Creating a Smart Space for Learning

Automated Negotiation of Authentication and Authorization

Daniel Olmedilla, L3S Research Center

Information Society Technologies (ist) PROGRAMME

EU Review, Vienna, 27/05/2005

Motivation: Buying in Internet

Bob wants to access an electronic AI book at "E-Book Store" (a web site he found while surfing in Internet)

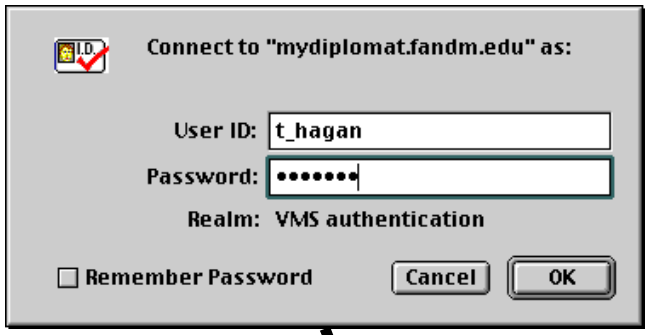
Previously, E-Book requires Bob to register providing full name, age, complete address, telephone and e-mail

Bob does not mind to give his full name and age but he does not like to provide his complete address, telephone and e-mail. However, he does not have any other option so he does it (although he does not provide his real address and telephone).

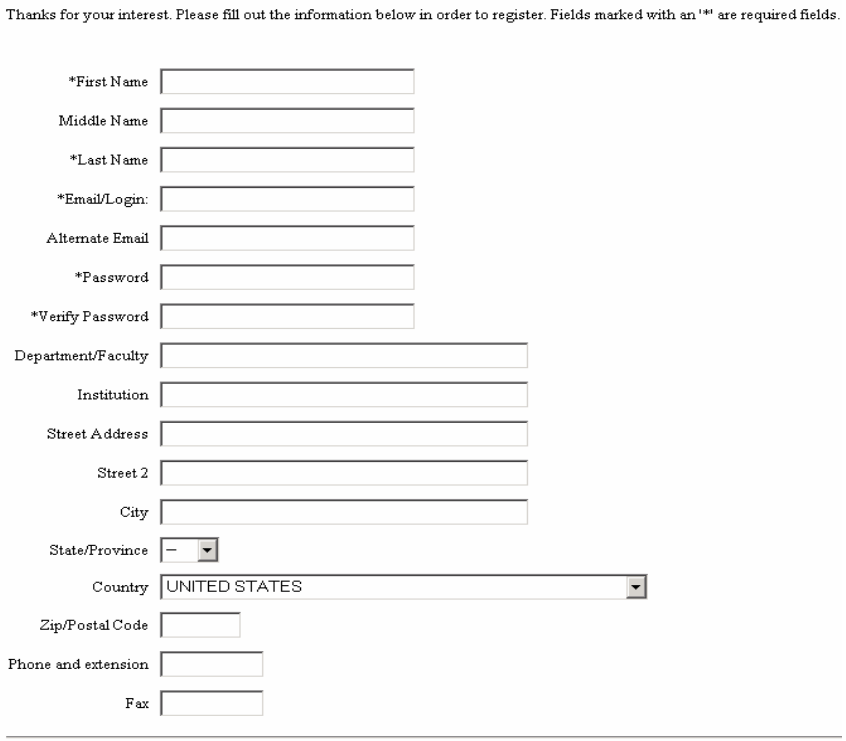
E-Book sells that book. Therefore now it asks Bob to provide his credit card information. Bob would not mind to buy the book because it is not too expensive and he is really interested in reading it. However, he has never heard about E-Book so he decides to not buy it

Traditional Access Control for Decentralized Systems

Assumption: I already know you---you have a local account!



Not a member?



Requirements

Systems

Traditional distributed environments

- Close environments: providers and requesters are known in advance
- Server must trust the client: unidirectional (registration)

WWW, P2P, GRID: dynamic networks

- Nodes are usually not known in advance
- Trust between strangers is needed
- Bi-directional access control required

Users

Do not want to register at any site (tedious task)

Want control over what information they disclose and to set levels of privacy

- E.g. My first name has not the same level than my credit card number

Want assurance about what other nodes will do with their information

- They want to know about the other party

Trust Negotiation

Trust is based on parties' **properties**

Every party can define access control policies to control outsiders' access to their sensitive resources

Establish trust **iteratively** and **bilaterally** by the disclosure of certificates and by requests for certificates

Trust Negotiation

Goal → to protect resources from unauthorized access

New approach to establishing trust between strangers

- Initial trust among nodes is not necessary
- No need for registration (or even registration automatically)

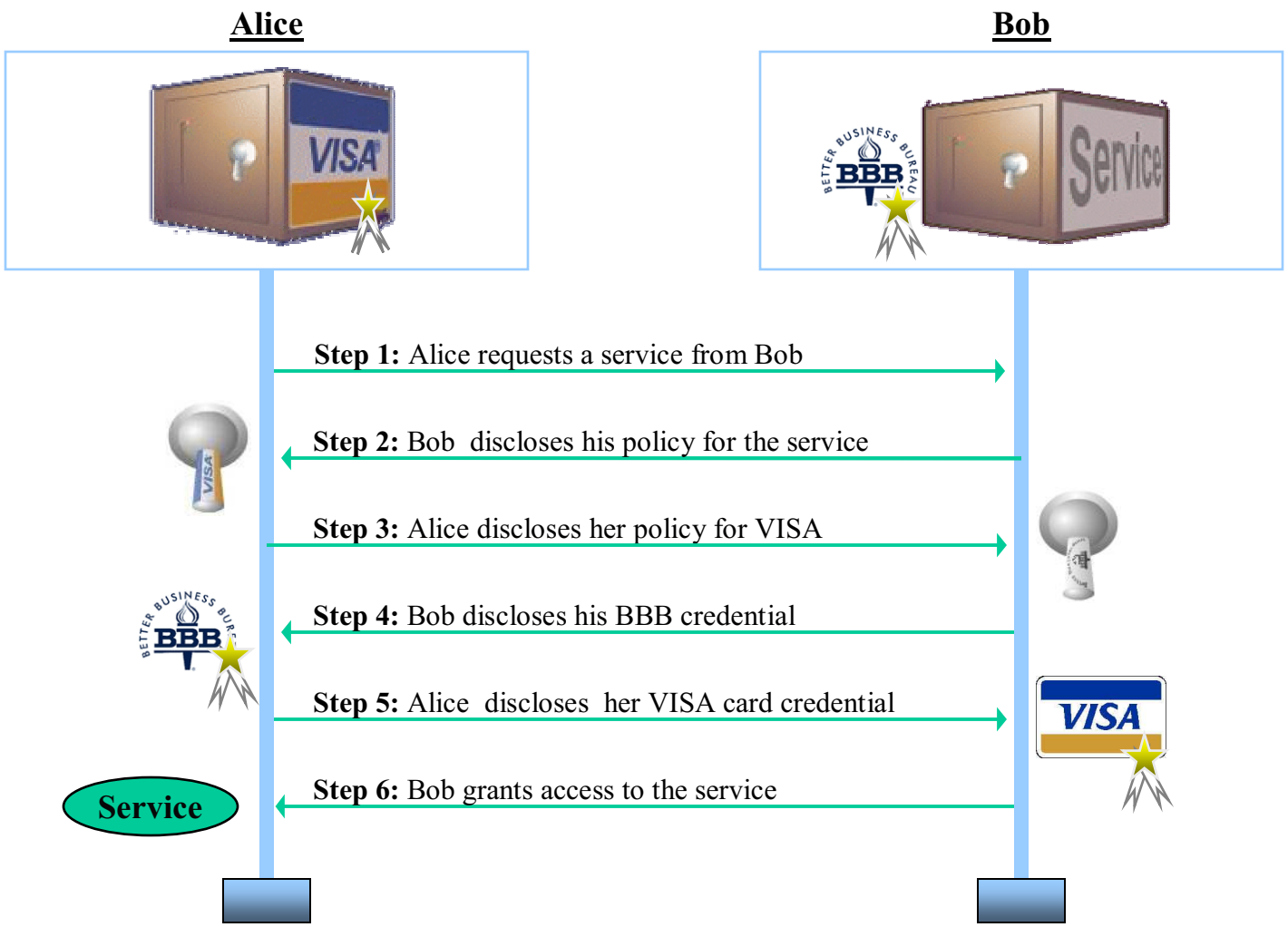
Use of credentials: online analogue to the paper credentials in real life

Negotiation according to policies

- Access control policies can be used in both sides (requester and provider)

Delegation

Trust Negotiation → trust is established gradually through an iterative exchange of digital credentials


Alice
Bob
VISA
BBB
Service
Step 1: Alice requests a service from Bob
Step 2: Bob discloses his policy for the service
Step 3: Alice discloses her policy for VISA
Step 4: Bob discloses his BBB credential
Step 5: Alice discloses her VISA card credential
Step 6: Bob grants access to the service
Service

Credentials and Policies

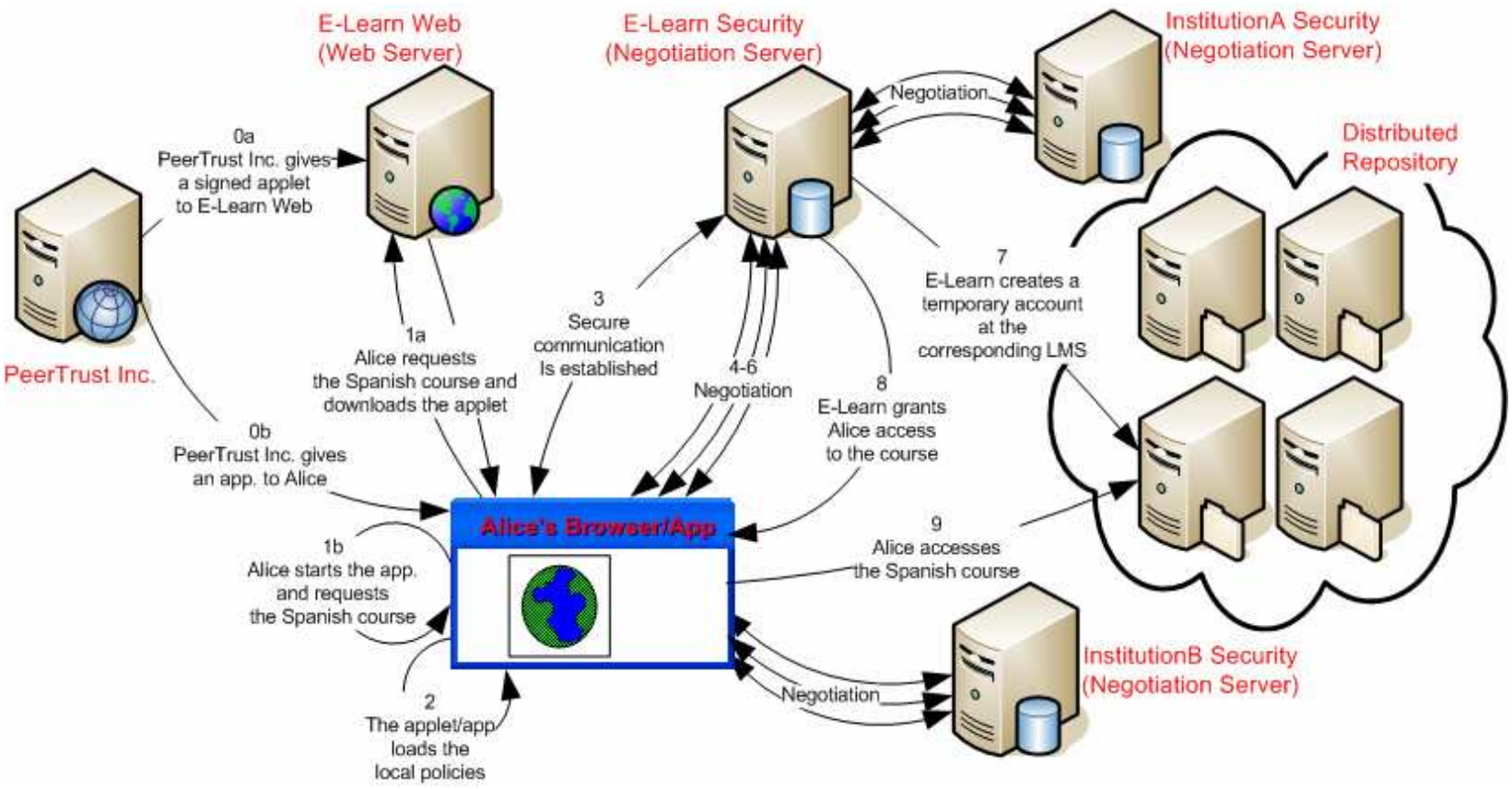
Property-based credentials

- Describe one or more properties / attributes of the owner asserted by the issuer, signed with the private key of the issuer
- As credentials contain sensitive information, they are not shown until the other part demonstrates that it is qualified to have such sensitive information
- E.g. student('Alice Smith') @ 'Hanover University'

Access Control Policies

- Protect a resource or a credential
- Specify credentials that the other negotiation participant must provide in order to get access
- Several policies can be involved during the negotiation
- Several policies for the same resource or credential
- Policies can be protected like any other resource
- E.g. freeAccess(Course,User) ← student(User) @ 'Hanover University'

Network Diagram



References

Workshop on Trust Security and Reputation on the SW (in conjunction with ISWC'04):

http://trust.mindswap.org/trustWorkshop/

Security Agent in an Applet

http://www.l3s.de/~olmedilla/projects/trust/applet/instructions.html

Demos

http://www.l3s.de/~olmedilla/projects/trust/demos/demoSequenceHigh.html

http://www.l3s.de/~olmedilla/projects/trust/demos/demoTreeHigh.html

http://www.l3s.de/~olmedilla/projects/trust/demos/demoSequenceHigh.html

Live Negotiation

Publications

No Registration Needed: How to Use Declarative Policies and Negotiation to Access Sensitive Resources on the Semantic Web
European Semantic Web Symposium

The Pudding of Trust
IEEE Intelligent Systems Journal, Vol. 19(5)

Driving and Monitoring Provisional Trust Negotiation with Metapolicies
IEEE 6th International Workshop on Policies for Distributed Systems and Networks (POLICY 2005)

Negotiating Trust on the Grid
2nd Workshop on Semantics in P2P and Grid Computing at the 13th International World Wide Web Conference

Ontology-Based Policy Specification and Management
European Semantic Web Conference

Discovery and Contracting of Semantic Web Services
W3C Workshop on Frameworks for Semantic in Web Services

Questions

THANKS !

QUESTIONS ?