Digital Identity Management and Trust Negotiation

E. Bertino[1], A.Bhargav-Spantzel[1], A.C.Squicciarini[2]
[1]CERIAS, Purdue University, [2]University of Milan, Milan, Italy

Federated Identity:

A federated identity is a digital credential analogous to a country passport. A federation is a set of organizations which establish trust relationships within which the federated identity is considered valid.

Trust Negotiation Model:

The gradual disclosure of credentials and requests for credentials between two stranger entities, with the goal of establishing sufficient trust so that parties can exchange sensitive resources.

- *The goal:* establish trust between parties in order to exchange sensitive information and services
- *The approach:* establish trust by verifying properties of the other party.

Building Blocks:

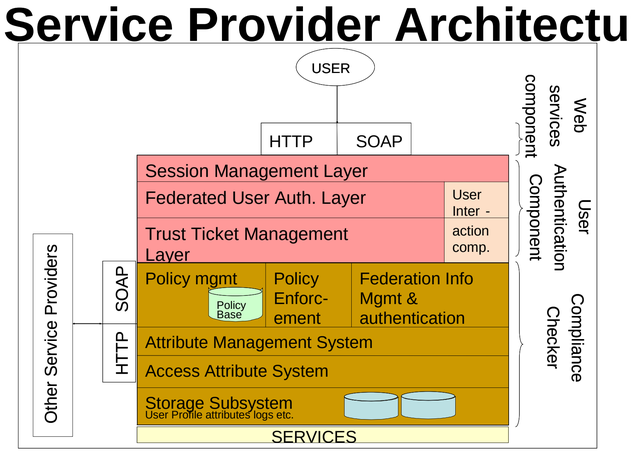
1. **Subject Credentials:** Assertions about the credential owner issued by a Certification Authority

2. **Disclosure policies:** Statements expressing trust requirements by means of credential combinations, protecting access to resources, sensitive information and disclosure of sensitive credentials.

Integrating Federated Identity and Trust Negotiation Model:

The *approach* we propose requires negotiation between service provider and user and among service providers.
The negotiation protocol depends on the different types of users which are given as follows:
- Users that are *members* of the federation
- *External* users (new or repeated)

FAMTN Service Provider Architecture:

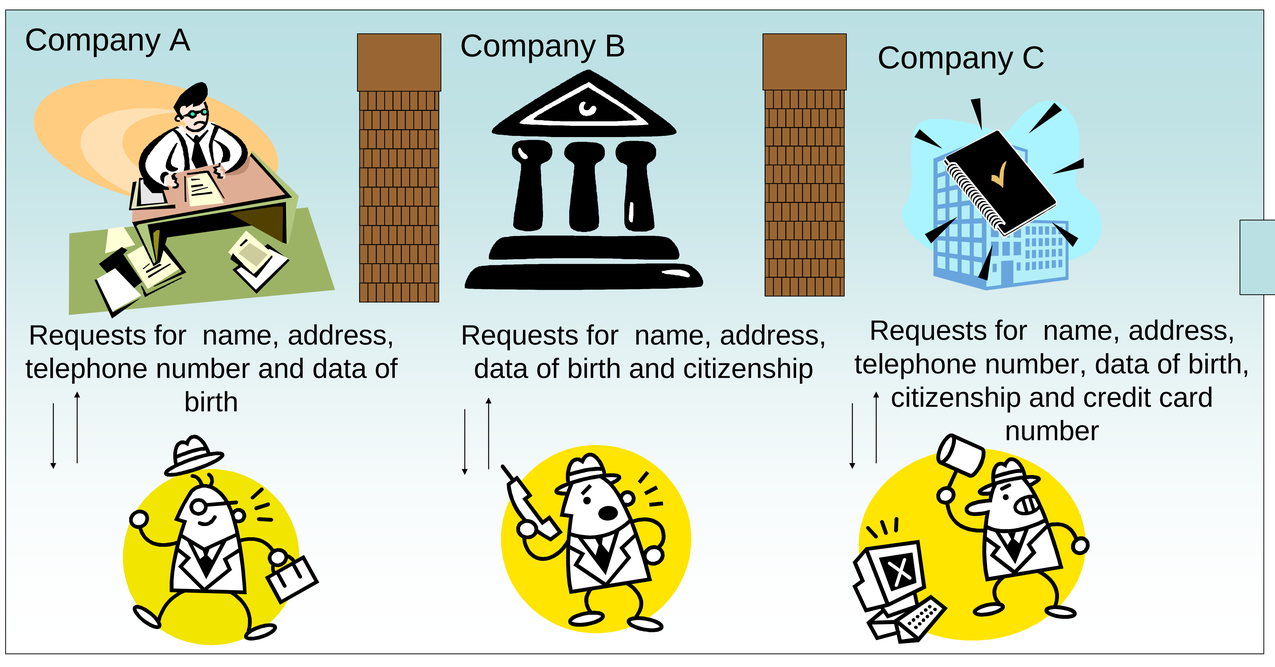


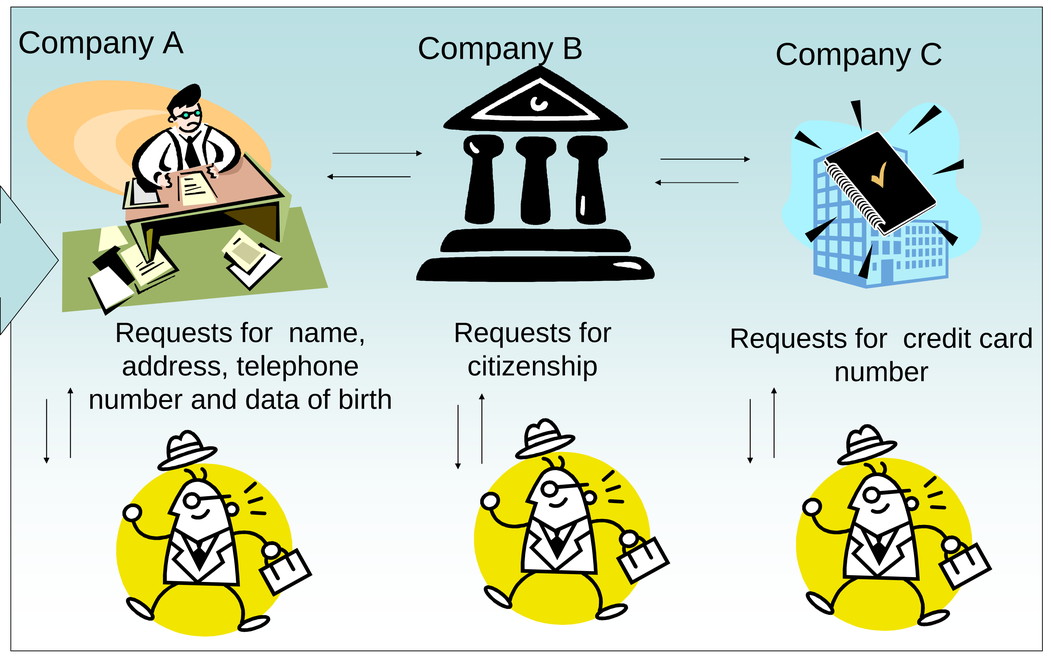
Strategies Support:

- **Sensitive policies protection:** disclosure policies logically linked
- **Negotiation similarity:** negotiation caching techniques
- **Previous successful negotiations:** trust tickets

Sharing Attributes in a Federation:

- Expressing privacy preferences in attributes
- Federation member hierarchy





PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center