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**

ANSA Phase III

WWW'95 Security on the Web

Owen Rees

Abstract

These are the slides used to describe the ANSA view of distributed system security principles at the panel session “Security on the Web” at the WWW’95 conference in Darmstadt, Thursday April 13th 1995.

They are based on a presentation on the Security Framework given to the Technical Review Committee of the ESPRIT ISA project in April 1992.

APM.1456.01 **Approved** 7th April 1995

External Paper

Distribution:
Supersedes:
Superseded by:

- Owen Rees <rtor@ansa.co.uk>
- ANSA — Object-based Architecture for open distributed systems
  - started 1985 — now in Phase III
- APM — Architecture Projects Management Limited
  - Projects, consulting and training in wide area networked and distributed object-based interactive multi-media information systems.
- Find out more at <URL:http://www.ansa.co.uk/>

Enterprise and Information

- Purpose and Meaning
- Enterprise defines meaning of "security"
  - Policy: Objectives, missions, constraints
  - Soundness
  - Evolution towards security, stability
  - Federation, multiple policies — conflicts
  - Obligations — responsibility, accountability, liability
  - Agents, Activities, Resources — permitted relationships
  - Administrations and authority structures
  - Proxies, delegation
  - Trust
- Information
  - Data / Information — representation and interpretation

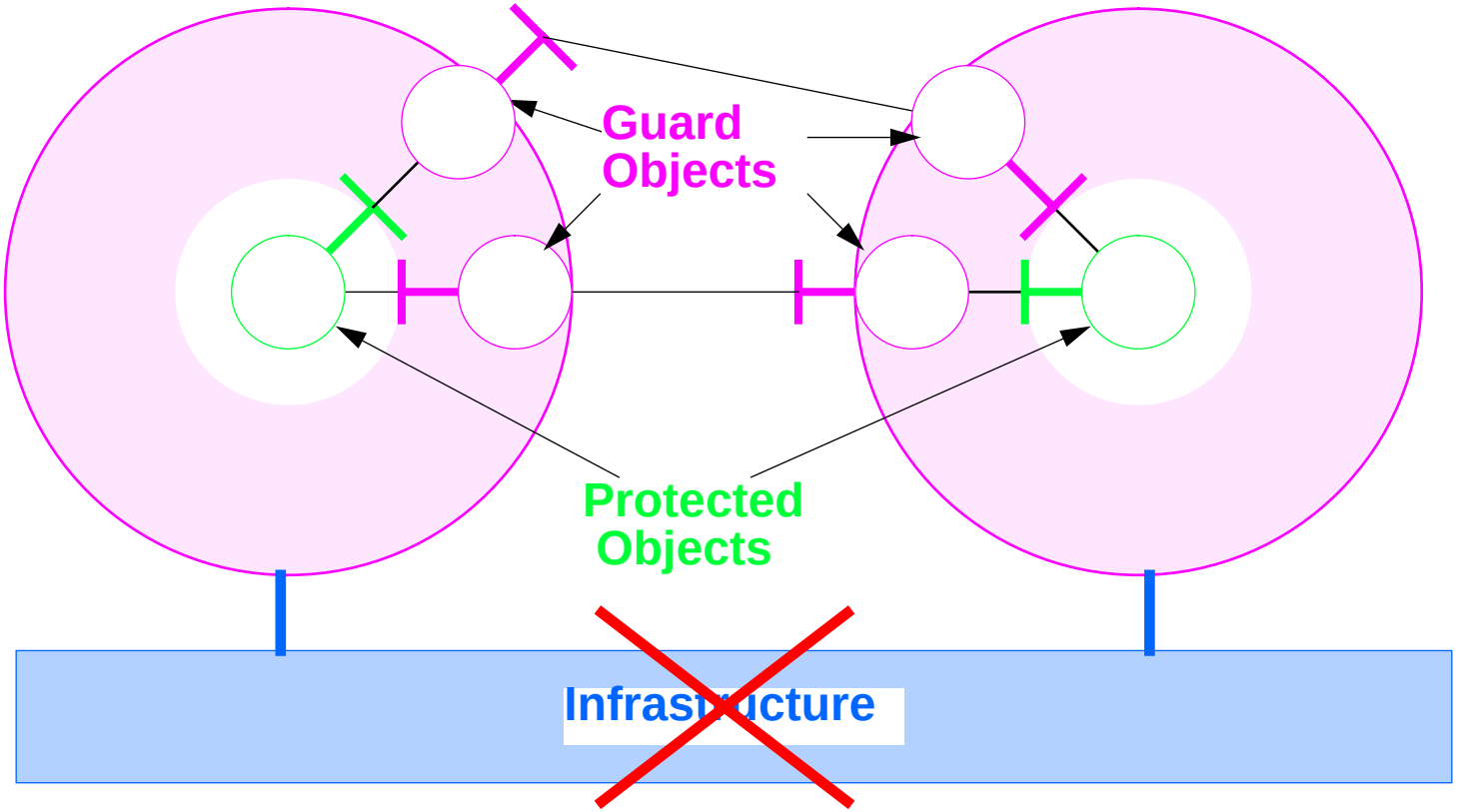
ANSA Object Model

- **Encapsulation and interaction**
  - Enforce encapsulation
  - Control interaction
- **Granularity of control**
  - Object — unit of encapsulation
  - Interface — unit of provision of service, unit of granting of access
- **Controlled delegation**
  - Interface reference passing — least privilege
  - Sealed representation — forwarding, storing without granting right to use

Naming

- **Security requires identification**
  - Sameness
  - Distinctness
- **Comparing entities by comparing their names**
  - Names are relative to contexts
  - Generation and resolution processes
  - Federation
- **Identifiers — what assumptions are being made?**
  - Not an alias — only name for entity in this context
  - Not a homonym — name of only one entity in this context

Infrastructure Model



Summary

- **Enterprise model**
  - concepts
  - relationship to security requirements
- **Naming model**
  - identification
  - making comparisons and distinctions
- **ANSA object model**
  - Encapsulation and interaction
  - Granularity of control
- **Infrastructure model**
  - transparent security
  - generic and specialised components