NORTEL
NORTHERN TELECOM

Nortel Secure ORB

Dave Stringer - Distributed Systems & OMG Standards
e-mail: d.r.stringer@nortel.co.uk

Cindy Morton - Security Standards
e-mail: cmorton@nortel.ca

John Warne - Distributed Systems: Security Technology
e-mail: j.p.warne@nortel.co.uk

Our Implementation

Nortel ORB

- Optimised for Performance
- Multiple Protocol Support
- Bindings Multiplexed over Transport Connections
- Provides APIs to manage aspects of the Bindings

Entrust

- PKI - Public Key Infrastructure
- SPKM - Simple Public Key Mechanism
- GSS API - Generic Security Services API
- Modular Toolkit

Departures from CORBAsec

No Symmetric Key

- No Kerberos V5

No Delegation

- neither simple delegation nor restricted delegation

No Secure Interoperability

- that is SPKM is integrated with Nortel's proprietary RPC protocol
- not yet implemented in the context of IIOP

Choices within CORBAsec

Interceptors

- represent a trade-off between separate development and flexibility
- use of DII Request object is a performance hit
- we chose not to use interceptors
- therefore no replaceability of ORB Services

Various “loose ends” intended to give implementors freedom

- may actually be underspecified
- complicate conformance assessment