Poseidon House
Castle Park
Cambridge CB3 0RD
United Kingdom

TELEPHONE: **Cambridge (01223) 515010**
INTERNATIONAL: **+44 1223 515010**
FAX: **+44 1223 359779**
E-MAIL: **apm@ansa.co.uk**

Training

ANSAwise - DCE Security Architecture [Eurocontrol]

Mark Madsen

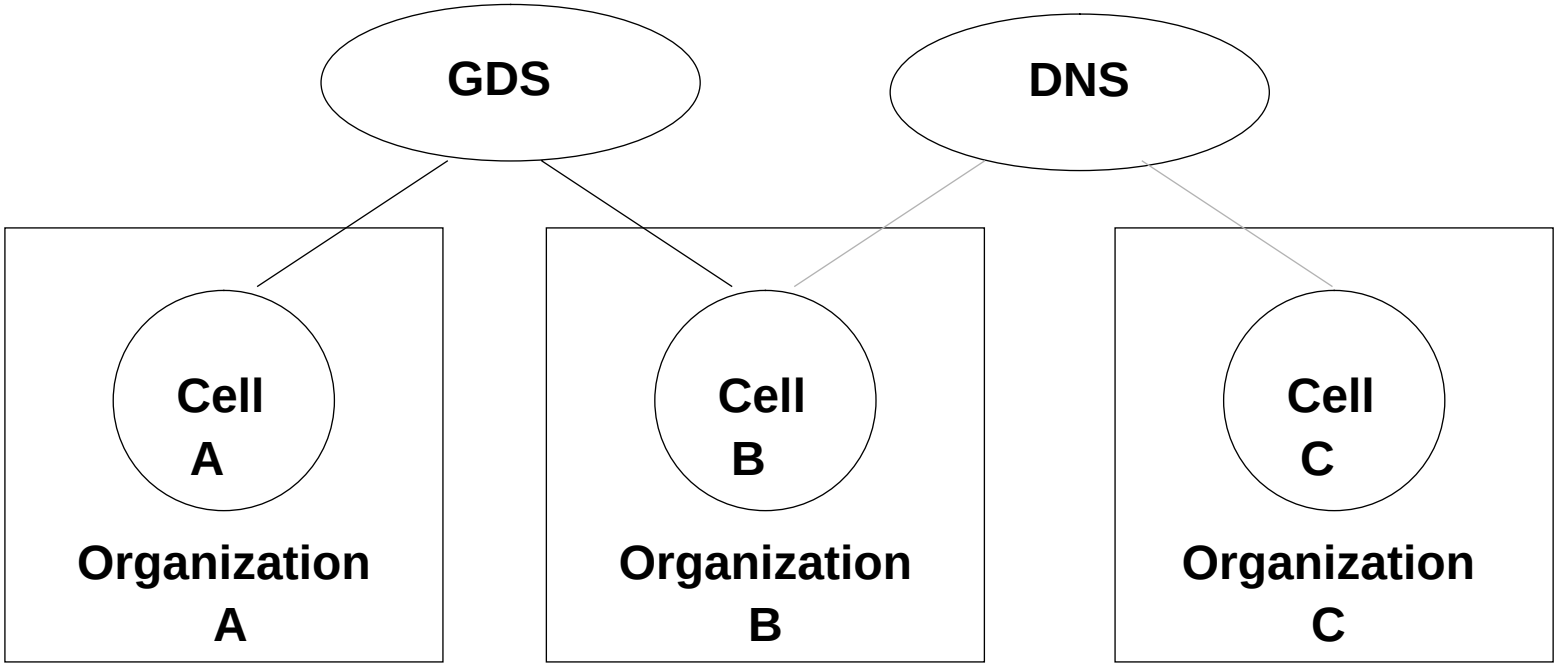
Abstract

This module of the ANSAwise training programme reviews the fundamental DCE services related to security implementation (those in the DCE Secure Core), identifies their limitations, and shows how they will evolve in future versions of DCE.

APM.1621.01 **Approved** 16th October 1995
Briefing Note

Distribution:
Supersedes:
Superseded by:

DCE Security Service

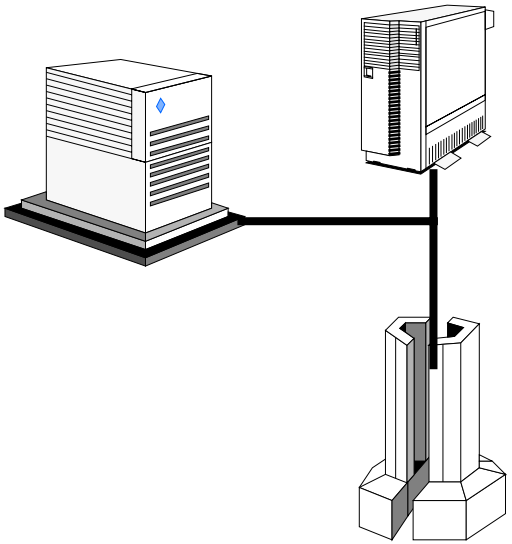


In this session

- ***Explain the DCE Security Architecture***
  - **its key features**
  - **how it contrasts with CORBA**
- ***Show how these services will evolve in future***

The OSF's Focus

- ***Interoperability***



The OSF's Method of Work

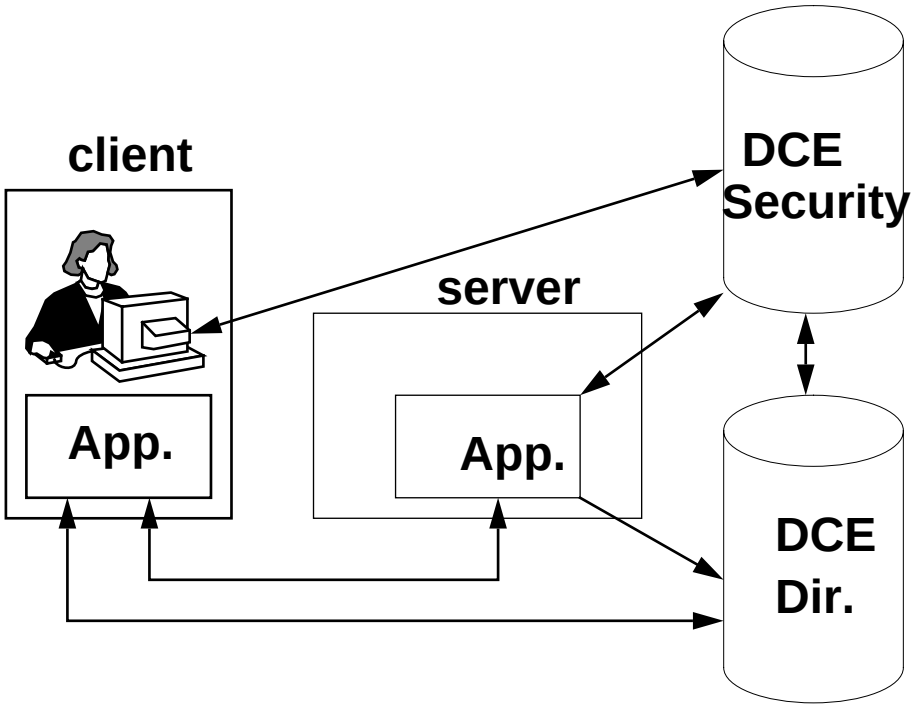
- *Obtain technology by soliciting offerings*
- *Integrate it*
- *License it to vendors*

DCE Services

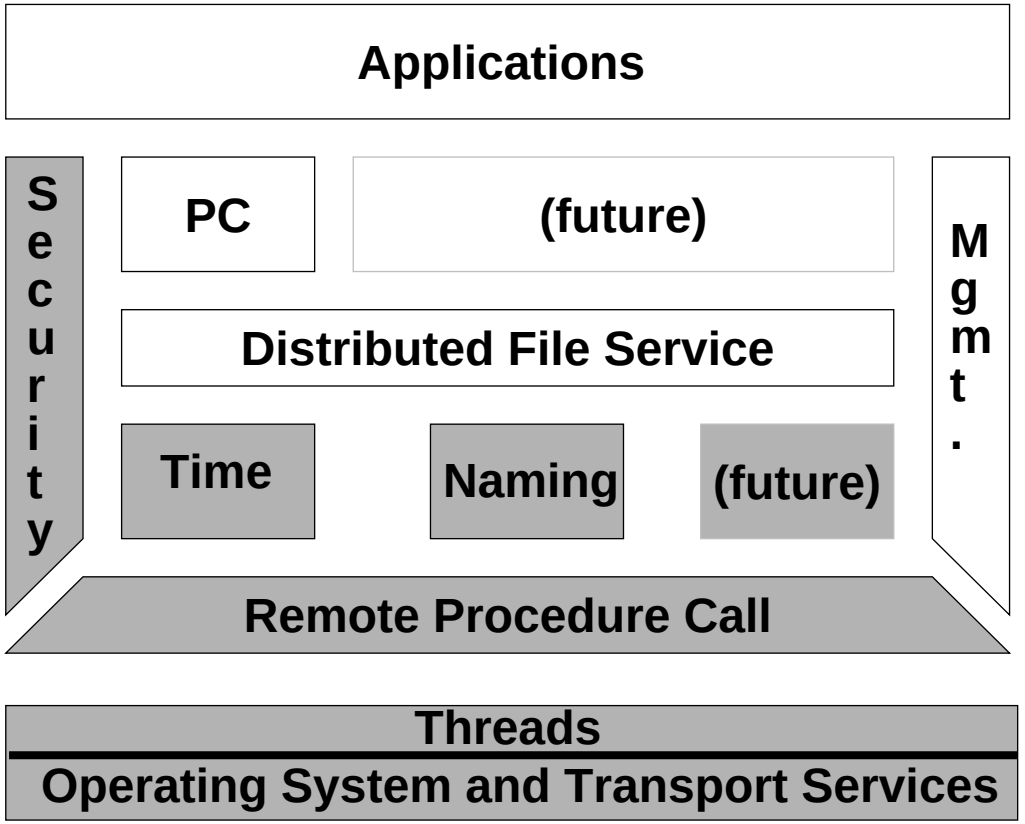
- *Uses a layered model*
- *Fundamental Services are explicitly used by applications*
  - for example, Distributed Time Services
- *Data-sharing services are integrated into the operating system*
  - for example, PC file and printer service
- *The ‘secure core’ services are required components*

The DCE Environment

- *Clients and servers interact with the 'core services'*



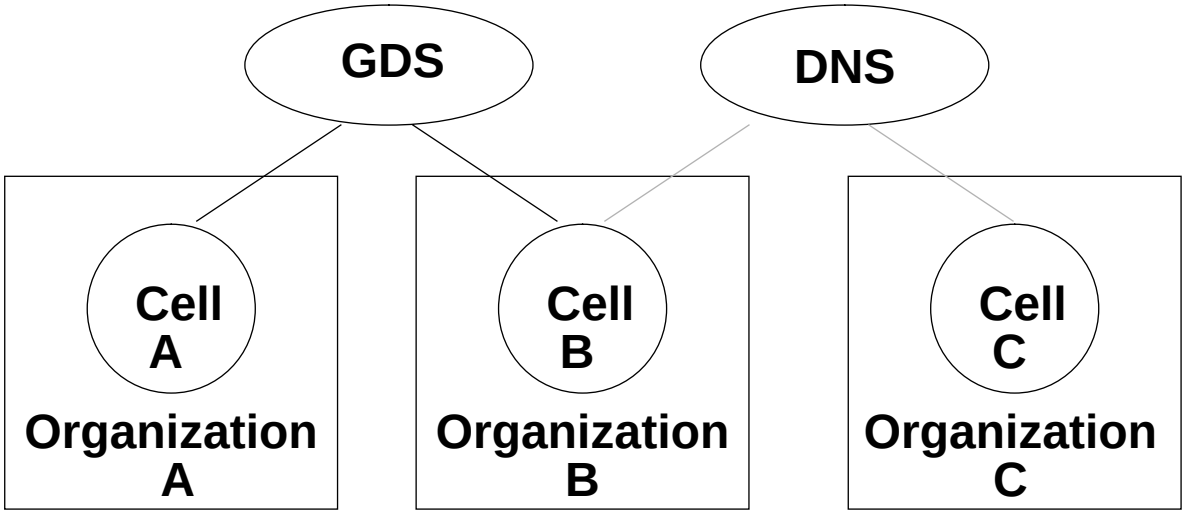
The DCE Component Architecture



DCE System Configurations

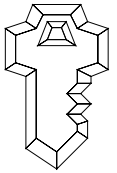
- *Organized into administrative domains called cells*
- *A machine can only be in one cell*
- *Resources are registered in cells*
- *Cells are intended to support up to thousands of machines - or more*

Cell Interconnection



- ***Cells can be interconnected via X.500 GDS, Internet DNS, or both***

DCE Security Services



- ***Based on MIT Project Athena's Kerberos technology (Version 5)...***
- ***... and POSIX 1003.6 (Draft 12) Access Control Lists***
- ***The DCE security protocols are complex, but even the programmer need not see it***
  - **the security services are the interface**

DCE Security Components

- *Authentication Service*
  - allows a process to verify the identity of another process
- *Authorization (Privilege) Service*
  - allows a server to determine whether client access should be granted to a resource
- *Registry Service*
  - maintains the DCE security database
- *Access Control List Facility*
  - allows users to grant and revoke access to resources they own
- *Login Facility*
  - authenticates a user to the security service by means of a password

Using DCE Security

- *End-users use the Login Facility*
  - and probably the Access Control List Facility
- *Administrators use the Registry service*
  - for creating user accounts
  - for cross-cell authentication, between clients and servers in different cells
- *Administrators control security servers*
  - including controlling the replication of security data
- *Administrators control local machine access*

Distributed Security Is Mutual

- *Servers must protect themselves against clients*
- *Clients must protect themselves against servers*
- *Client applications do not need to use the security services directly*
  - typically, they just use Authenticated RPC
- *Server applications use Authenticated RPC too*
  - and also Access Control Lists to control client access to their objects

Authenticated RPC Options

- *Authentication service*
  - No authentication
  - Secret Key
- *Protection level*
  - Beginning of RPC session only
  - Message/packet integrity
  - Encryption
- *Authorization service*
  - Uncertified
  - Certified

Authentication Responsibility

- ***Authentication is a shared responsibility...***

	Server Preference No Authentication	Server Preference Authentication
Client Preference No Authentication	Unauthenticated	Unauthenticated
Client Preference Authentication	*(Fails)*	Authenticated

- ***... but servers must beware!***

- ***Servers must check client preference, if they wish authentication***

Issues with DCE 1.0

- *Administration is tiresome*
- *Many vendors have non-integrated login*
  - must log in to operating system and DCE separately
- *Security loopholes*
  - trivial passwords allowed even under the strictest policy
  - no password expiry
  - unlimited login attempts
  - no auditing
- *Only 32 ACL permissions*

DCE Futures

- *DCE 1.1*
  - Improved administration
  - Security enhancements
  - Internationalization
- *DCE 1.2*
  - to be determined

Interoperability between DCE and CORBA?

- ***The CORBA DCE-CIOP does* not *give service interoperability between DCE and CORBA***
  - **it only gives protocol interoperability for requests and responses**
- ***Service interoperability could in principle also be achieved....***
  - **... like all high-level gateway solutions, transparency is difficult**
  - **... the two architectures are different**

CORBA and DCE - Usability

- *DCE provides services that the CORBA OMA does not yet provide*
  - **But the OMG are filling in the gaps fast**
- *DCE programs are large and tend to be slow*

CORBA and DCE - Markets

- *DCE implementations are mainly from large vendors*
- *Some large vertical markets have settled on DCE*
- *CORBA implementations include smaller vendors*

Summary

- *DCE services are available to distributed clients*
  - the DCE services are themselves distributed
- *The big gaps remain in debugging, testing, and administration*
  - opportunities for third parties
- *For more on DCE*
  - on DCE generally, see *Introduction to DCE* (OSF)
  - for answers to Frequently Asked Questions, see via the World Wide Web http://www.osf.org:8001/
- *For X.500, see CCITT Blue Book Volume VIIII - Fascicle VIII.8: Recommendations X.500-X.521*