



University of  
Milan

## Trust- X: A trust Negotiation proposal

E. Bertino  
Purdue University  
and Cerias

E. Ferrari  
University of Insubria,  
Como, Italy

A. C. Squicciarini  
University of Milan,  
Milan, Italy

### Who can you trust?

- Can you trust strangers?
- Who do you trust online?
- How could you gain the trust of strangers online?
- What must strangers do to gain your trust online?

### 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.

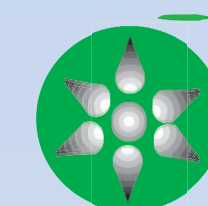
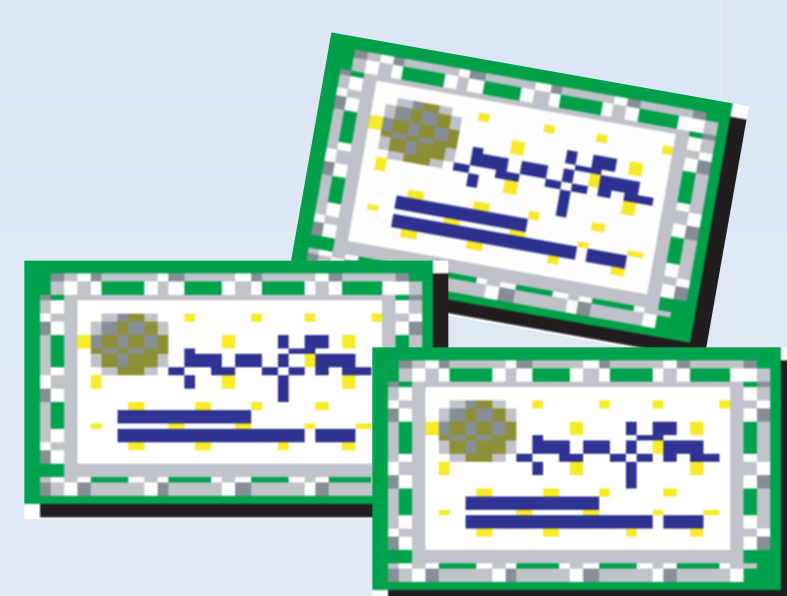
### Building blocks :

#### 1. Subject Credentials

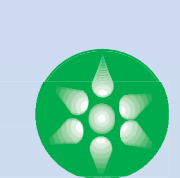
assertions about the credential owner issued by a Certification Authority

#### 2. Disclosure policies

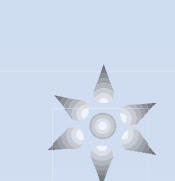
statements expressing trust requirements by means of credential combinations, protecting access to resources, sensitive information and disclosure of sensitive credentials.



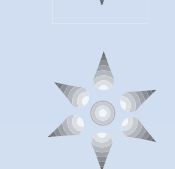
Our proposal: the **Trust- X** system, a comprehensive XML based framework for trust negotiations including:



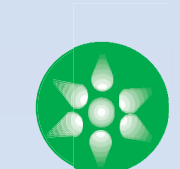
**X-TNL**....the language , able to handle multiple and heterogeneous certificate specification:



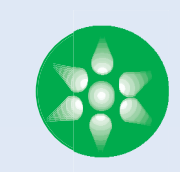
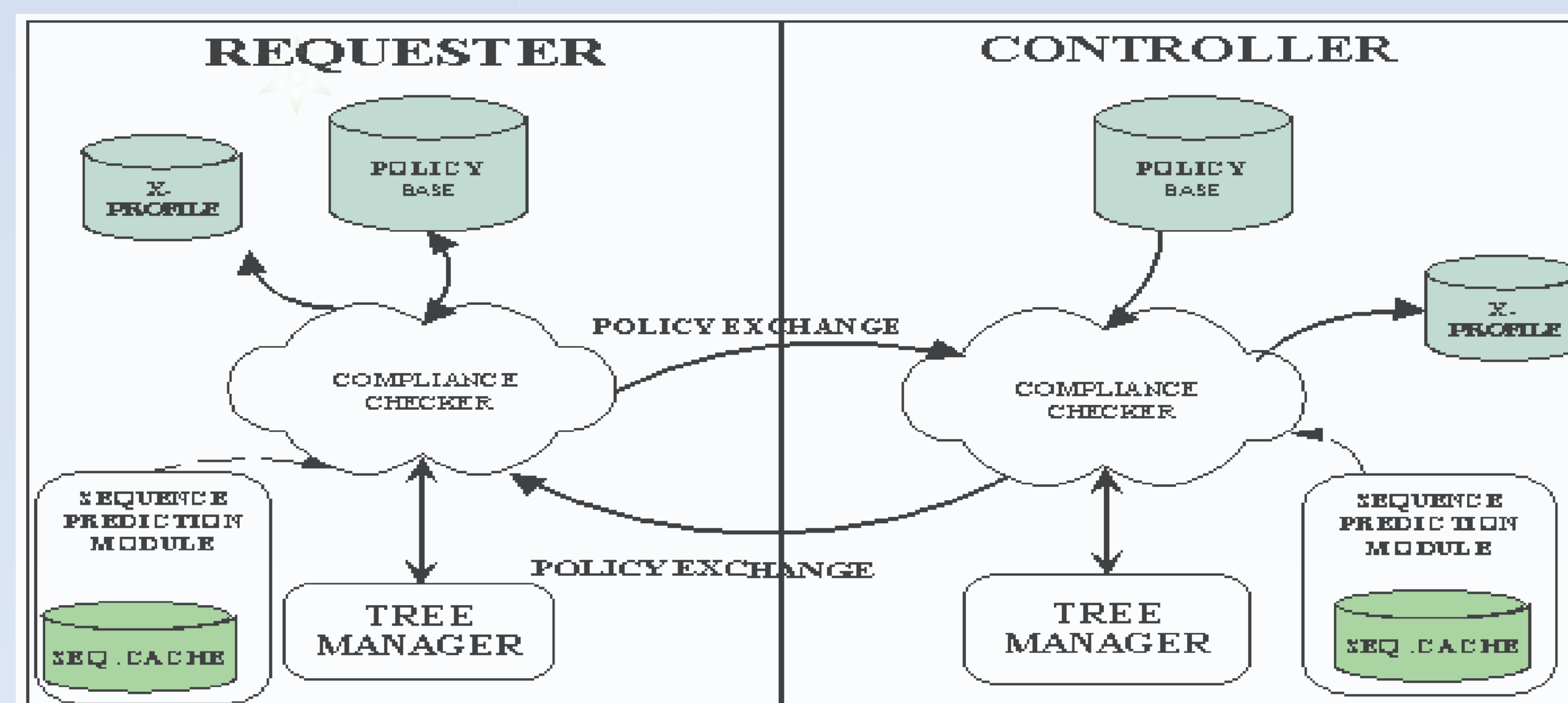
Credential



Declarations

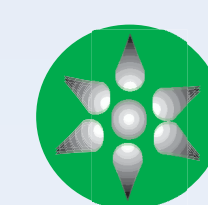


System architecture



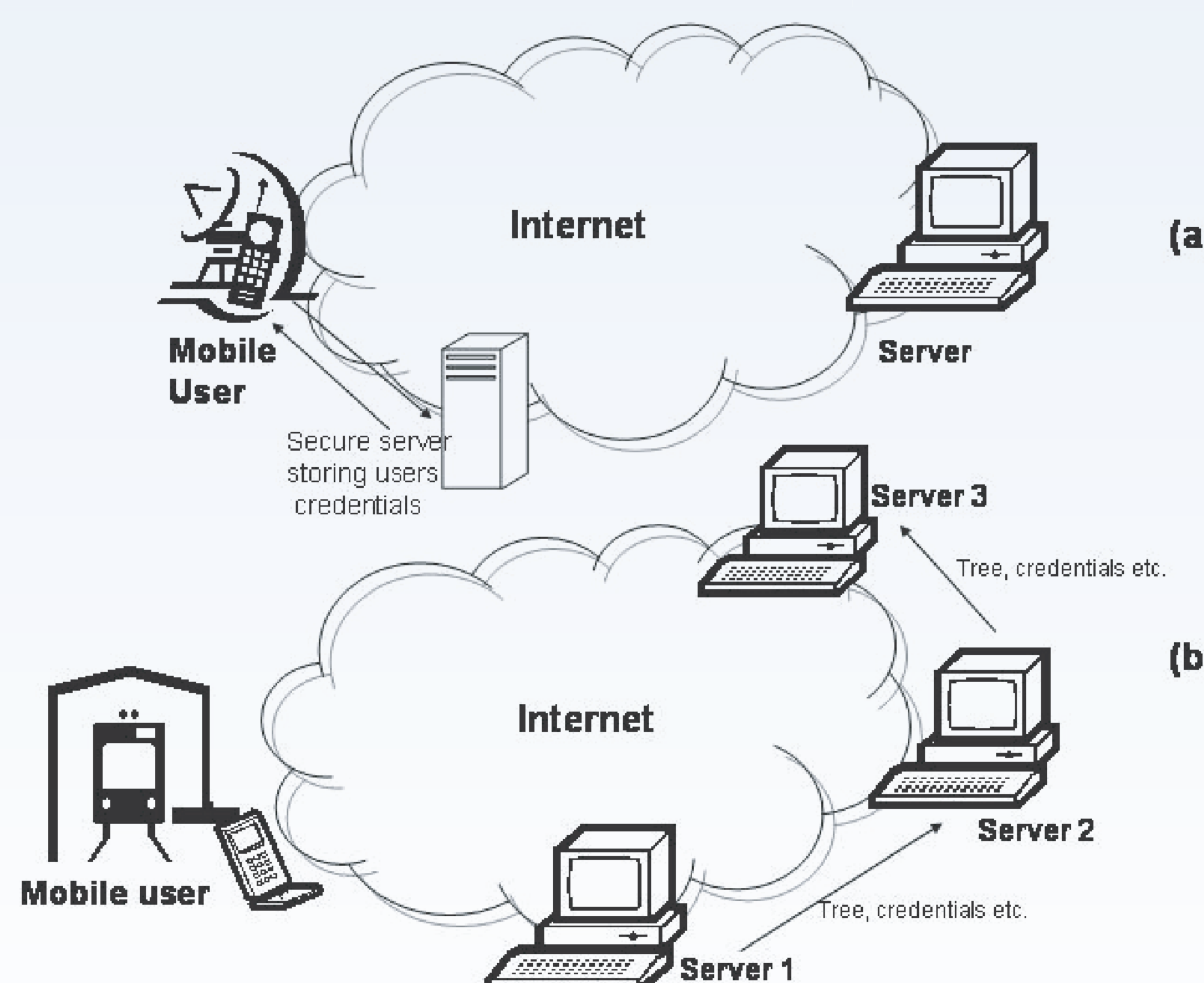
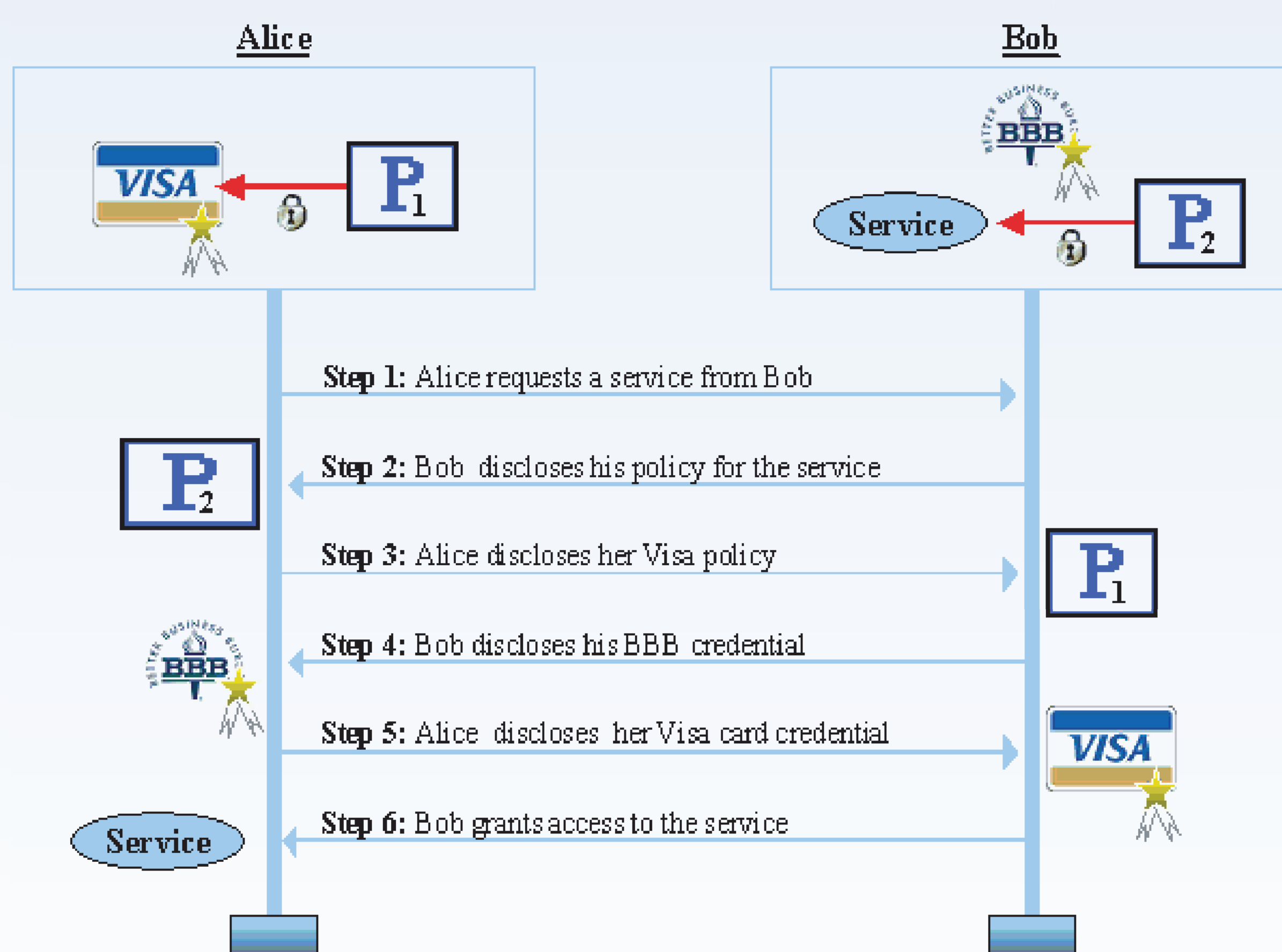
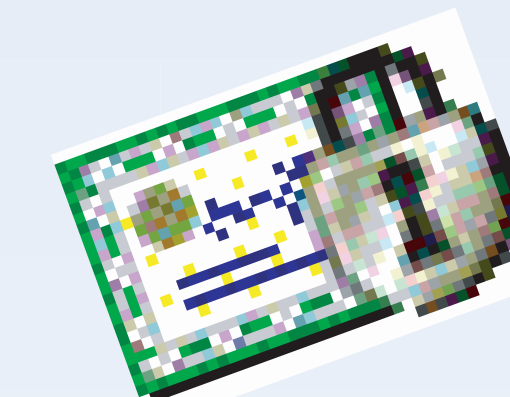
Strategies support

- Sensitive policies protection...protection needs organized in several disclosure policies logically linked and gradually disclosed during the negotiation
- Negotiation similarity... negotiation caching techniques
- Previous successful negotiations.. trust tickets



How about privacy?

- Privacy-preserving negotiation techniques
- Integration with P3P platform
- Partial disclosure of a credential during negotiation process for protecting sensitive elements in a differentiated way



.....What's next.....

- Multi party negotiations
- Recovery mechanisms for recovering from failed or suspended negotiations
- Mobile negotiations
- Full integration with P3P platform, version 1.1.