



## **Appendix F2-4**

### Sample Physical Security Mechanisms

Logical Security Services	Physical Security Mechanisms
Entity Unique Naming	Naming standards Naming procedure Directory system
Entity Registration	Registration policy Registration authority system Registration procedure
Entity Public Key Certification	Certification policy Certification authority system Certification procedure Certificate syntax standards Certificate publishing mechanism (directory) Certificate revocation list (CRL) CRL publishing and management (directory)
Entity Credentials Certification	Certification policy Certification authority system Certification procedure Certificate syntax standards Certificate publishing mechanism (directory) Certificate revocation list (CRL) CRL publishing and management (directory)
Directory Service	Directory system Directory access protocols Directory object and attribute syntax rules Directory replication
Entity Authentication	Login procedure User passwords and tokens Client user agents for authentication Authentication exchange protocols Authentication server system Directory system
Session Authentication	Mutual two-way and three-way authentication exchanges Session context (finite state machine)
Message Origin Authentication	Message source identifiers, protected by: Message integrity checksums Digital signatures Hashing
Message Integrity Protection	Message integrity checksums Digital signatures Hashing
Message Replay Protection	Message nonce values protected by message integrity checksums

Logical Security Services	Physical Security Mechanisms
Message Contents Confidentiality	Message contents encryption Encryption key management Routing control to physically secure networks
Non-Repudiation	Digital signatures Notarisation servers Transaction logs Trusted third party certification / arbitration
Traffic Flow Confidentiality	Traffic padding
Authorisation	Roles Fixed role associations with entities Real-time role association with entities Authorisation certificates
Logical Access Control	Local access control agents Local role access control lists (ACLs) Central access manager (CAM) CAM role ACLs Central application access control agents Central application role ACLs Database management system mechanisms File system mechanisms
Audit Trails	Event logs Event log integrity protection mechanisms Event log browsing tools Event log analysis tools Reporting tools
Stored Data Confidentiality	Logical access control mechanisms Physical access control mechanisms Stored data encryption Media storage security Media disposal procedures
Stored Data Integrity Protection	Message integrity checksums Digital signatures Hashing
Software Integrity Protection	Development lifecycle controls Delivery and installation controls Production system configuration control Production system change control Production system management authorisation Crypto-checksums on object code images Regular inspection of object code images and checksums Anti-virus tools
Software Licensing Protection	Software metering

Logical Security Services	Physical Security Mechanisms
System Configuration Protection	Production system configuration control Production system change control Production system management authorisation Cryptographic checksums on configuration data files Regular inspection of configuration data files and checksums
Data Replication and Back-Up	Regular back-up copying Back-up media management: labelling, indexing, transport, storage, retrieval, media recycling, media disposal
Software Replication and Back-Up	Master software media management: labelling, indexing, transport, storage, retrieval
Trusted Time	Secure time server with clock Secure time server protocols
User Interface for Security	GUI login screens GUI security message screens Single sign-on mechanism Ergonomic design of authentication devices Help desk for security problem resolution
Security Policy Management	Data content monitoring and filtering Real-time system monitoring
Security Service Management	Security service management sub-system Secure management protocols Management agents in managed components Access control at all agents and sub-systems Security alarms
Security Training and Awareness	Training courses Training manuals and documentation Publicity campaigns
Security Operations Management	Operator authentication mechanisms Operator activity logs Operations event logs
Security Provisioning	Security service management sub-system Secure management protocols Management agents in managed components Access control at all agents and sub-systems Security alarms
Security Administration	Security service management sub-system Secure management protocols Management agents in managed components Access control at all agents and sub-systems Security alarms

Logical Security Services	Physical Security Mechanisms
Security Monitoring	User activity logs Application event logs Operator activity logs Management event logs Event log browsing and analysis Reporting Real-time system monitoring and Alarms
Security Measurements and Metrics	Cryptographic test mechanisms Inspection tools Penetration testing Statistical tests
Security Alarm Management	Security alarms Security alarm monitoring
Intrusion Detection	Intrusion 'signature' analysis on network traffic Real-time system monitoring Alarms
Incident Response	Data collection and analysis Incident assessment procedures Response action management procedures
User Support	Help desk Trouble ticketing system
Disaster recovery	Data back-ups Software back-ups Data restoration procedures Off-site back-up storage Back-up media management: indexing, labelling, transport, storage, retrieval, recycling, disposal Redundancy of hardware Redundancy of communications lines Recovery plans Recovery procedures
Crisis Management	Vested authority in a crisis manager and crisis management team Assessment procedures Escalation procedures Activation procedures
System Audit	Independent inspection Regular scanning with system audit tools

Logical Security Services	Physical Security Mechanisms
Physical Security	Secure premises with locks, guards, etc Locked rooms for servers, operations and communications Physical protection for cabling Authorisation procedures Identification badges and visitor procedures Supervision of contract engineers etc
Personnel Security	Hiring, background checking and vetting procedures Training courses, booklets, publicity campaigns Disciplinary procedures
Environmental Security	Site-selection procedures Fire prevention, detection and quenching Flood avoidance, detection and removal Air temperature and humidity controls Electrical power protection mechanisms