



Appendix F2-3

Sample Security Services
(in a multi-layered control strategy)

Defensive Strategy	Security Services
Prevention	<p>Entity Security Services:</p> <ul style="list-style-type: none"> • Entity unique naming • Entity registration • Entity public key certification • Entity credentials certification • Directory service • Entity authorisation • Entity authentication • User authentication • Device authentication <p>Communications Security Services:</p> <ul style="list-style-type: none"> • Session authentication • Message origin authentication • Message integrity protection • Message content confidentiality • Non-repudiation • Message replay protection • Traffic flow confidentiality <p>Application and System Security Services:</p> <ul style="list-style-type: none"> • Entity authorisation • Logical access control • Audit trails • Stored data integrity protection • Stored data confidentiality • Software integrity protection • Software licensing management • System configuration protection • Data replication and back-up • Software replication and back-up • Trusted time • User interface for security <p>Security Management Services:</p> <ul style="list-style-type: none"> • Security policy management • Security training and awareness • Security operations management • Security provisioning • Security monitoring • Security measurement and metrics • Security administration (privilege management) • User support • Physical security services • Environmental security services

Defensive Strategy	Security Services
Containment	Entity authorisation Stored data confidentiality Software integrity protection Physical security Environmental security Security training and awareness
Detection and Notification	Message integrity protection Stored data integrity protection Security monitoring Intrusion detection Security alarm management Security training and awareness Security measurement and metrics
Event Collection and Event Tracking	Audit trails Security operations management Security monitoring Security measurement and metrics
Recovery and Restoration	Incident response Data replication and back-up Software replication and back-up Disaster recovery Crisis management
Assurance	Audit trails Security audit Security monitoring Security measurement and metrics