

**Imperial College  
London**

# **Trust and the Establishment of Ad-hoc Communities**

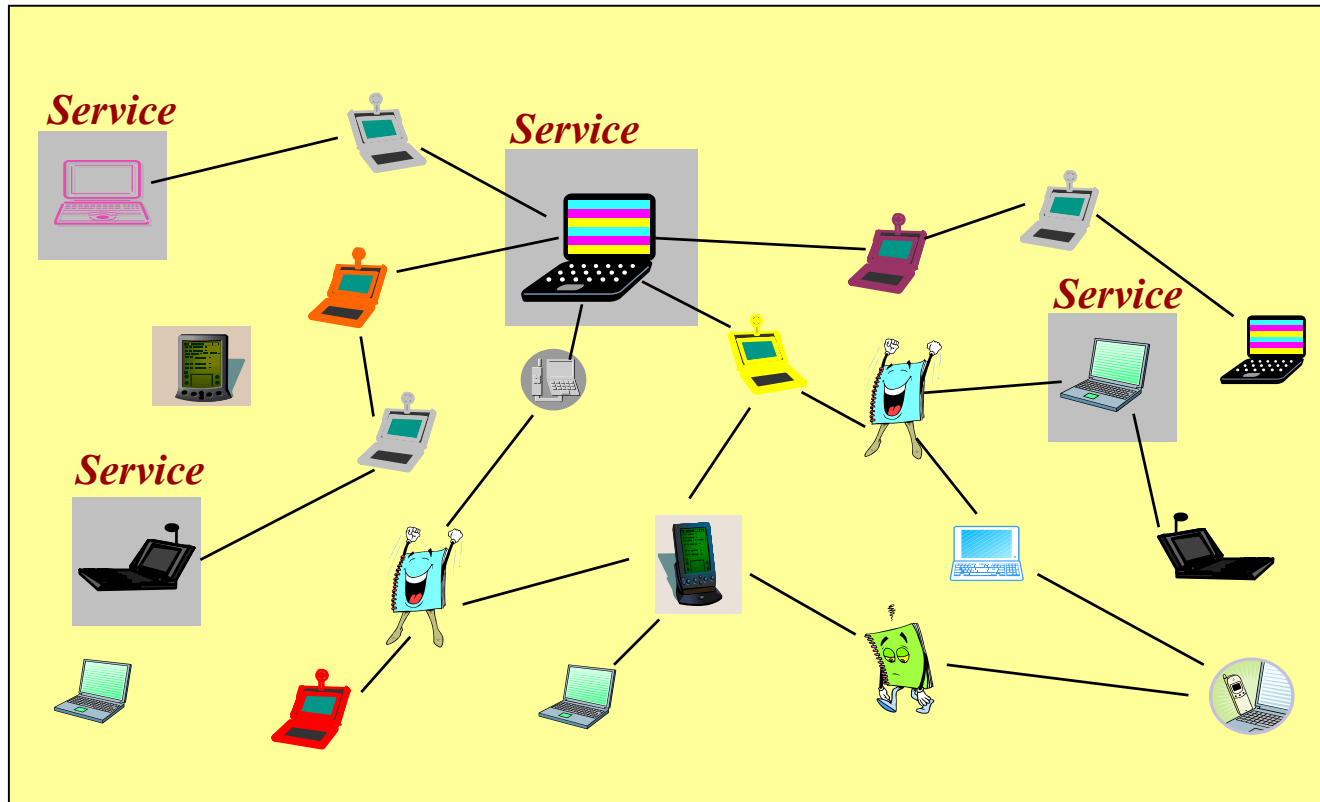
Sye Loong KEOH and Emil LUPU

Department of Computing, Imperial College London, UK



The Second Internal iTrust Workshop on Trust  
Management in Dynamic Open Systems

## Community

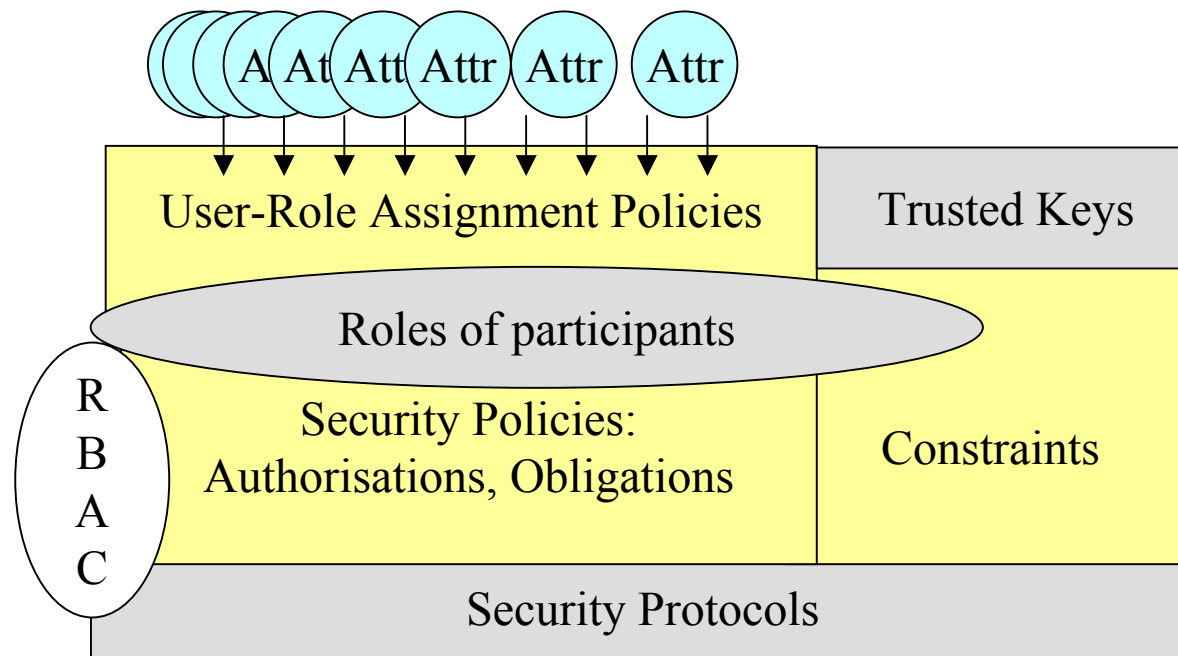


Well-defined  
Rules

Security  
Issues

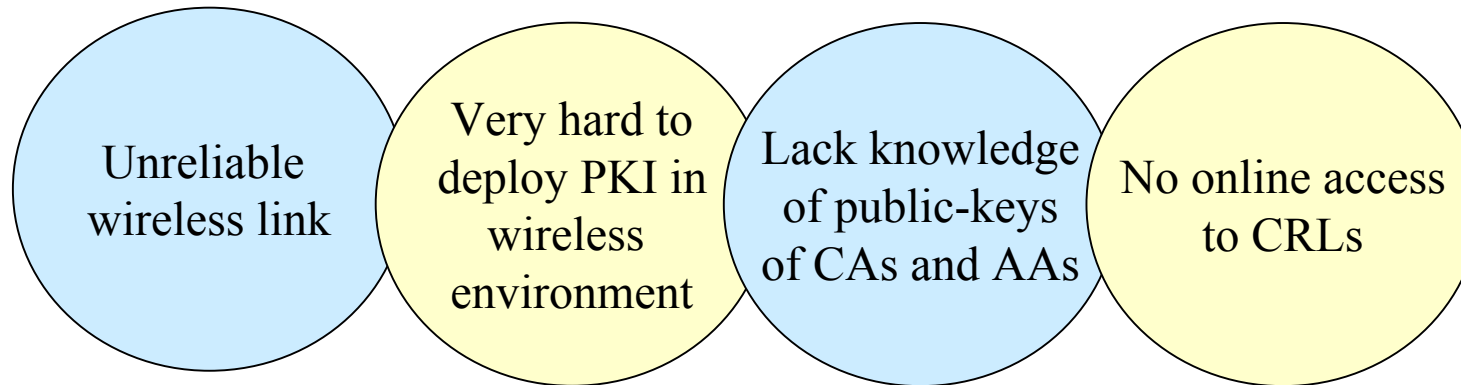
Trust  
Solution?

- *Community doctrine*
  - *A specification of the configuration and security policies of an ad-hoc community.*



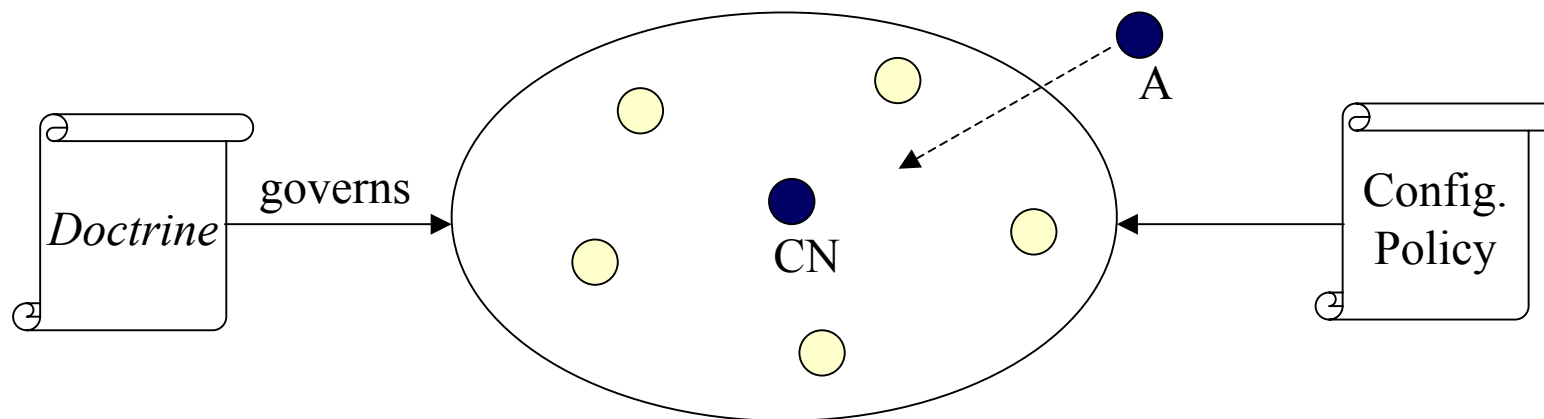
- *Doctrines are:*
  - *Parameterised by the participants.*
  - *Made publicly available to potential users.*
  - *Used to instantiate community with different participants.*
- All the participants must adhere to the rules defined in the *doctrine*.
- However, they have to rely on each other to enforce these rules.

# Trusting Peers?



- Allows entities to exchange information, i.e. certificates they know or have verified.
- The use of *Credential Assertions*.
- To ascertain a user's identity, role information, memberships or other attributes.

- The validity of assertions is measured based on:
  - Do you trust the issuer? **Trusted key ring**
  - Is the asserted information trustworthy? **Partial verification**
- Assumptions - Members in the community are
  - Trusted to abide to policies.
  - Trusted to issue assertions.



- A policy-based approach to establish ad-hoc communities using *doctrines*.
- An initial approach towards providing some level of trust based on *credential assertions*.
- Rely on peers in the community to provide security information.
- A better trust model and the use of recommendations and past experience.