Some Directions of Research for MIKADO : From Security Issues To Security Domains

Marc Lacoste (FT R&D)

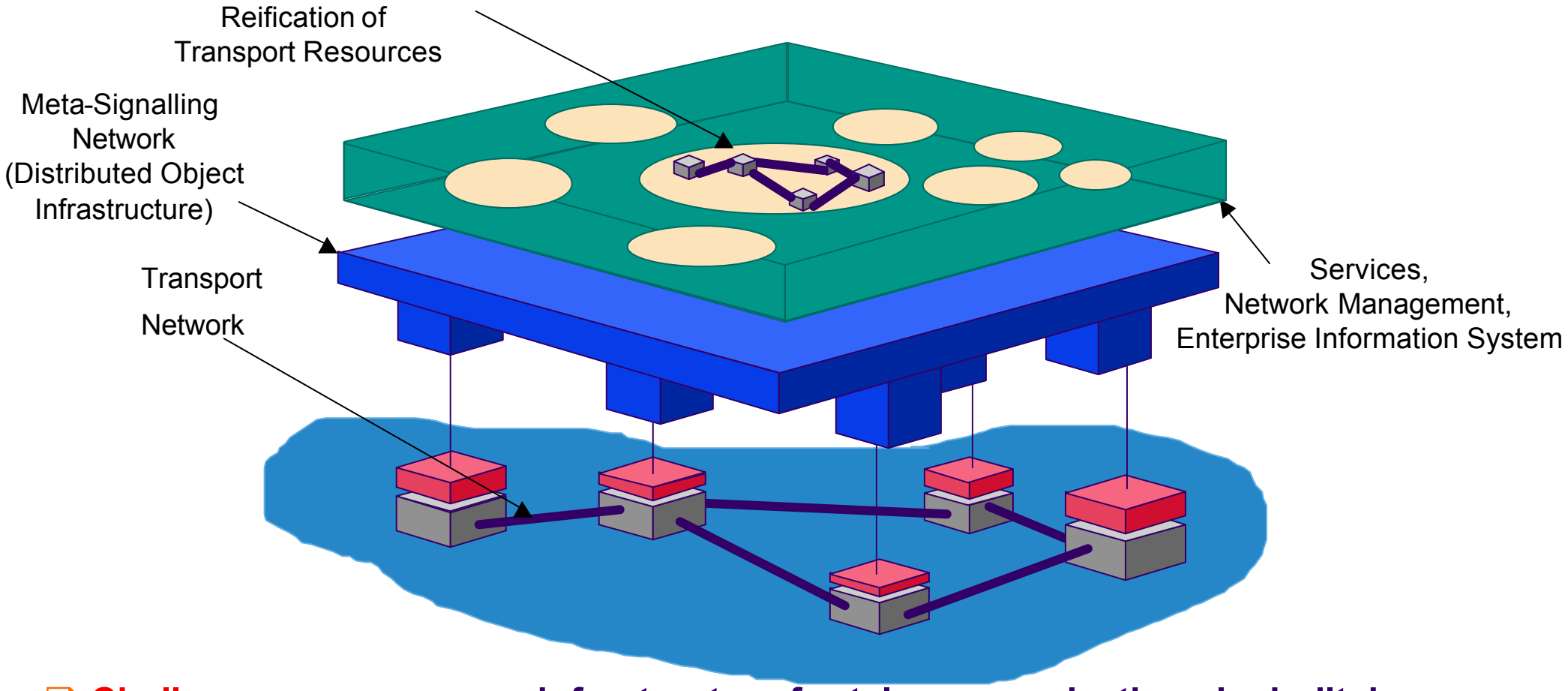
MIKADO Kick-Off Meeting

Security concerns for telco networks (1)

- **Security is a primary concern for telco networks like France Telecom's enterprise information system**
  - ✓ **Global computing environments :**
    - Openness
    - Pervasiveness of networking
  - ✓ **Protection guarantees :**
    - Confidentiality,
    - Integrity
    - Availability
  - ✓ **An overall and end-to-end approach of security is necessary:**
    - Language
    - Middleware
    - Operating system

Security concerns for telco networks (2)

- **Telco networks can be seen as large scale distributed systems…**
  … Partitionned into several kinds of domains, some of which overlap

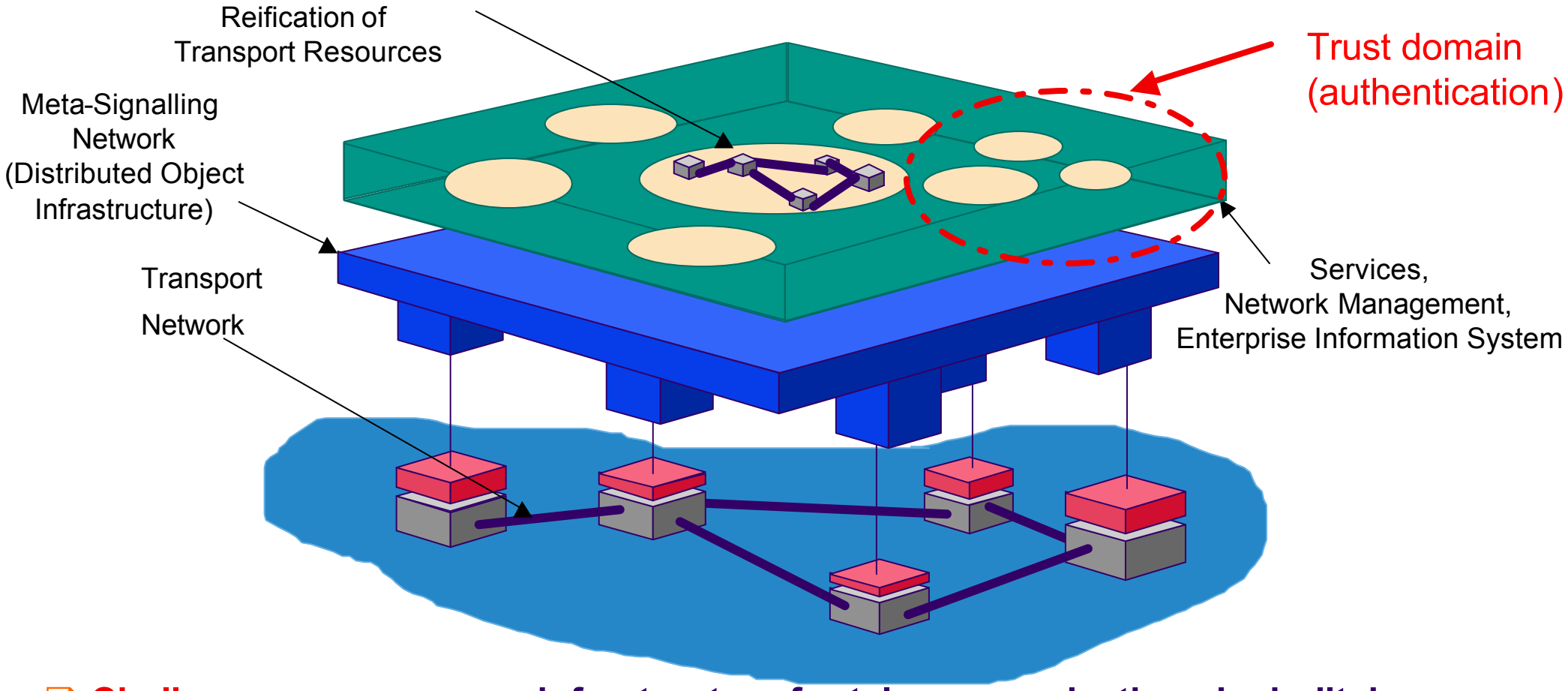


- **Challenge : can a secure infrastructure for telecommunications be built by superposition of several types of security domains ?**

France Télécom R&D

Security concerns for telco networks (2)

- **Telco networks can be seen as large scale distributed systems…**
  … Partitionned into several kinds of domains, some of which overlap

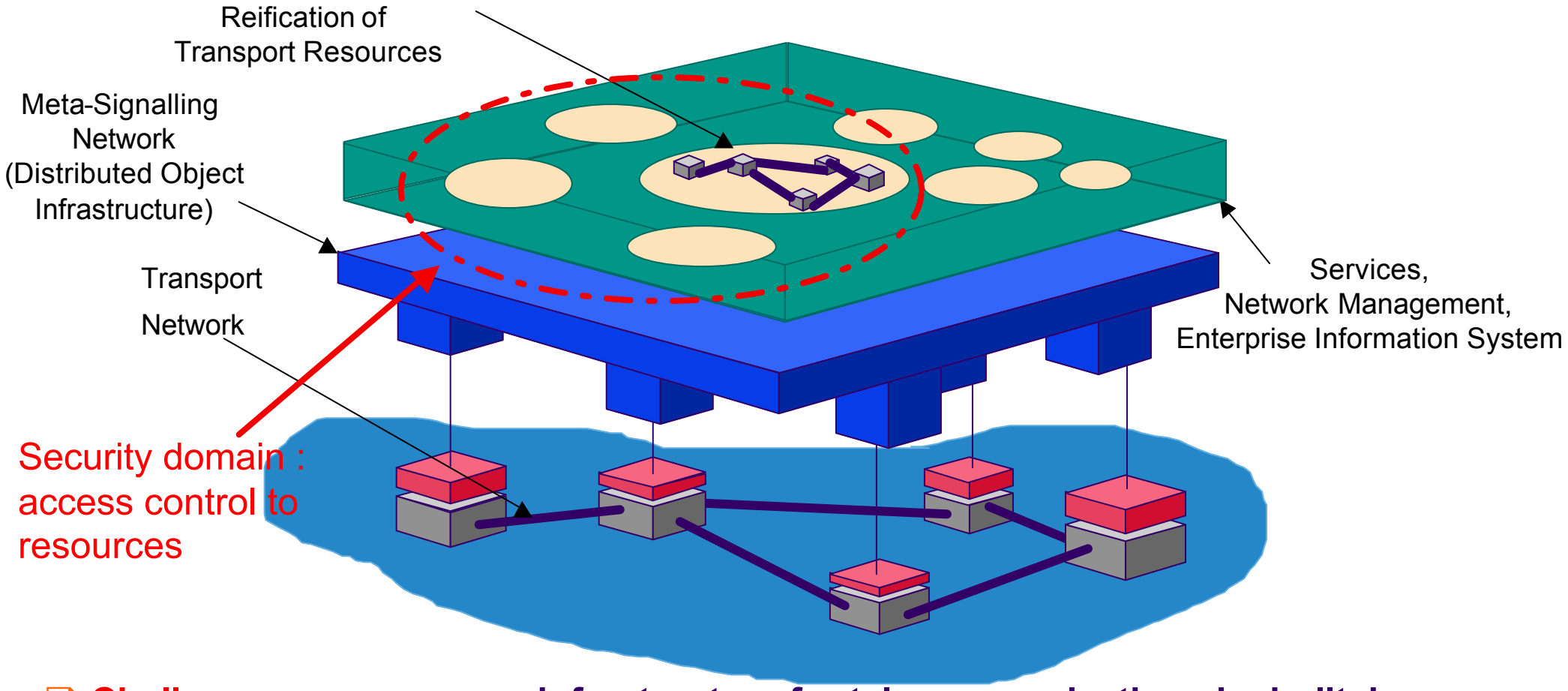


- **Challenge : can a secure infrastructure for telecommunications be built by superposition of several types of security domains ?**

France Télécom R&D

Security concerns for telco networks (2)

- **Telco networks can be seen as large scale distributed systems…**
  … Partitionned into several kinds of domains, some of which overlap

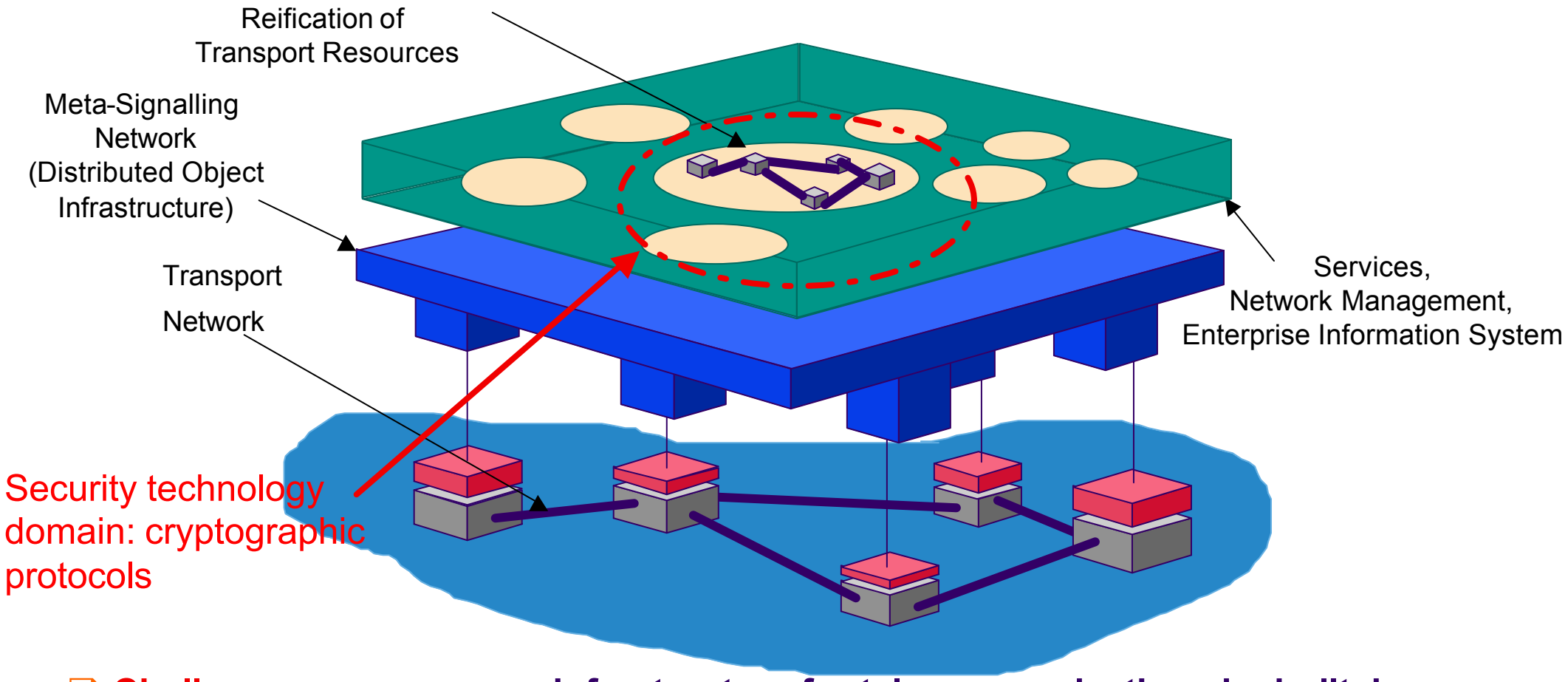


- **Challenge : can a secure infrastructure for telecommunications be built by superposition of several types of security domains ?**

France Télécom R&D

Security concerns for telco networks (2)

- **Telco networks can be seen as large scale distributed systems…**
  … Partitionned into several kinds of domains, some of which overlap



- **Challenge : can a secure infrastructure for telecommunications be built by superposition of several types of security domains ?**

From telco networks to MIKADO security domains

- **A MIKADO domain :**
  - ✓A **strong abstraction** to deal in a uniform way with distributed system partitions
  - ✓An embodiment of a **homogeneous vision of security** at all levels
- **Domain-based security in MIKADO :**
  - ✓**Security Models with domains as first-class citizens : WP1**
    - ➔**Language-based security**
  - ✓**Middleware and Virtual Machine Technology : WP3**
    - ➔**Definition of secure APIs**
  - ✓**[Operating Systems Security]**

From telco networks to MIKADO security domains

- **A MIKADO domain :**
  - ✓A **strong abstraction** to deal in a u
  - ✓An embodiment of a **homogeneou**
- **Domain-based security in MIKADO**
  - ✓**Security Models with domains as**
    - ➔**Language-based security**
  - ✓**Middleware and Virtual Machine**
    - ➔**Definition of secure APIs**
  - ✓**[Operating Systems Security]**

« The API sits on the boundary between trusted and untrusted environments. It is the point where cryptography, protocols, access controls, and operating procedures must all come together to enforce the security policy.

Designing a secure and robust API is a fundamental challenge which has until recently been overlooked both by formal methods and software engineering researchers … API design could be the next basic research challenge. »

Mike Bond and Ross Anderson, Security Group at the University of Cambridge Computer Laboratory, IEEE Computer, October 2001.

Programming models for security (WP1)

- **Proposed contribution with MIKADO partners:**
  - ✓ **Analysis of the state of the art in programming models for security**
    - **Process calculi**
    - **Logics**
  - ✓ **Definition of specialized subcalculi of the MIKADO core programming model for security domains**
    - **Two special types of security domains could be considered:**
      - **Trust (authentication) :** design and analysis of security protocols. Guarantees of authenticity or secrecy.
      - **Access control**
    - **Relation with existing calculi / logics**

Programming models for security (WP1)

- **Some possible process algebras :**
  - ✓ **Access-control oriented calculi**
    - **Ambient-like calculi :** security by scoping and by the locality construct : ambients (capabilities) ; safe ambients (coactions) ; boxed ambients; seal-calculus (portals)
    - **Linda-based paradigm :** KLAIM (type system to statically enforce security properties)
  - ✓ **Cryptographic extensions of existing name-passing calculi :** spi-calculus, sjoin-calculus
  - ✓ **Extensions of calculi with authentication constructs :**
    - Join+auth (Abadi, Fournet, Gonthier)

- **Some possible logics :**
  - ✓ **Authentication :** BAN logic. Analysis of questions of belief (trusts assumptions) in authentication protocols
  - ✓ **Access control :**
    - « A calculus for access control » (Abadi) : formalisation of ACLs. A calculus of principals + extension by a modal mogic. Group intersection (domain overlap) is taken into account.

Components for secure distributed infrastructures (WP3)

❑ Proposed contributions with MIKADO partners:

- ✓ **Analysis of the state of the art** in virtual machine technology for secure distributed infrastructures

- ✓ **Definition of a specialization for security components of the MIKADO Core Software framework**
  - Refinement of the design patterns identified in the Core Software Framework for security components implementing different domain types:
    - ❖ **Authentication**
    - ❖ **Authorization**
  - **Definition of security APIs**

Components for secure distributed infrastructures (WP3)

- **Proposed contributions with MIKADO partners:**
  - ✓ **Development of software prototypes implementing the MIKADO programming models for security. For instance:**
    - ✓ **Middleware Level :**
      - ✓ Specialization of the **k -VM** for the design and analysis of distributed authentication protocols
      - ✓ Implementation of the specialized security framework using the ObjectWeb Component Framework Implementation. Possible coupling with CORBA or Java environments.
    - ✓ **[Operating System Level :]**
      - ✓ Introduction of security domains in the **Think** ExoKernel (FTR&D, INRIA)