifier
SAMP	Security Association Management Protocol
SATCOM	Satellite Communications
SBIS	
SCI	Special Compartmented Information
SDE	Secure Data Exchange
SESEP	Security Exchange Service Element Protocol
SILS	Secure Interoperable LAN/MAN Standard
SMAP	Security Management Application Process
SMIB	Security Management Information Base
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPDF	Security Policy Decision Function
SPEF	Security Policy Enforcement Function
TAC	Terminal Access Control
TAFIM	Technical Architecture Framework for Information Management
TLSP	Transport Layer Security Protocol
TFS	Traffic Flow Security
TRM	Technical Reference Model
UA	User Agent
USAF	US Air Force
USN	US Navy

USFIB	US Foreign Intelligence Board
USG	US Government
VLSI	Very Large Scale Integration