



**Poseidon House
Castle Park
Cambridge CB3 0RD
United Kingdom**

TELEPHONE:
INTERNATIONAL:
FAX:
E-MAIL:

**Cambridge (01223) 515010
+44 1223 515010
+44 1223 359779
apm@ansa.co.uk**

Training

ANSAwise - The Future of Distributed Systems

Mark Madsen

Abstract

Distributed systems are developing rapidly as the takeup of sophisticated theory by commercial concerns increases, and as the Internet and the World Wide Web drive the requirements of users for more accurate information and higher-performance services. Especially important is the application of Internet technology within corporations, leading to company-wide Intranets being developed.

This module examines the crystal ball of the near to mid-term future and explains which technologies will become important on that timescale.

APM.1722.01

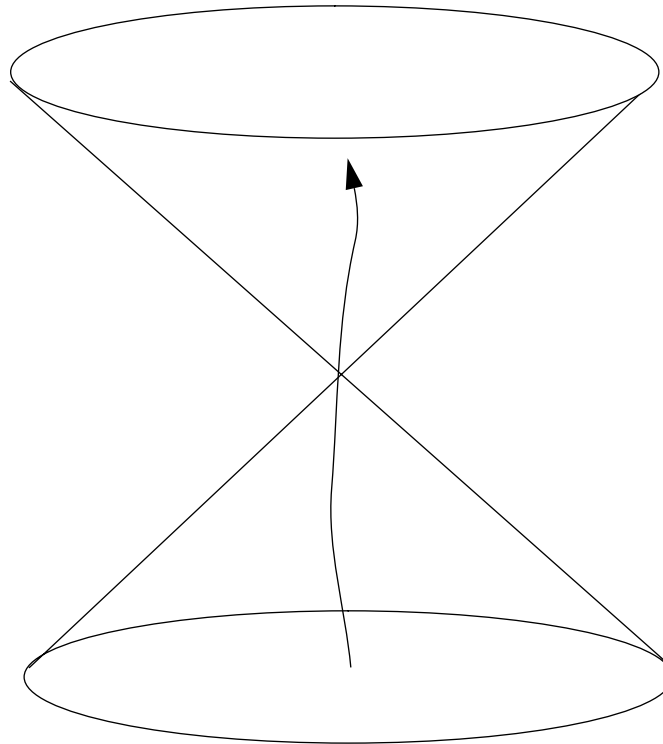
Approved
Briefing Note

4th April 1996

Distribution:
Supersedes:
Superseded by:



The Future of Distributed Systems





In this session

- Describe key developments now happening in distributed systems
- Show how these will affect
 - companies and businesses
 - development of new systems
- Predict future changes in the working of
 - the Internet
 - corporate intranets



Key Areas of Distributed Systems

- **The Internet**
- **The WWW**
- **Intranets**
- **CORBA**



Internet Developments

- Influenced mainly by IAB (Internet Architecture Board) initiatives
- These may be in research areas
 - IRTF (Internet Research Task Force)
- Or in engineering areas
 - IETF (Internet Engineering Task Force)



IRTF Responsibility

- **The IRTF is guiding research on ways to make the Internet more usable**
 - especially ways to find information more effectively
- **Premier among these is the Harvest project**
 - this will perform distributed indexing of Internet sites
 - allowing the indexes to be shared between sites
 - this is a lightweight approach to global indexing



IETF Areas of Rapid Change

- Applications Area
- IPng
- Security Area



Applications Area

- **Things changing rapidly in this area are**
 - **HyperText Markup Language (html)**
 - **HyperText Transfer Protocol (http)**
 - **Multipurpose Internet Media Extensions (MIME)**



IPng Area

- **Internet Protocol version 6 (IPv6) - the Next Generation**
- **IPv6 will have many new capabilities added to those of IPv4**
 - many more network addresses possible
 - security
 - address auto-configuration
- **Transition mechanisms from IPv4 to IPv6 are provided**



Security Area

- **Rapid change topics here are**
 - **Authenticated Firewall Traversal (aft)**
 - **IP Security Protocol (ipsec)**
 - **Public-Key Infrastructure (pkix)**
 - **Web Transaction Security (wts)**
 - **One Time Password Authentication (otp)**



WWW Developments

- **IETF/W3C standards**
 - **URN WG**
 - **URC WG**
 - **PICS Initiative**

- **Near-term business changes will be concentrated on**
 - **Java scripts and code**
 - **Commerce on the WWW**
 - **Security of WWW sites**



URNs

- **Uniform Resource Names**
 - **location-independent names**
 - **designed to be long-lived and stable (immutable)**
 - **like ISBNs for books, or CORBA object references**



URCs

- **Uniform Resource Characteristics**
 - **descriptions of resources or services**
 - **may be ephemeral**
 - **will be used to resolve URNs to URLs (and for other purposes)**



PICS

- **Platform for Internet Content Selection**
- **Driven by W3C together with industry leaders**
- **Purpose is to filter undesirable/unwanted content**
 - **on a per-site basis in the near term**
 - **on a per-resource basis in the long term**



Java Scripts and Code

- **Authentication of Java byte codes is issue**
- **Will be developed using digital signatures**
- **Signature methods based on public key encryption**
 - **fastest to develop and implement**
 - **legal limitations affect security of session keys**



Commerce on the WWW

- **Authentication**
 - Public key cryptosystems
 - Smartcards for fingerprinting user roles
- **Payment Systems**
 - SET secure electronic transactions protocol (Visa, Mastercard)
 - Payment infrastructures (E2S project)
 - Micropayments
- **Electronic cash**
 - DigiCash
 - Scrip



Authentication

- Will be done by using Smartcards for identification
- Digital signatures stored in Smartcard
- Public key mechanisms for signatures
 - perhaps even encryption?
 - limiting factor is governments
- Will be on a per-access basis
 - can be automatic and transparent
- Will be able to limit the number of times an access is made
 - like credit card limits today



SET

- **SET (Secure Electronic Transaction)**
- **Public standard, available for scrutiny**
- **Owned by Visa and Mastercard**
 - **will be built in to future webservers and browsers**
 - **Netscape and Microsoft amongst others**
- **Will be used to replace present method of sending card numbers**



Payment Infrastructures

- These are being developed by a variety of projects
- APM is involved in E2S
 - “End to End Security on the Internet”
- These will create secure payment systems for Internet commerce
 - security is key necessity for deployment



Micropayment

- **Micropayment is the term for small electronic payments**
- **Digital has estimated that micropayments could be very small**
 - **less than 1/100 of a US cent**
 - **but still be worthwhile**
- **This will make previously unprofitable services highly profitable**
 - **such as charging for web page download**



Electronic Cash

- **Systems like this are already being deployed**
- **They will soon become widely available**
 - **presently banks are unhappy with encryption-related issues**
- **Examples are**
 - **DigiCash**
 - **CyberBucks (Mark Twain Bank)**



Security of WWW Sites

- **Firewall challenges**
 - Protecting against protocol tunnelling
 - Fine-grained service access
- **Webserver access controls**
 - Kerberos authentication on servers
 - PGP/PEM protection of URLs
- **Subscription services**
 - will be based on digital authentication



Firewalls

- **Webservers will need subtle and powerful firewalls**
 - because the business stakes are high
- **They will protect against spoofing**
 - using secure IP
- **They will use at least one layer of sacrificial technology**
 - to detect illegal accesses with high degree of certainty



Access Control

- Kerberos-type third party authentication will be the basis for access
- The Kerberos ticket authority will require independent verification
 - such as that provided by Verisign
- Servers will have fine-grained access control
 - possibly on the level of individual URLs
 - obtained using PGP/PEM encryption of links



Intranet Developments

- **Corporations will use more internal information services**
 - **direct business support**
 - **indirect business**
- **WWW paradigms are widely known and used**
 - **companies use WWW-based service access mechanisms**
- **Companies will have micro-Internets**
 - **Intranets**

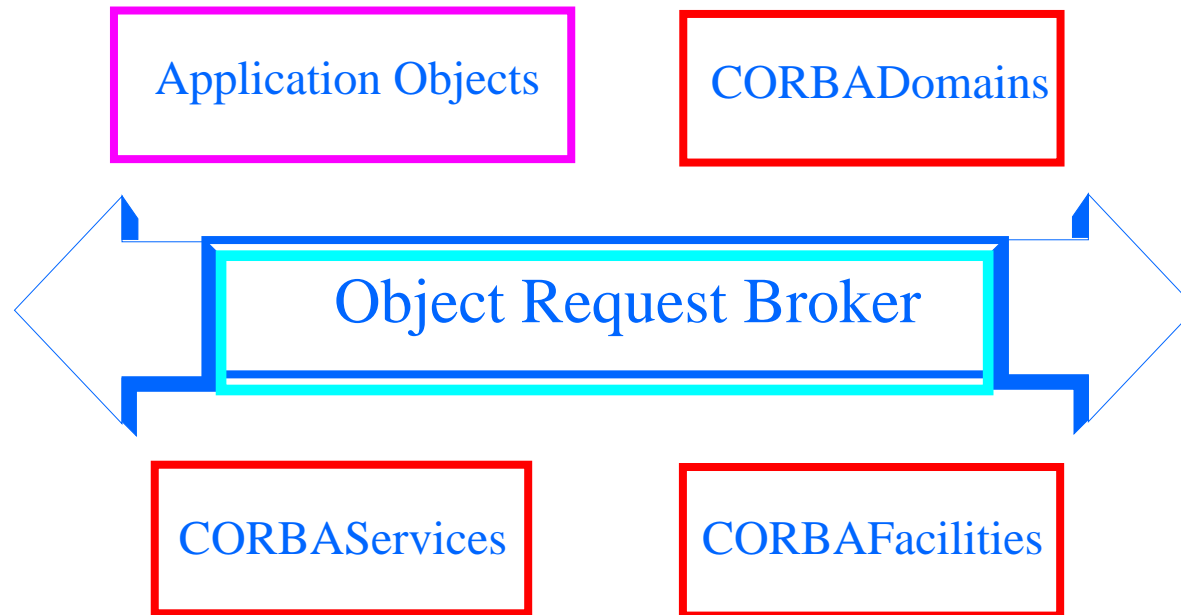


CORBA Developments

- These are covered in more detail in the CORBA Futures presentation
- Multimedia
- Security
- OMA revision
 - Vertical market integration
 - Horizontal market integration



Revised Object Management Architecture





Summary

- **The WWW will drive changes in the functioning of**
 - corporate information systems
 - corporate business processes
 - the Internet and CORBA

- **CORBA will change to provide better support for**
 - custom services
 - gatewaying to the Internet
 - secure reliable transactions



More information?

- For more on IPv6/IPng
 - [<URL:http://playground.sun.com/pub/ipng/html/ipng-main.html/>](http://playground.sun.com/pub/ipng/html/ipng-main.html/)
- For more on the future of the Harvest Project
 - [<URL:http://harvest.cs.colorado.edu/>](http://harvest.cs.colorado.edu/)
- For more on DigiCash
 - [<URL:http://www.digicash.com/>](http://www.digicash.com/)
- For more on Verisign
 - [<URL:http://www.verisign.com/>](http://www.verisign.com/)
- For more on the future of the WWW
 - see *The World Wide Web - Beneath the Surf*, by Mark Handley and Jon Crowcroft, UCL Press, 1994, ISBN 1-85728-435-6 [<URL:http://www.citenet.net/main/info/books/bts/book.html>](http://www.citenet.net/main/info/books/bts/book.html)