Beyond Anonymity - Pseudonyms

- Person pseudonym
- Role pseudonym
- Relationship pseudonym
- Role-relationship pseudonym
- Transaction pseudonym
Beyond Anonymity - Pseudonyms

- person pseudonym
- role pseudonym
- relationship pseudonym
- role-relationship pseudonym
- transaction pseudonym

linkability -> anonymity
The Problem

initiator

connection request

pseudonym $P_R$

choose pseudonym $(P_R)$

pseudonym $P_I$

responders

choose pseudonym
A Solution?

initiator

connection request, ID_R

choose pseudonym (ID_R)

pseudonym P_R, ID_R

choose pseudonym (P_R)

pseudonym P_I, ID_I

responder
Open questions

• ID - properties?
  – Spoofing?
  – Randomly distributed over a large range?
  – Linkability?
  – Cryptography and DoS?
• Reaction on wrong $P_I$?
• Other approaches to the problem?