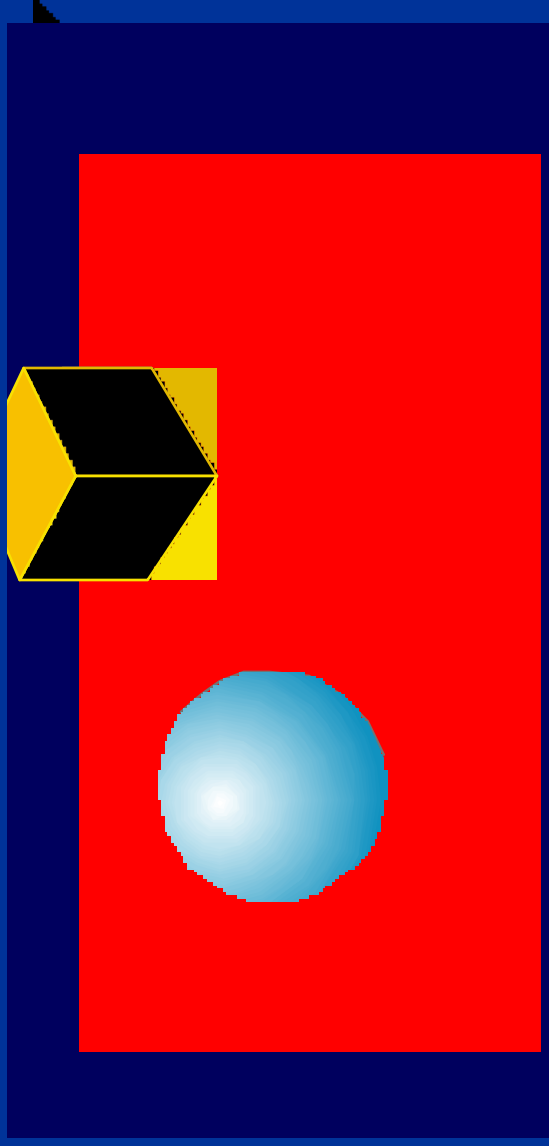


VISIGENIC



SSL Based CORBA Security

Santosh Rau

santosh@visigenic.com

VisiBroker 3.0 for C++



- Thread Management API
 - Thread Pool
 - Thread Per Session (available in 2.0 also)
- Connection Management
- Interceptors
- Plug in Object Adapters
 - IIOP-SSL Object Adapter

Secure Sockets Layer

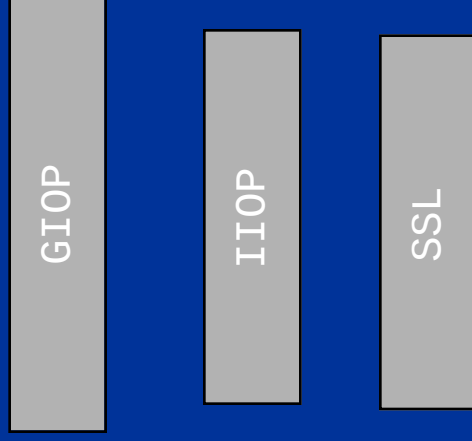


- Client/Server Model
- Message privacy
- Message integrity
- Authentication using X509 certificates

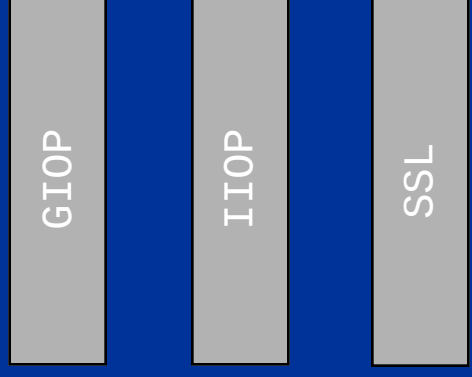
CORBA Security with SSL



Client



Server



IIOP-SSL Object Adapter



- **BOA_init**
 - Adapter ID - “VIS_SSLIIOP”
- **Set up “CredStore” for storing server credentials**
- **IOR indicating SSL as a mechanism**
 - TAG_SSL_IOP
 - Use this tag when registering objects with adapter

CredentialStore



- Stores Server Credentials
- Stores trust management objects
 - Implemented by a custom SSL Handler

SSL Handler



- Allows applications, client or server, to take specific actions
- Useful for
 - Additional verification of certificates
 - Seeding random number generator

Credentials



- **Server Credentials**
 - Private key
 - Trusted Certificate Authority public key(s)
 - Server Certificates (chain)
 - Client Authentication
- **Credentials apply to **all** server objects**

Session Information



- **Currently exposed at object invocation time**
 - Peer identity through X509 certificates
 - Selected cipher suite
- **Custom Interceptors may use this information**

Smart Binding (client)



- Selects IIOP over SSL based on IOR encoding
 - IOR registered with “osagent” by the adapter

VisiBroker 3.0 for C++



► Libraries

- SSLRef 3.0
- SSLPlus
- BSAFE
- Certificate handling toolkits
 - BCERT
 - SSLPlus

Visigenic Software



Questions....