CORBA Security Service

The assets of an enterprise need to be protected against perceived threats. The amount of protection the enterprise is prepared to pay for depends on the value of the assets, and the threats that need to be countered. The security policy needed to protect against these threats may also depend on the environment and how vulnerable the assets are in this environment. This CORBA Security service provides a security architecture which can support a variety of security policies to meet different needs.

The security functionality defined by this specification comprises:

- Identification and authentication of principals (human users and objects that need to operate under their own rights) to verify they are who they claim to be.
- Authorization and infrastructure based access control - deciding whether a principal can access an object domain, individual object, or operation on an object, normally using the identity and/or other privilege attributes of the principal (such as role, groups, security clearance)
- Security auditing to make users accountable for their security related actions. It is normally the human user who should be accountable. Auditing mechanisms should be able to identify the user correctly, even after a chain of calls through many objects.
- Security of communication between objects, which is often over insecure lower layer communications. This requires trust to be established between the client and target, which may require authentication of clients to targets and authentication of targets to clients. It also requires integrity protection and (optionally) confidentiality protection of messages in transit between objects.
- Non-repudiation provides irrefutable evidence of actions such as proof of origin of data to the recipient, or proof of receipt of data to the sender to protect against subsequent attempts to falsely deny the receiving or sending of the data.

The CORBA security model is security technology neutral. For example, interfaces specified for security of client-target object invocations hide the security mechanisms used from both the application objects and ORB (except for some security administrative functions). It is possible to implement CORBA security on a wide variety of existing systems, reusing the security mechanisms and protocols native to those systems.

The security service can control access to an application object without it being aware of security, so it can be ported to environments that enforce different security policies and use different security mechanisms. However, if an object requires application level security, the security attributes must be delegated and made available to the application for access control.

This document defines the core security facilities and interfaces required to ensure a reasonable level of security of a CORBA-compliant system as a whole.