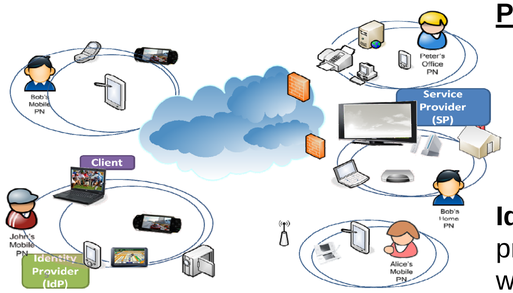
RISK ASSESSMENT FOR BETTER IDENTITY MANAGEMENT IN PERVASIVE ENVIRONMENTS

Patricia Arias Cabarcos, PhD Student, Telematic Engineering Department, University Carlos III of Madrid

PERVASIVE Computing Laboratory

1. Motivation



Pervasive scenarios:

- Are multiservice, multiprovider, multidevice
- Allow cooperation and collaborative apps. (e.g. Personal Networks Federation)

Identity Management (IdM): indispensable to provide a seamless/secure user experience within the ecosystem of pervasive services

Goal: Dynamic Federation

2. Current Identity Management Solutions

IdM frameworks: SAML/Liberty Alliance, WS-Federation, OpenId.

Limitations: No trust or rigid trust (based on static preconfiguration), poor scalability, users are mostly unaware, interoperability

Challenges:

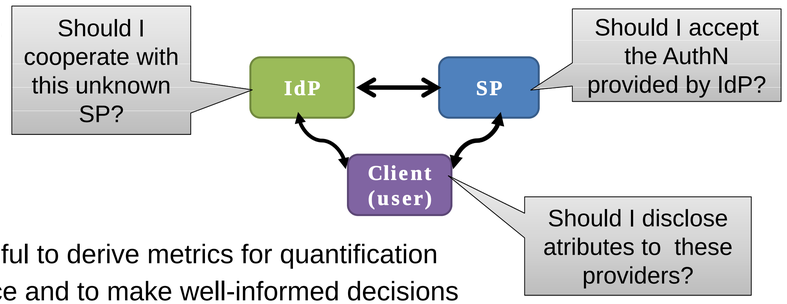
We need to **modify current IdM systems** to:

- Minimize dependence on pre-configuration, making entities autonomous and capable of making trust decisions dynamically
- Introduce a **risk management model** to enhance security and deal with uncertainty
- Take advantage of common knowledge and enrich trust mechanisms (e.g. reputation-based trust)

3. Risk Assessment in Identity Management

Every actor has to make decisions that imply dealing with risk:

- **Pre-Federation Phase**
- **Post-Federation Phase**



Risk computation:

$$TR = \sum_{i}(R_i) \quad i = 1, \ldots, N$$

$$R = P \times I$$

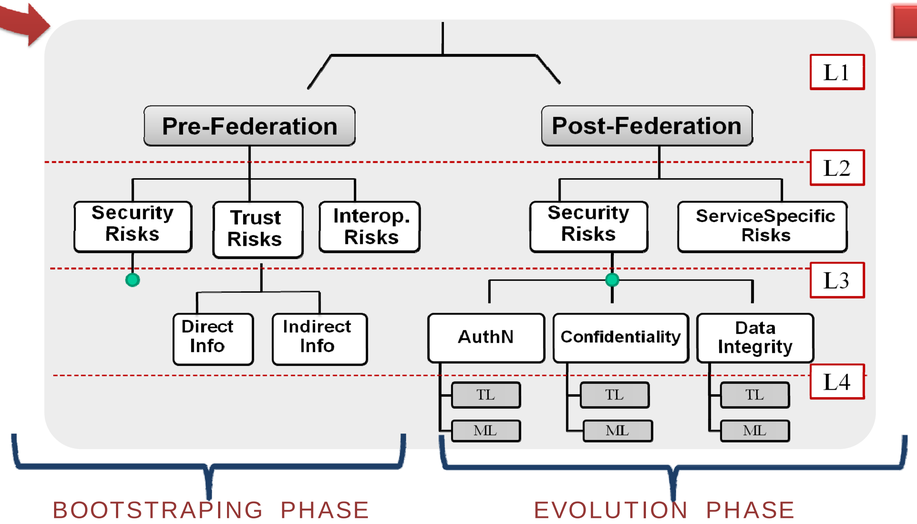
Quantification is hard → no previous work in IdM

Approach: metric-based
First step: taxonomy

We propose a **Risk taxonomy** that:

- Compiles the characteristics of Federated IdM systems
- Makes possible risk decomposition in small subsets. Useful to derive metrics for quantification
- Should be adopted by every entity to enrich its intelligence and to make well-informed decisions

4. Risk Taxonomy



5. Risk Metrics

"If you cannot measure (or model) it, you cannot improve it"
-Lord Kelvin

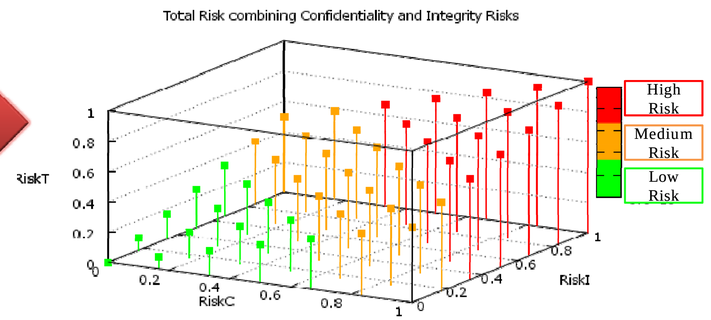
Metric Name: Integrity (INT)
Range: 0 – 6
Description: Measures integrity at transport and message level based on underlying cryptography,
↑Integrity ↓Risk

Metric Name: Confidentiality (CONF)
Range: 0 - 6
Description: Measures confidentiality at transport and message level based on underlying cryptography,
↑Confidentiality ↓Risk

More metrics: Level of assurance, SLA / Metadata compliance, Anonymity degree, Time validity window, Data Sensitivity …

6. Work in Progress & Future Lines

- Aggregation of risks $RiskT = \propto \times \underbrace{\frac{Max(CONF) - CONF}{Max(CONF)}}_{RiskC} + (1-\propto) \times \underbrace{\frac{Max(INT) - INT}{Max(INT)}}_{RiskI}$



- Definition of a comprehensive set of metrics
- Develop a prototype capable of engaging in secure dynamic federations