Securing Passive Objects in Mobile Ad-Hoc Peer-to-Peer Networks

Rene Mayrhofer
Institut für Praktische Informatik
Johannes Kepler Universität Linz, Austria

29.6.2003

Outline

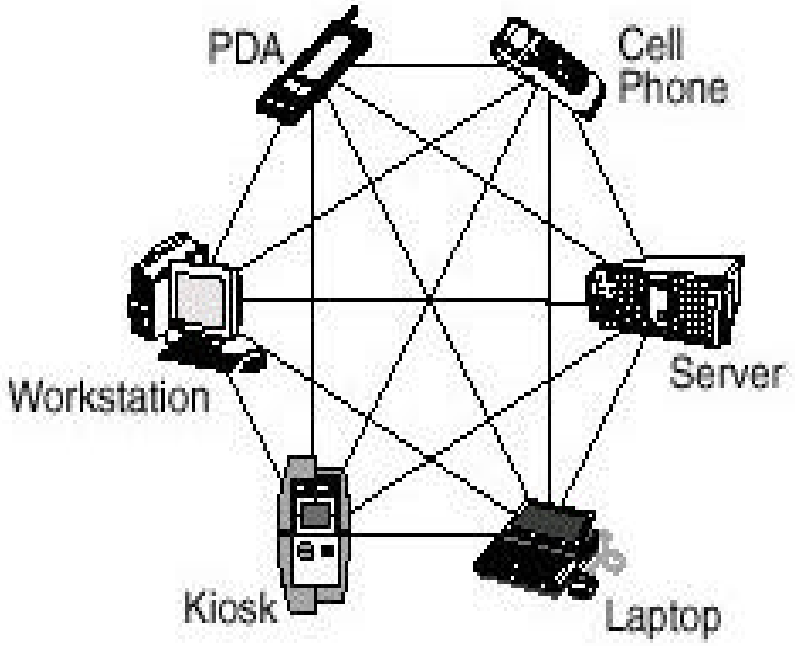
- Introduction: SmartInteraction project
- Passive Objects
- Security architecture
- Protocol
- Security with limited resources

The SmartInteraction project

- Aim: interact with persons, things and places in a natural and non-obtrusive way.
- Base technology: ad-hoc, mobile peer-to-peer networks
- Contribution: software framework

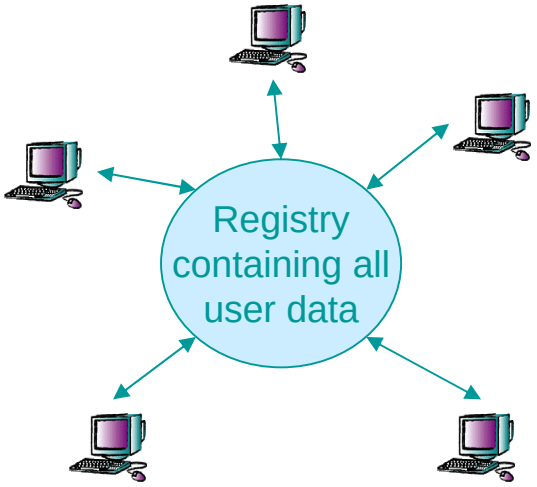
Mobile Ad-Hoc Peer-to-Peer Networks

- Direct communication between peers
- Peers are mobile
- Interaction upon spatial proximity of devices
- No single central authority (e.g. CA)
- Interaction happens ad-hoc without previous information exchange between devices (e.g. no pre-shared keys)

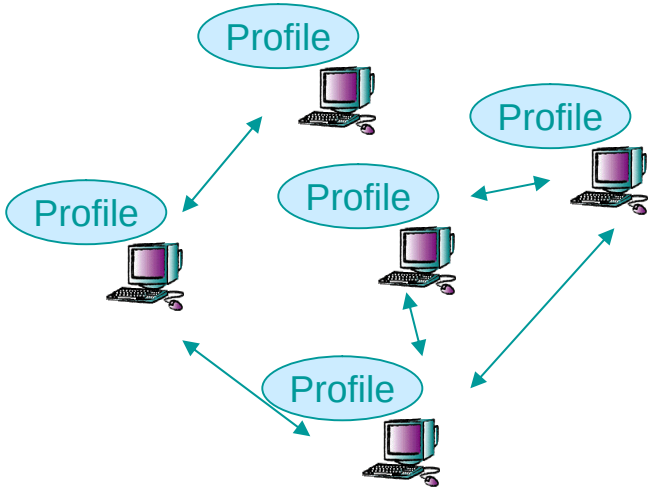


Profiles

Storing user data and matching between users can be done using a registry or by saving a profile at each user‘s device



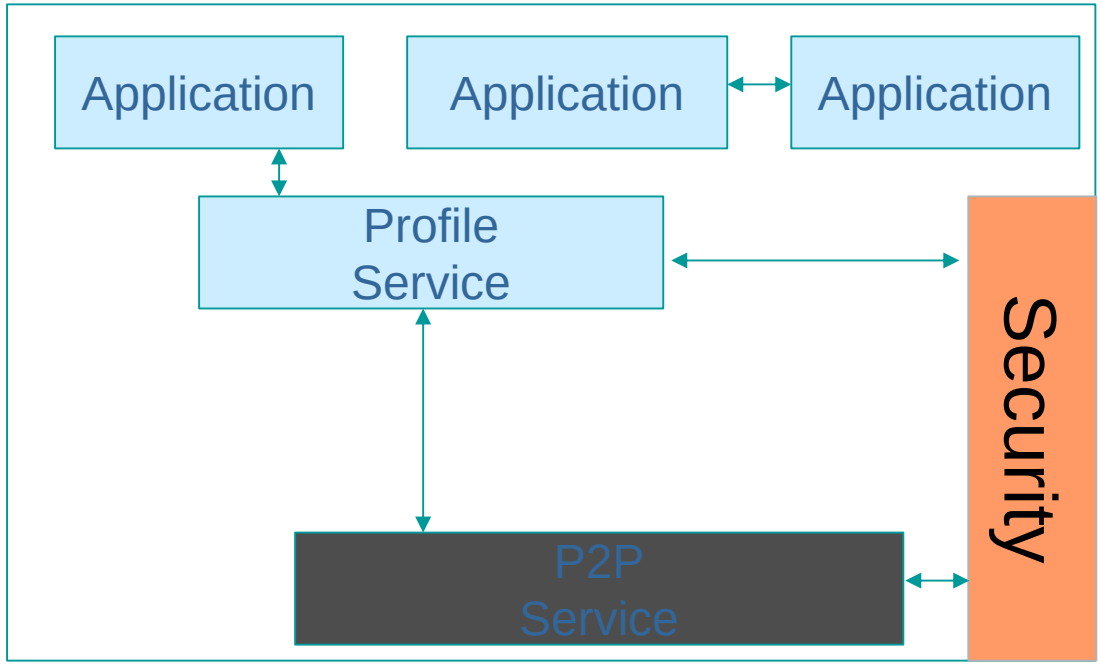
- Requires communication infrastructure to registry
- Registry decides whether two users match



- Ad-hoc communication
- User device decides whether another user matches or not

Framework component model

- Component-based architecture offers more flexibility on embedded devices
- Security component allows applications encrypted, signed but completely transparent communication



Outline

- Introduction: SmartInteraction project
- Passive Objects
- Security architecture
- Protocol
- Security with limited resources

Passive Objects

- Normal peers are complex (CPU, memory, wireless communication technology)
- Natural interaction with real-world objects (places, things) requires integration into the peer-to-peer infrastructure

> *An object is passive with regards to to executing custom code, i.e. it does not have processing power that could be exploited to run parts of a custom software. Objects are required to have a unique identification number (*ID*)*

Interacting with Objects

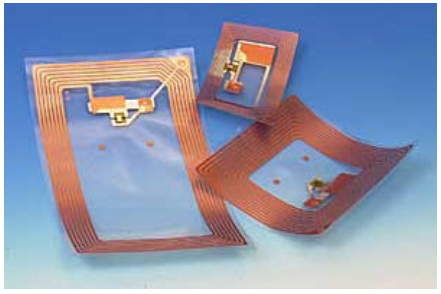
- Since objects are passive, a proxy representing the object is needed for interaction

- Possibilities for proxies in ad-hoc peer-to-peer networks:
  - Local proxy
  - Remote proxy

Examples for Objects

Barcode

RFID
(active)



RFID
(passive)

IrDA

Outline

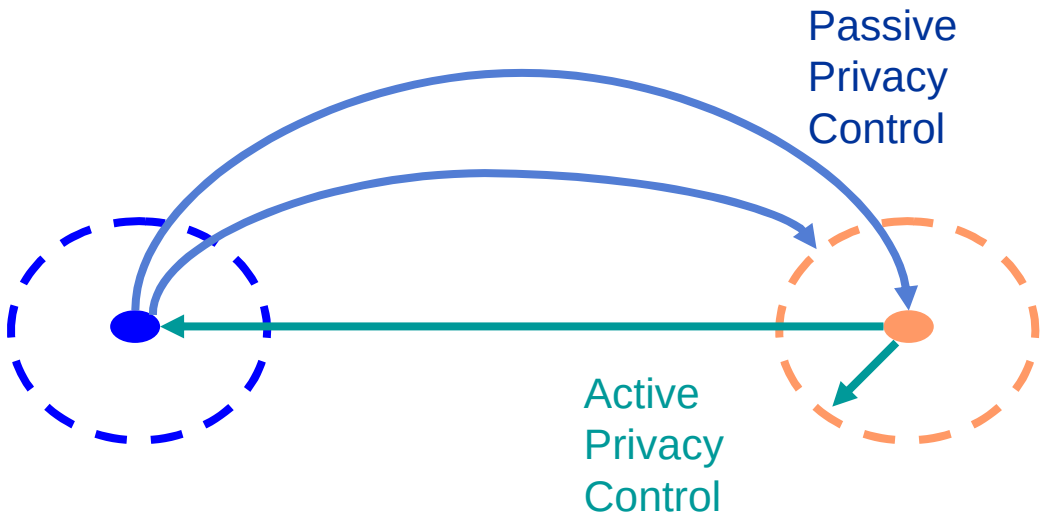
- Introduction: SmartInteraction project
- Passive Objects
- Security architecture
- Protocol
- Security with limited resources

Privacy in Ad-Hoc P2P Systems

- “Passive” Privacy:
  - Don’t bother the user with all incoming information.

  ⇒ Shielding
- “Active” Privacy:
  - Don’t send confidential information to all clients.

  ⇒ Filtering



Requirements

- Active and Passive Privacy measures
- Use of multiple roles per device
- No single central authority / trusted third party
- Verification, validation and authentication done locally
- Allow for local policies
- Techniques that require manual setup or interaction should be optional
- Context-based switching of privacy policies

Used techniques

- Symmetric algorithms for encryption of messages: **AES**
- Asymmetric algorithms for mutual authentication of roles (signatures) and encryption of session keys: **RSA** and **ECC**
- Digest generation for signatures: **SHA-256**
- Certificates for user roles: **X.509v3**
  (Transferred to the device in a bootstrap phase)

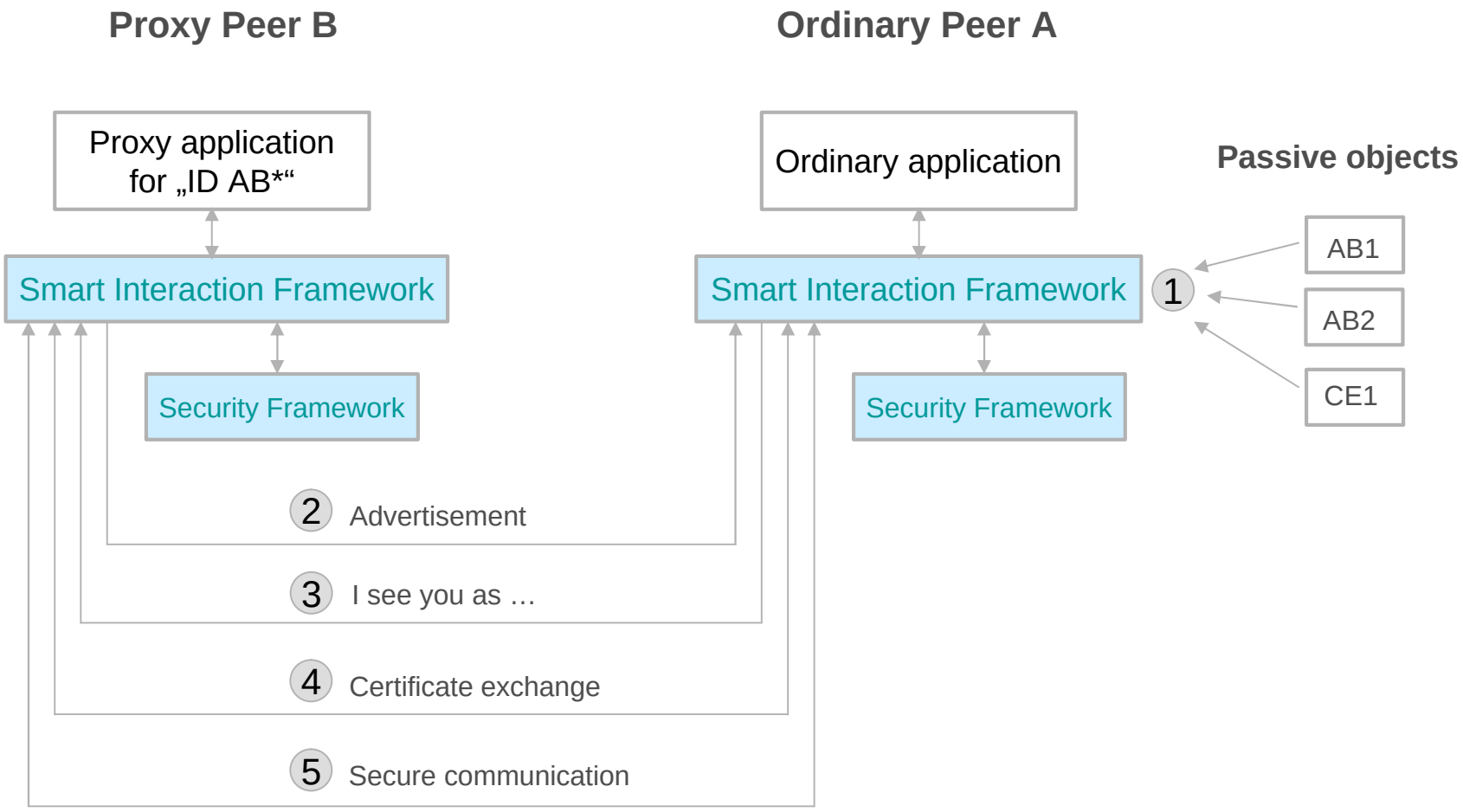
Reason for choosing X.509v3:

- Widely used standard
- Allows definition of custom fields (meta information) in certificate (OpenPGP does not seem to have a standard for that)
- Good tools for private CAs

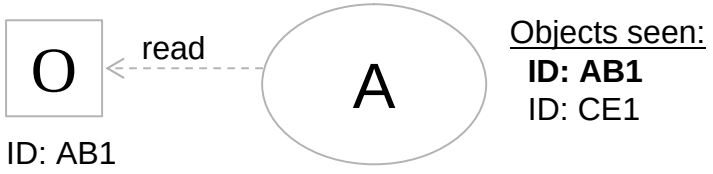
Outline

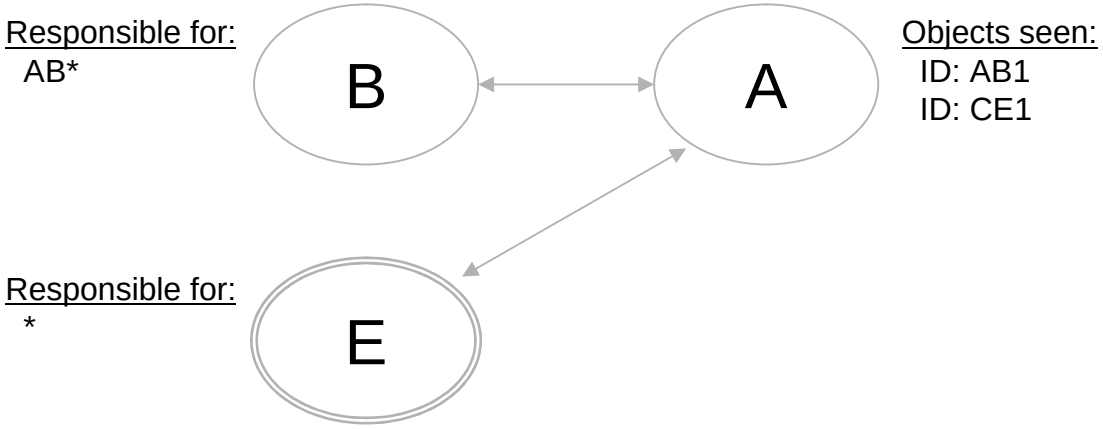
- Introduction: SmartInteraction project
- Passive Objects
- Security architecture
- Protocol
- Security with limited resources

Protocol for Interaction with Passive Objects

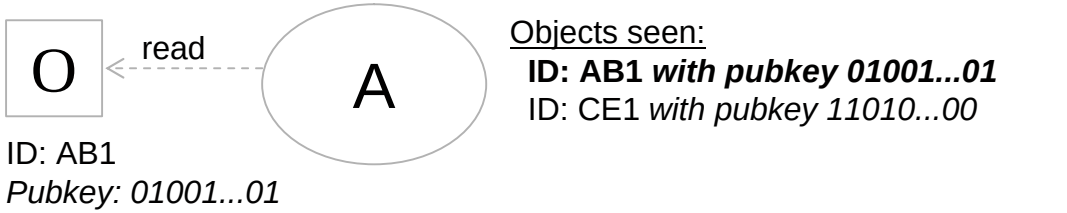


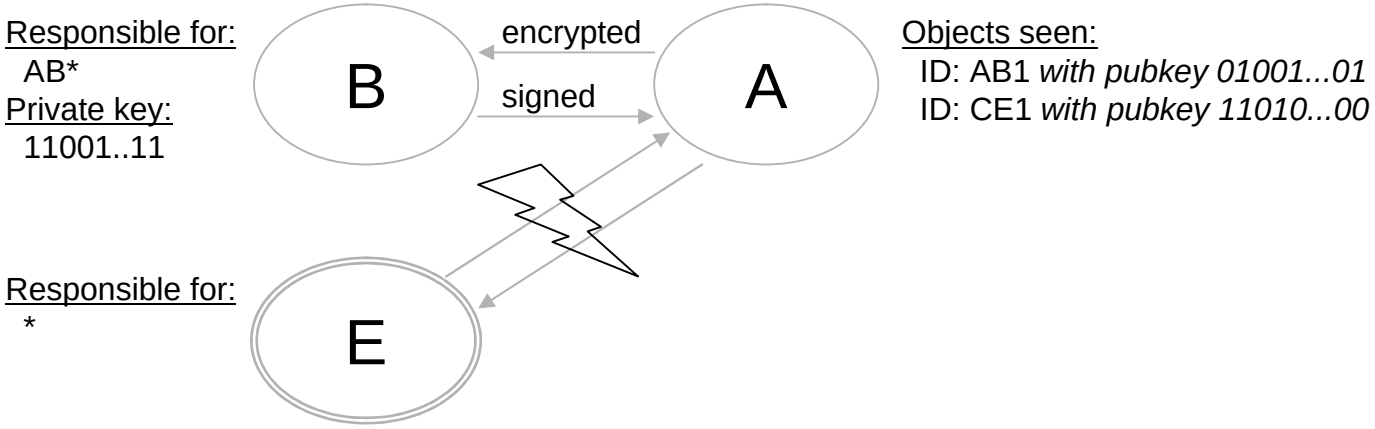
Without Security





With Security





- With **public keys on objects**, peers can validate a proxy‘s claim for responsibility locally.

Outline

- Introduction: SmartInteraction project
- Passive Objects
- Security architecture
- Protocol
- Security with limited resources

Key sizes

- Objects typically have severely limited storage
- E.g. iD2 RFID-Tag has 64 Bytes
- RSA keys with reasonable size do not fit into the available storage

Algorithm	Parameters	Key size [Bytes]
RSA	1024 Bit modulus	**162**
DSA	1024 Bit prime	**442**
ECC	secp160r2 curve	**64**

Run time

	PC	Pocket Loox	Ipaq 3870
AES encryption	23	574,7	680,1
AES decryption	26,4	565,6	541,8
SHA-256 digest	16,4	306,9	770,3
RSA sign	73,8	360,2	421,6
RSA verify	2,2	142,5	187,8
RSA encrypt	6	34,6	151,8
RSA decrypt	48	132,5	254,3
EC sign	35,8	**8958,3**	**6622**
EC verify	51,6	**17138**	**11389,6**

Summary

- SmartInteraction project supports natural interaction between persons, places and things
- Peer-to-peer paradigm allows flexibility and fault-tolerance
- For interaction with real-world objects, integration into peer-to-peer infrastructure is necessary
- Objects are represented by proxies
- Passive objects without own processing power are unable to participate in authentication process between peers and proxies
- Public keys stored on read-only objects allow ordinary peers to validate proxy peers which possess the corresponding private key
- If storage size of objects is a problem, ECC keys can be used

- This architecture allows the use of standard, well-known cryptographic techniques for integrating passive objects into ad-hoc, mobile peer-to-peer systems without a single central authority.

Thank you for your attention !