

An Interdomain PKI Model Based on Trust Lists

Helena Rifà Pous
Jordi Herrera Joancomartí

Outline

- PKI challenges
- Trust Models
- Our proposal
- Use case
- Conclusions

PKI challenges

- **PKI penetration**
 - Server side applications (i.e. SSL, SSH protocols)
 - eID card
- **PKI penetration != usage**
- **Trust** on CAs depends on the scenario of use.
 - Users have to manage the trust.
- **Technical interoperability**
 - Implementation issues (open standards)
 - Certificate path verification
 - Certificate status
- **Legal and political interoperability**

Trust Models

Single CA
Hierarchical model
Mesh PKI

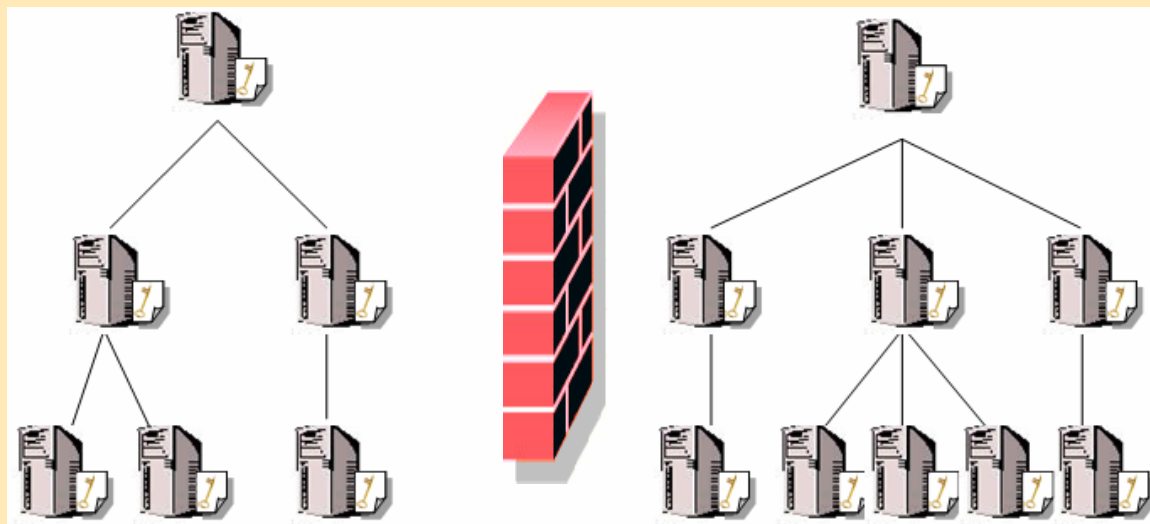
Bridge CA
Bridge VA
Trust Lists

Single CA



- Non scalable
- Politically unviable

Hierarchical model



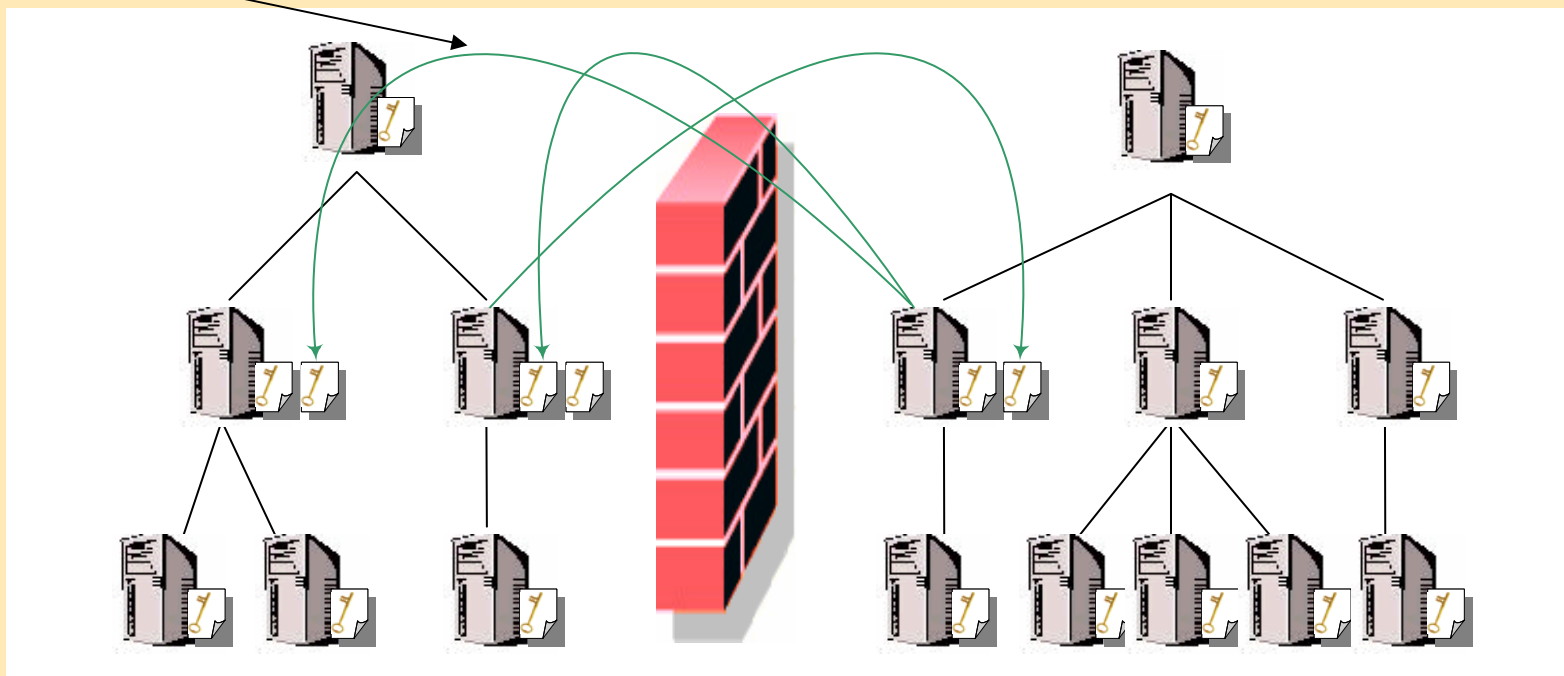
- Interconnected Trust Islands

Trust Models

Single CA
Hierarchical model
Mesh PKI

Bridge CA
Bridge VA
Trust Lists

cross-certify Cross-certificate model



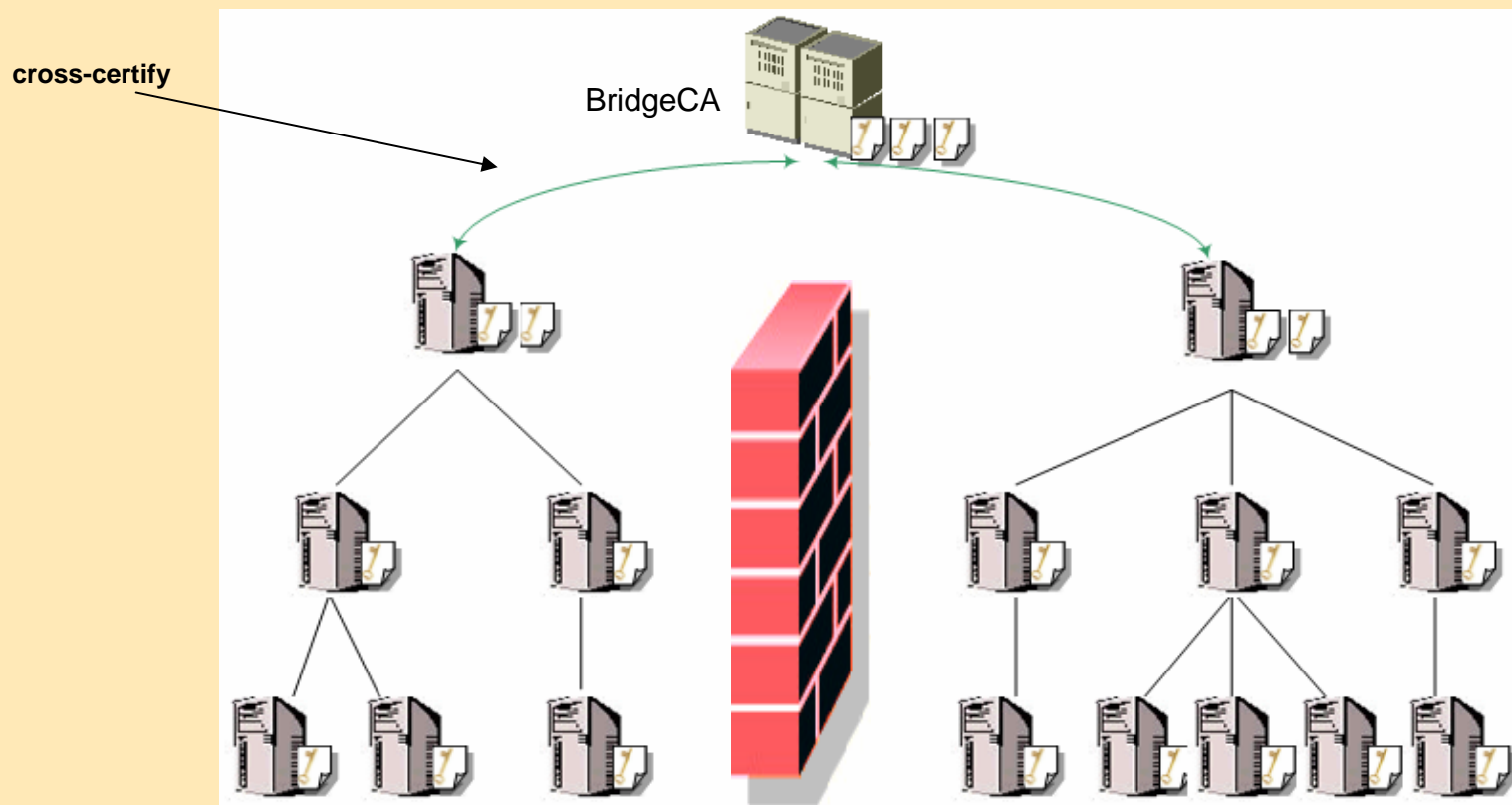
- Scalability problems
- Complex implementations

Trust Models

Single CA
Hierarchical model
Mesh PKI

Bridge CA
Bridge VA
Trust Lists

BridgeCA model



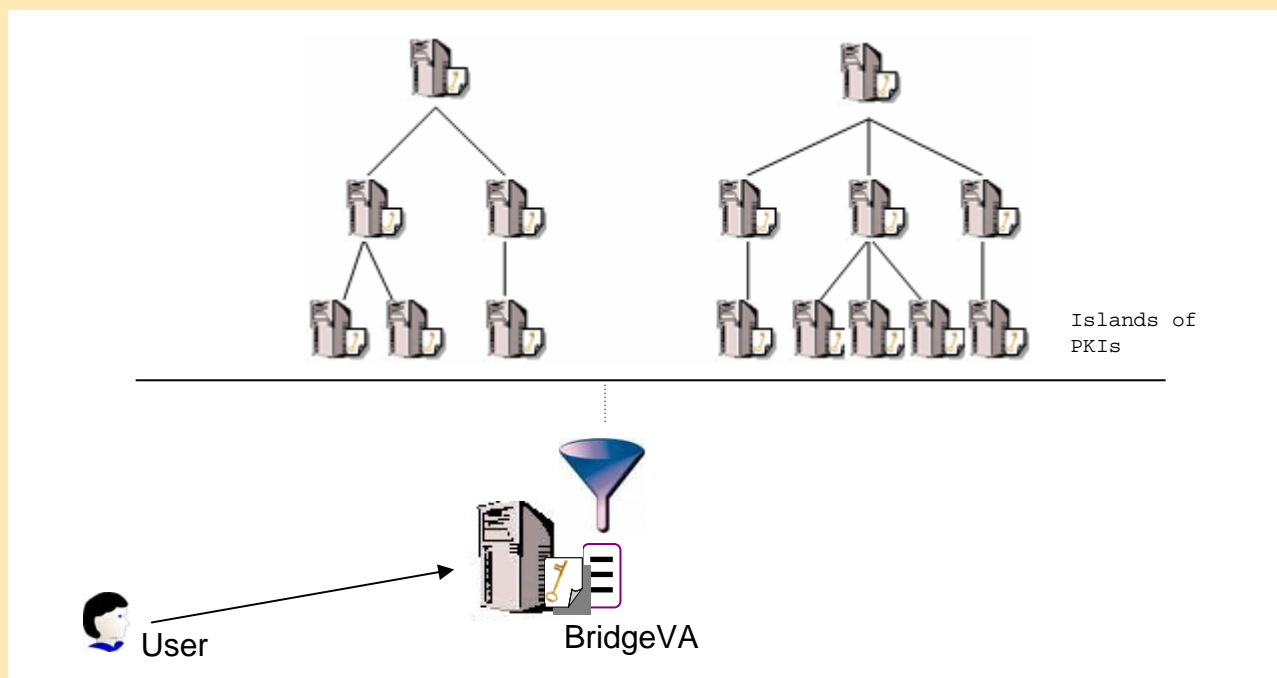
- The construction of certification paths is complex

Trust Models

Single CA
Hierarchical model
Mesh PKI

Bridge CA
Bridge VA
Trust Lists

Bridge VA



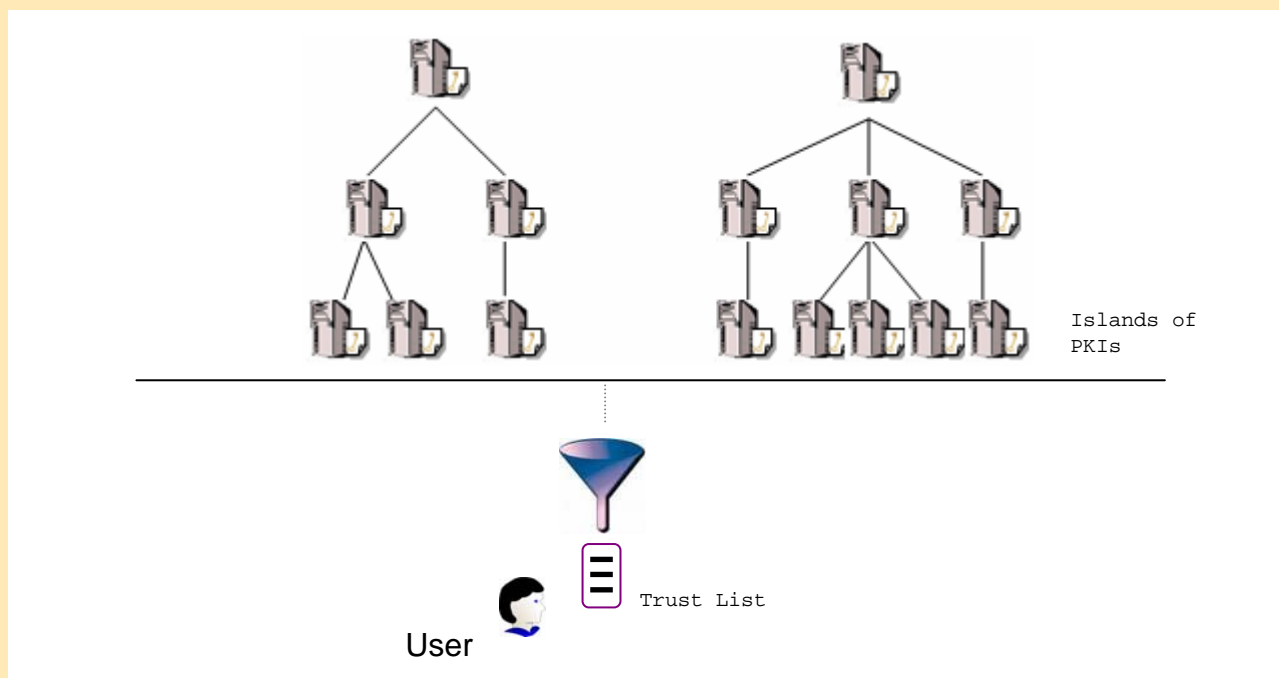
- Rigid model
- Trust is an attribute related with a relation and context

Trust Models

Single CA
Hierarchical model
Mesh PKI

Bridge CA
Bridge VA
Trust Lists

Trust List model



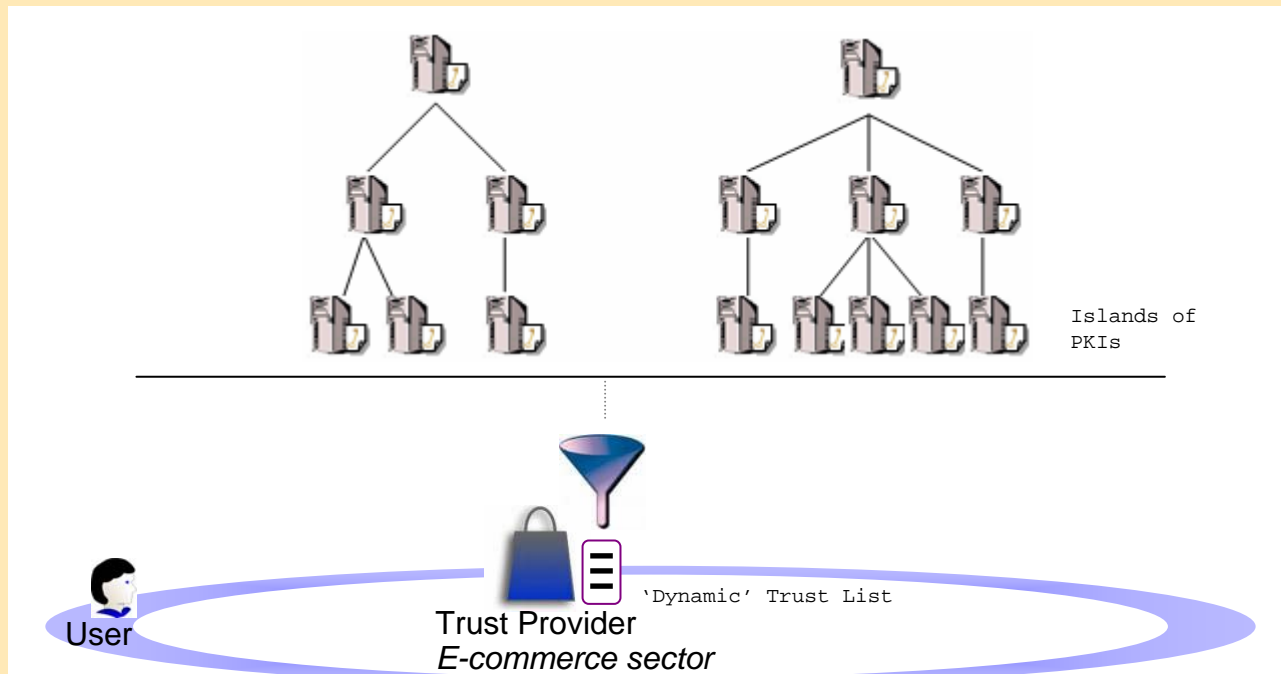
- Lack of qualifying information
- Dissemination and management

Open Issues





- Determining the **quality** of the certificate, which can be usually derived from the certificate policy
- Deciding if the certificate is **trustworthy** for the purpose at hand.
- Processing **certification paths**, that is, finding an ordered sequence of certificates from the end entity certificate to a trust anchor.

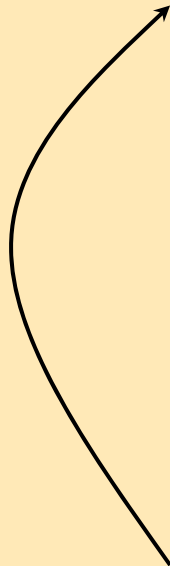
System Architecture: Elements

- **Trust Providers (TP)** are well known entities that have accredited political, legal or social impact (i.e. the Ministry of Law or recognized private enterprise). They **manage lists of CA** certificates that they consider **reliable** and that have the required quality for being used in some specific actions.

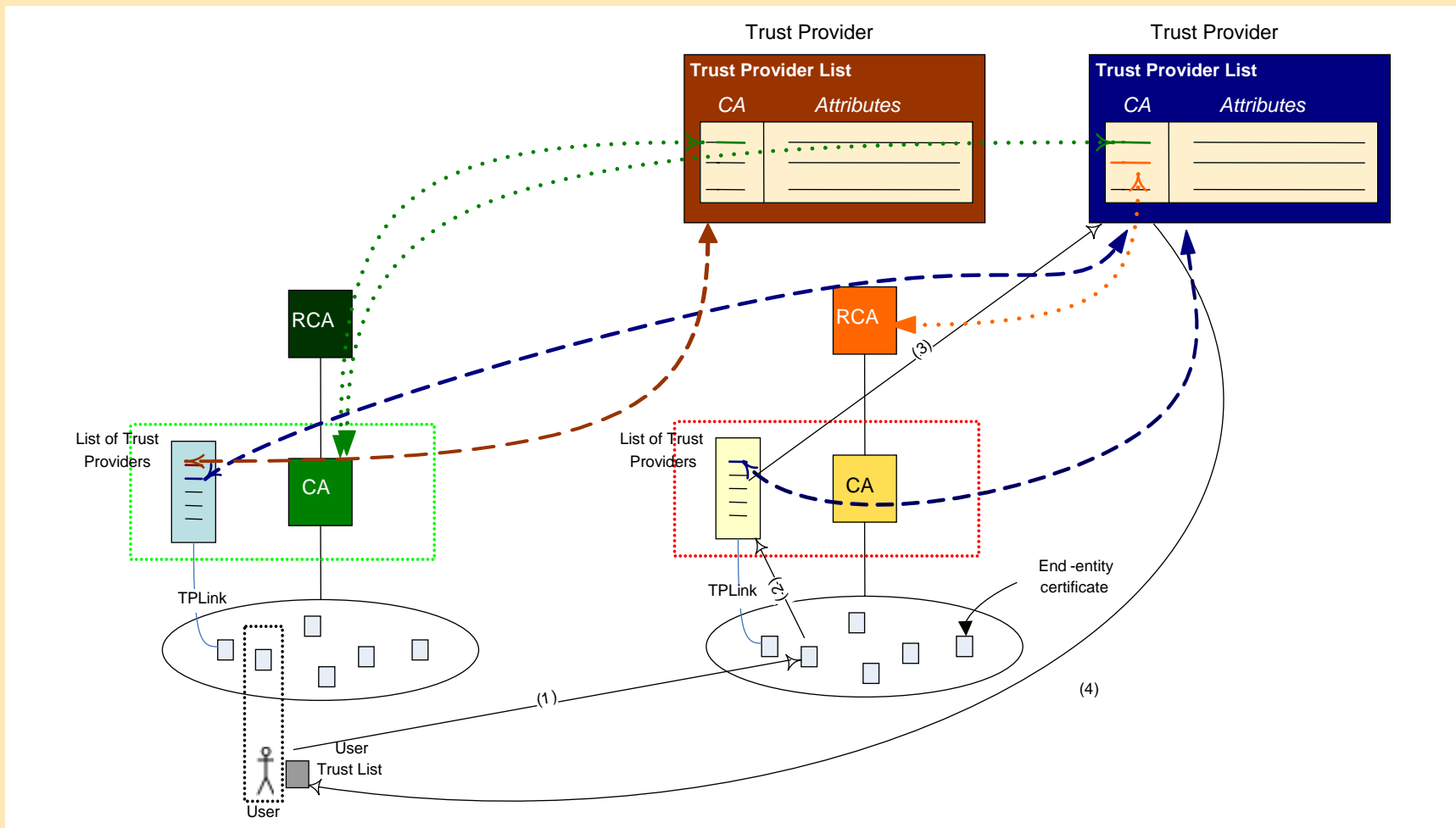


System Architecture: Elements

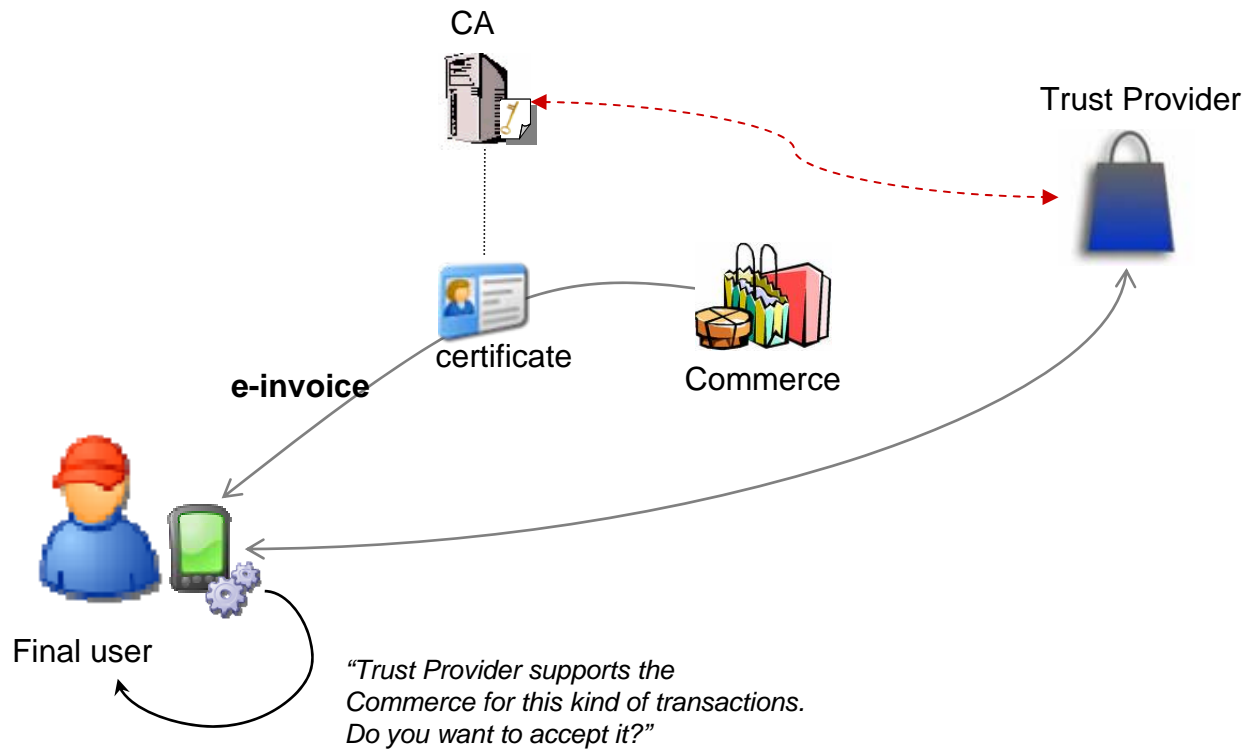
Element	List	Contents
Certificate 	Trust Provider Link	URL to the List of Trust Providers
CA 	List of Trust Providers	Trust Providers (Identifiers + Description)
Trust Provider 	Trust List	Info of the Owner CA certificate identifiers + qualifiers
End-Entity 	Trust List + Trust List Enforcement Engine	Info of the Owner CA certificate identifiers + qualifiers



System Architecture



Use case



Conclusions

- Trust model based on **trust lists**
 - **Categorized** trust lists
 - Trust management using **natural language**
- The **trust anchor** is the **TP**, not the CA
 - TPs are well known organizations close to the users
- Dissemination and promotion of TPs through a **certificate extension**

Thanks!

Helena Rifà Pous
hrifa@uoc.edu

