Recent Advances in Network Security

IDEMIX:
Pseudonomity for e-Transaction

January 19th, 2004

Presenter: Michael Nordhoff

Overview

1. Introduction
2. Ordinary certificates
3. Privacy – meaning / significance
4. Anonymity / Pseudonymity
5. Certificates Lifecycle / Role of CAs
6. IDEMIX
   - Project and Features
   - Example Scenarios
7. Problems
8. Resume

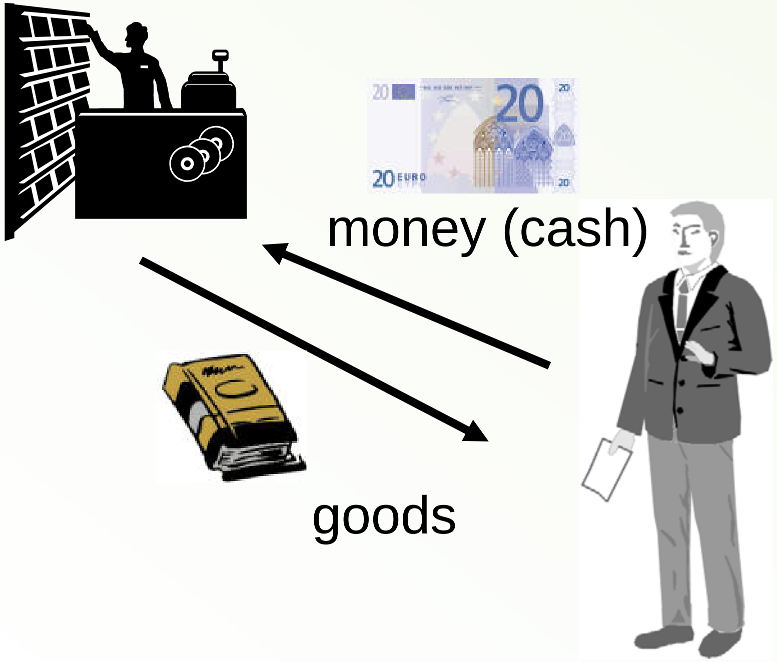
Introduction

- e-transaction & e-commerce more and more important
- without security: lack of acceptance
- solution: certificates with private/public key algorithms
- NOT solved: personal data protection
- keeping privacy with

  pseudonymous / anonymous certificates

Introduction (2)

usual purchase in a shop



no exchange of information

=> full privacy

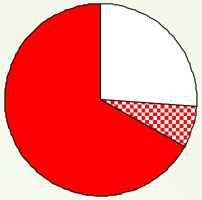
e-shopping via internet

sends lots of private information:

- credit card data (name, no, …)
- delivery address
- email address, phone number
- …

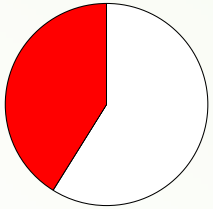
User Concerns regarding Privacy on the Internet

- being extremely/very **concerned** about divulging personal information online



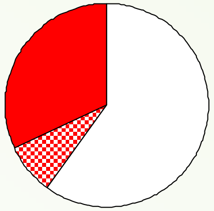
67 % - 74 %

41 %



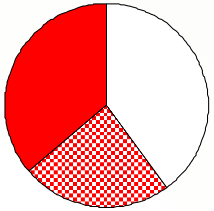
- have **left websites** that required registration information

- having entered **fake registration** information



32 % - 40 %

24 % - 64 %

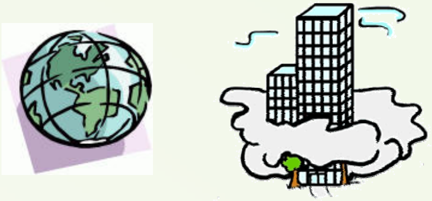


- having **refrained from shopping** online due to privacy concerns

[KOSCH03]

Different Primary Interests:

User /
Customer



E-Commerce Provider /
Seller

- wants to have control on use of own personal data
- wants to keep privacy/ anonymity

- wants to get the money
- wants to know the personal data of the liable person

Interests compatible or incompatible ?

Satisfying Sellers Interests:
Ordinary Certificates

- “A digital certificate is simply a statement signed by an independent and trusted third party. “[THAW]

Certificate
Of Authenticity

The bearer of this document holds title to Series 3 NYPD Fallen Heroes of the 9-11 Heroes Collection.

9-11

Serial # 00000058

- first standardized by ITU
- later modified by IETF (RFC 2459)

Ordinary digit. Certificates

- contents
  - subject name & other identity details
    (i.e. personal ID, email address, web site URL)
  - public key of identity
  - issuer (Certification Authority - CA)
  - validity period
  - attributes

- signed by the CA

Example: Certificate

```
Version: 0 (0x0)
      Serial Number: 0 (0x0)
      Signature Algorithm: md5withRSAEncryption
      Issuer: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
             OU=Certification Services, CN=www.thawte.com,
             Email=webmaster@thawte.com
      Validity
         Not Before: Nov 14 17:15:25 1996 GMT
         Not After: Dec 14 17:15:25 1996 GMT
      Subject: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
              OU=Certification Services, CN=www.thawte.com,
              Email=webmaster@thawte.com
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
             Modulus:
                00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:
                …
                a5:94:ac:8a:67
             Exponent: 65537 (0x10001)
   Signature Algorithm: md5withRSAEncryption
      7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:78:2b:a4:
      …
      ee:bc:0e:fe:fc:f8:9b:9d:70:e3
```

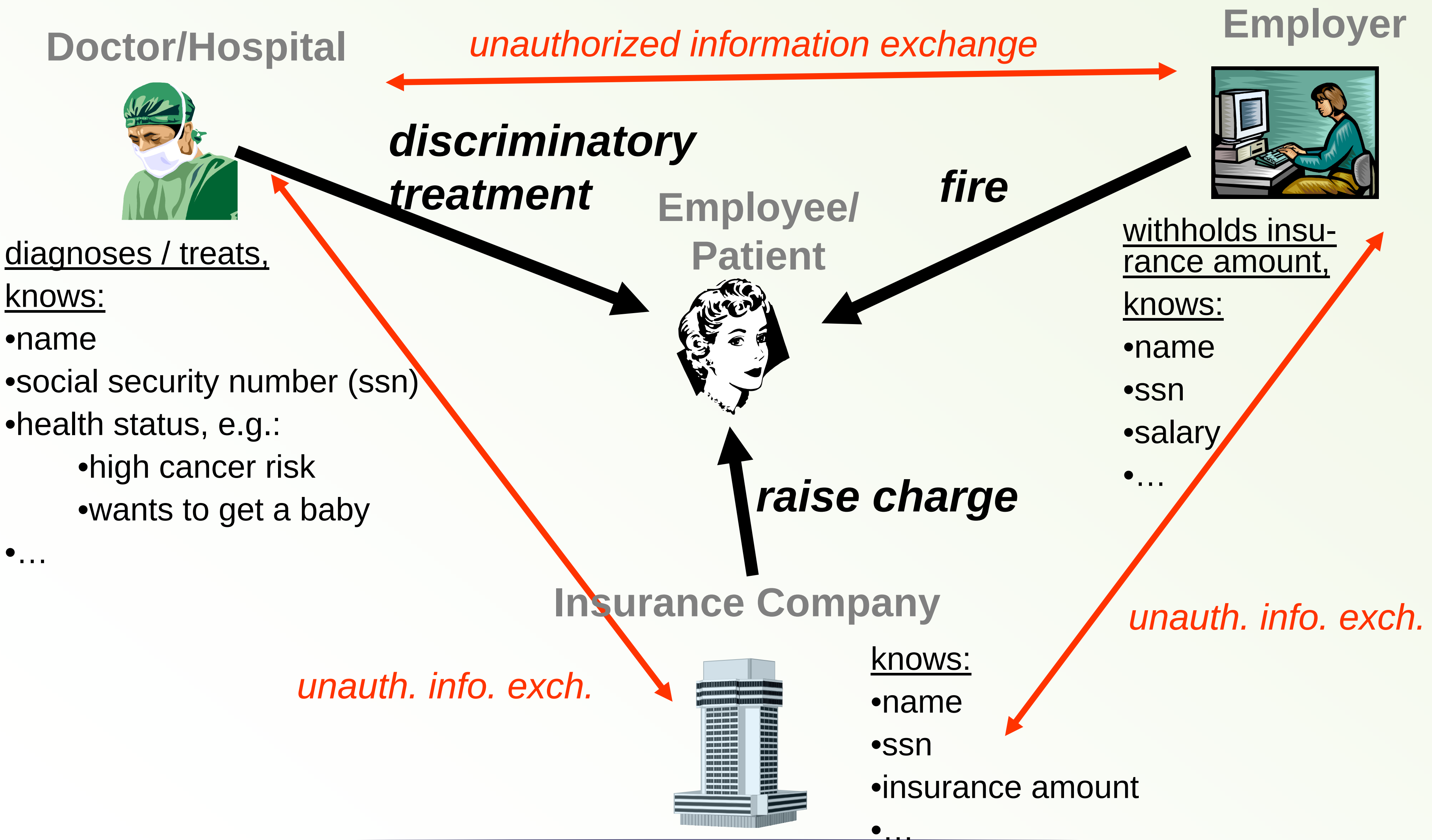
Satisfying Customers Interests: **Privacy - Meaning**

- in general: “the right to select what personal information about me is known to what people” [WES67]
- non-material value
- e-transaction privacy more or less protected by law in different countries
- **but**: you cannot check secrecy of service providing organizations

Problem: Non-Privacy

- organizations get information…
  - they do not need for the purpose of this interaction
  - they should not get because it is private
- organizations can intrude into privacy by…
  - linking data of different certificates sent by the same user
  - pooling data with other organizations
- organizations use private information for other purposes

Unauthorized privacy revealing



Doctor/Hospital

diagnoses / treats,

knows:

- name
- social security number (ssn)
- health status, e.g.:
    - high cancer risk
    - wants to get a baby
- …

unauthorized information exchange

Employer

withholds insurance amount,

knows:

- name
- ssn
- salary
- …

discriminatory treatment

fire

Employee/ Patient

raise charge

Insurance Company

knows:

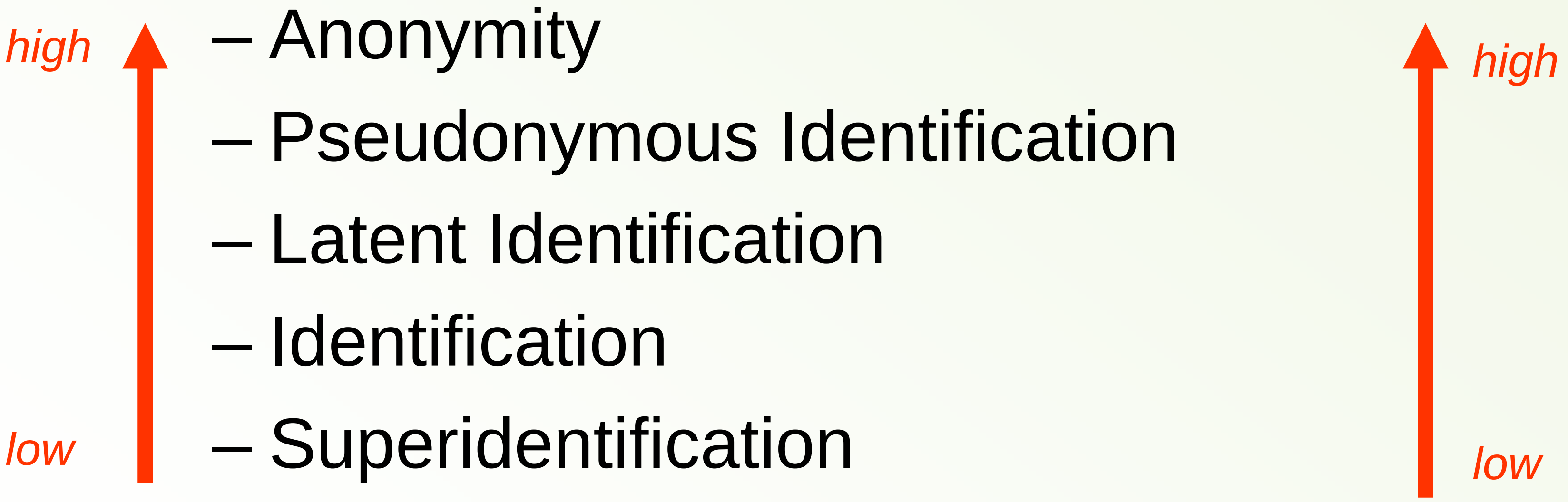
- name
- ssn
- insurance amount
- …

unauth. info. exch.

unauth. info. exch.

Identity spectrum must be balanced

- Levels of anonymity:



- – Anonymity
- – Pseudonymous Identification
- – Latent Identification
- – Identification
- – Superidentification

Try to satisfy both sides´ interests

Anonymity - Meaning

- “Anonymity is the state of being **not identifiable** within a set of subjects” [PF00]
- “[Anonymity] ensures that a user may use a resource or service **without disclosing** the user’s **identity**” [ISO99]

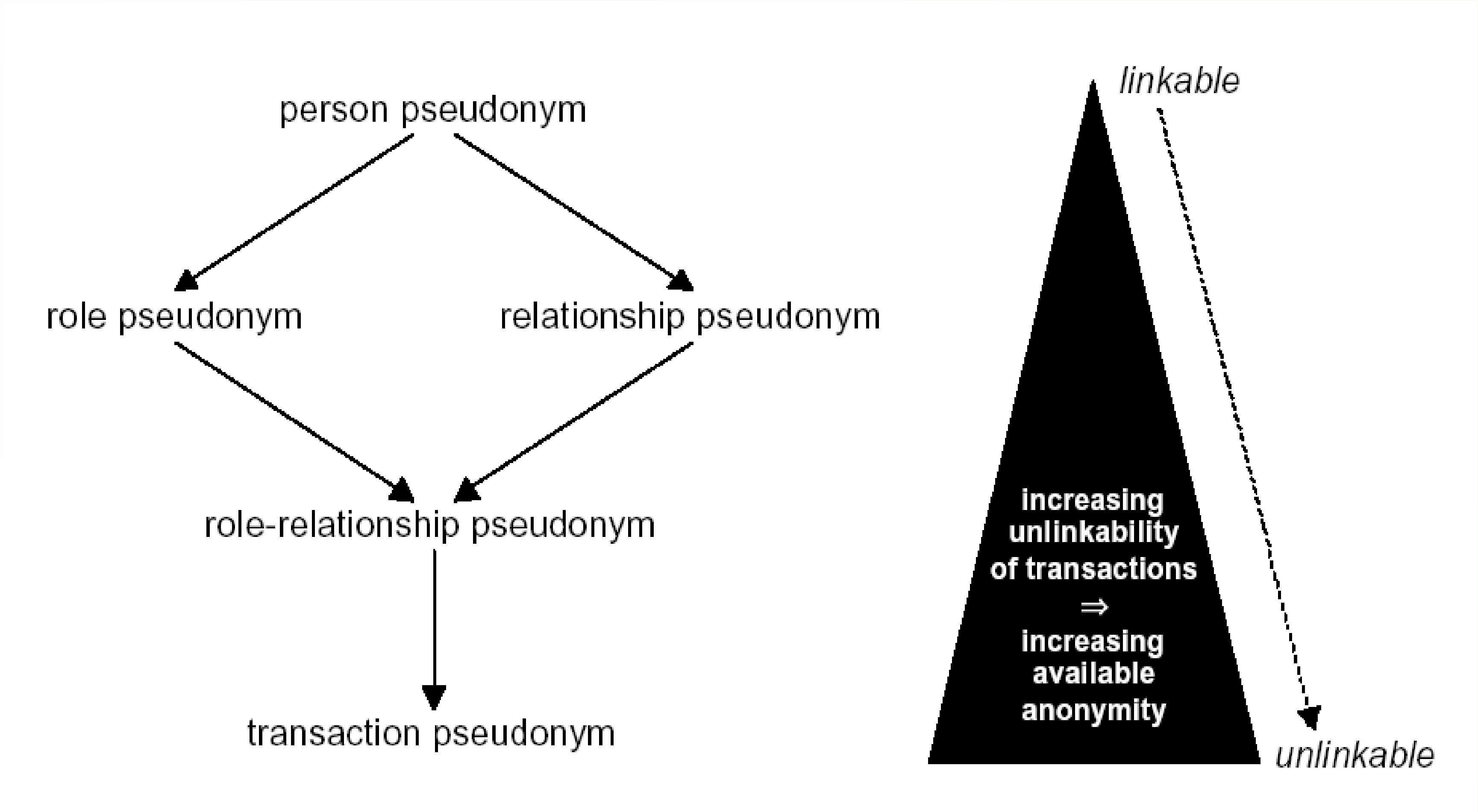
Pseudonyms/Pseudonymity

- Pseudonyms are identifies of subjects
- Pseudonymity is the use of pseudonyms as IDs [PF00]
- digital pseudonym:
  - bit string, unique as ID
  - used to authenticate the holder

Pseudonyms

- **dimensions**
  - public pseudonym
  - non-public pseudonym
  - unlinkable pseudonym
- **context**
  - personal pseudonym
  - role pseudonym
  - relationship pseudonym
  - role-relationship pseudonym
  - transaction pseudonym

Pseudonyms (context)


person pseudonym
role pseudonym
relationship pseudonym
role-relationship pseudonym
transaction pseudonym
linkable
increasing unlinkability of transactions ⇒ increasing available anonymity
unlinkable

[PF00]

Pseudonymous Certificate

- does NOT content the real subject (user) name
- pseudonym substitutes the real name
  - randomly chosen, artificial
  - keeps anonymity towards outsiders
  - can keep anonymity towards communication partners
- also standardized by ITU / IETF

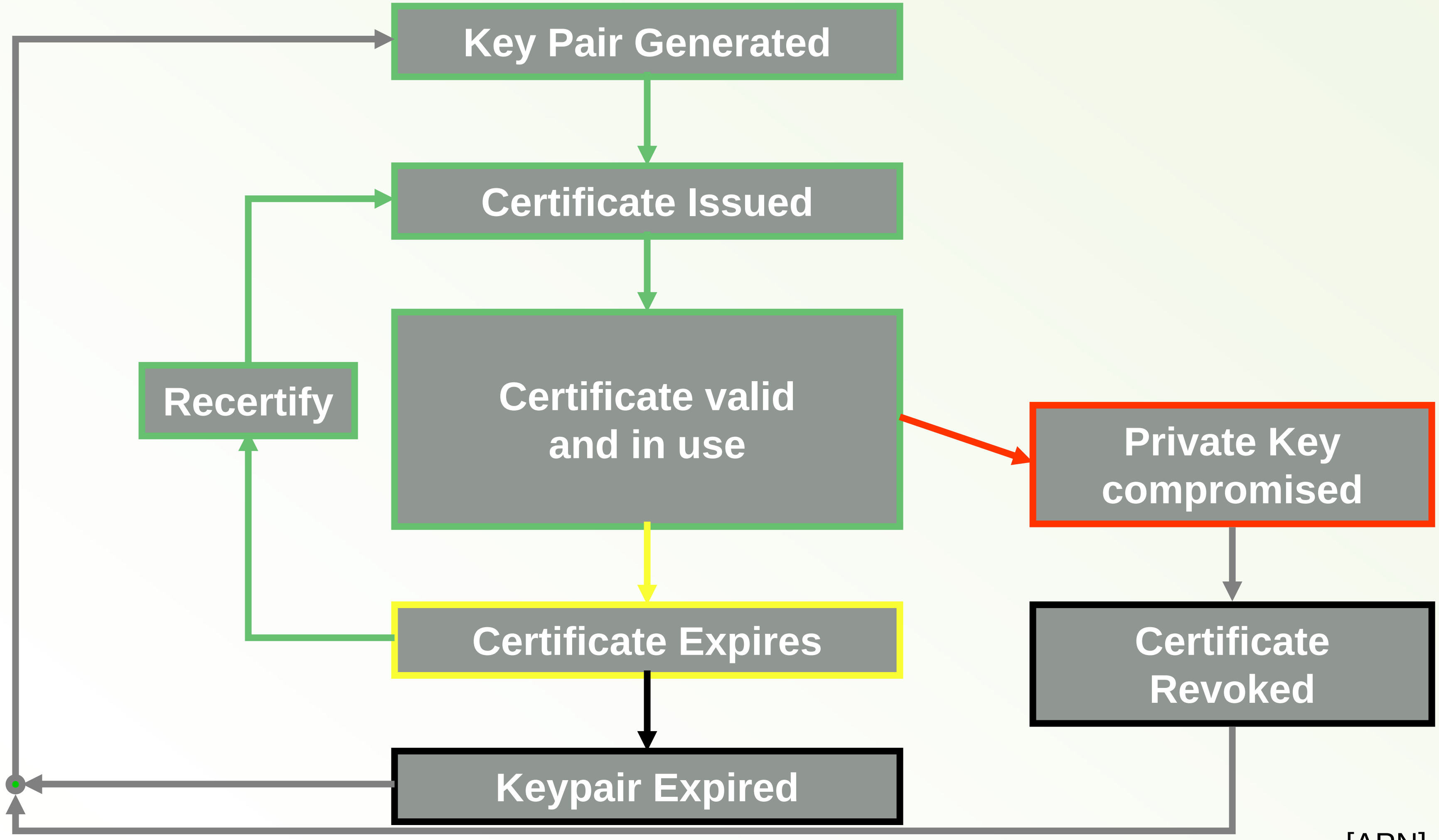
Insufficiency of **linkable** pseudonymous Certificate

- service provider can still link users' information of several transactions / make users' profiles
- involuntary de-anonymization by monitoring usage of services
- possibility of pooling data with other organizations to get out users' information and identity

Solution: **Transaction** Pseudonymous Credentials

- each transaction with different pseudonym
- no linkability between two transactions
- no transmit of certificate, just proof of possession

Certificates: Lifecycle



Key Pair Generated

Certificate Issued

Recertify

Certificate valid and in use

Private Key compromised

Certificate Expires

Certificate Revoked

Keypair Expired

[APN]

Role of CA / Pseudonymous-CA (PCA)

tasks of CA

- issuing signatures
- certifying validity and ID of dig. signature’s/public key’s owner
- revoking signature when private key compromised
- maintain pki-infrastructure

additional tasks of PCA

+ registering nym
+ verifying credential
+ **de-anonymization decision**
+ **global / local de-anonymization**

IDEMIX („IDEntity **MIX**“)

- project of engineers at IBM’s Zurich Research Laboratory, Switzerland
- prototype system to guarantee ‘anonymity’ in the Internet
- implementation of
  - cryptographic protocols
  - ‘pseudonym authority’ (credentials’ issuer)
  - web servers using anonymous access
- protocols also used in other projects / software

IDEMIX Features (1)

- organization knows users just by pseudonyms ("nyms")
- different nyms of same user cannot be linked
- user of a credential can prove possession of it without revealing the credential itself
- encoding of attributes: user can choose which attributes he reveals to the service provider

Necessary Information/Attributes
Example: Car rental system

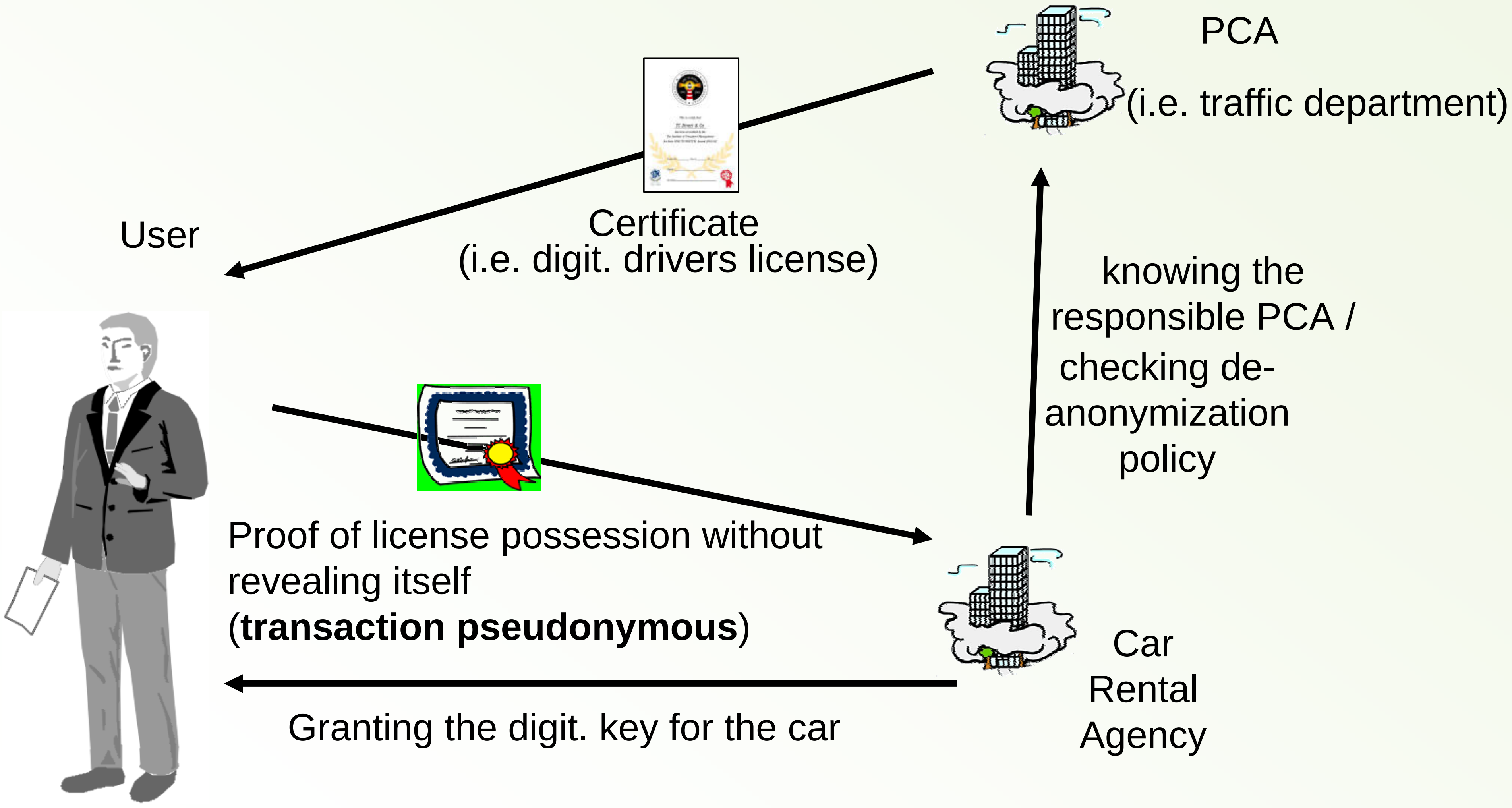
- reducing given information to prevent linkability / data pooling

information usually given	information actually needed
• *birthday: 11/23/1973*	• *age: 18 or over*
• *account balance: $ 16,357*	• *account balance > $ 5000*
• *all passport information*	• *nationality*
• *all driver's license information*	• *possession of driver's license*
• *dig. credential with attributes and personal information*	• *possession of a credential (i.e. an allowance to …)*
• *user's name*	• *(pseudonym)*

IDEMIX Features (2)

- different users cannot pool/share their credentials
- anonymity revocation by trusted third party in case conditions of foregoing agreement apply
- mechanisms to revocate credentials
- one-show credentials

Example Scenario : Issuing/Verifing



PCA

(i.e. traffic department)

Certificate
(i.e. digit. drivers license)

User

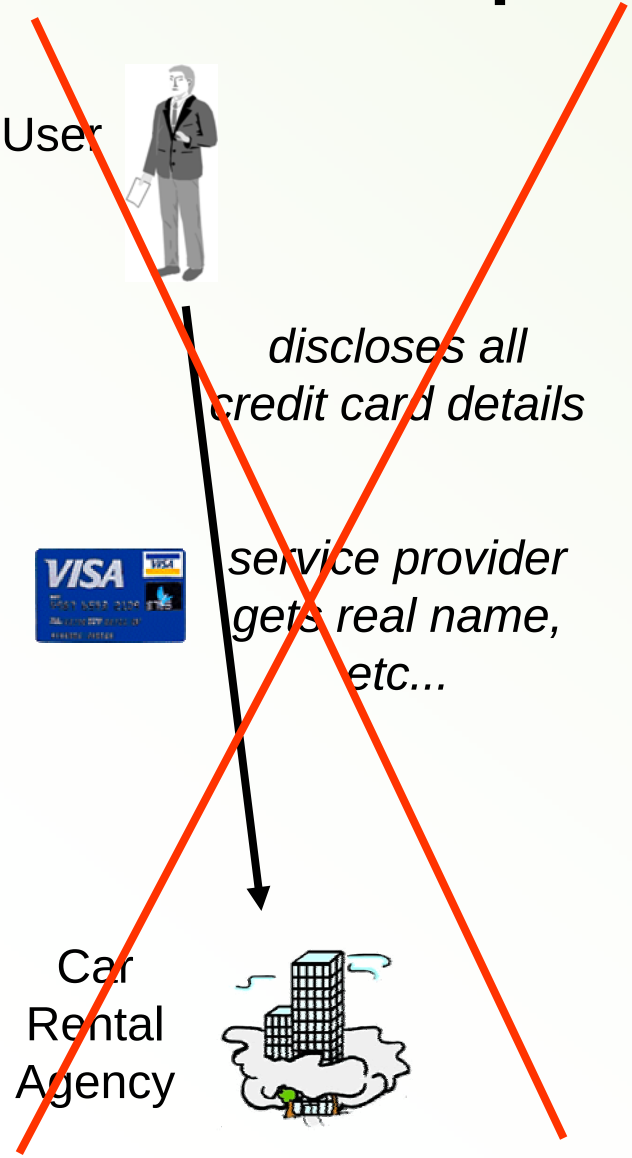
knowing the responsible PCA / checking de-anonymization policy

Proof of license possession without revealing itself
(**transaction pseudonymous**)

Car Rental Agency

Granting the digit. key for the car

Example Scenario : Payment

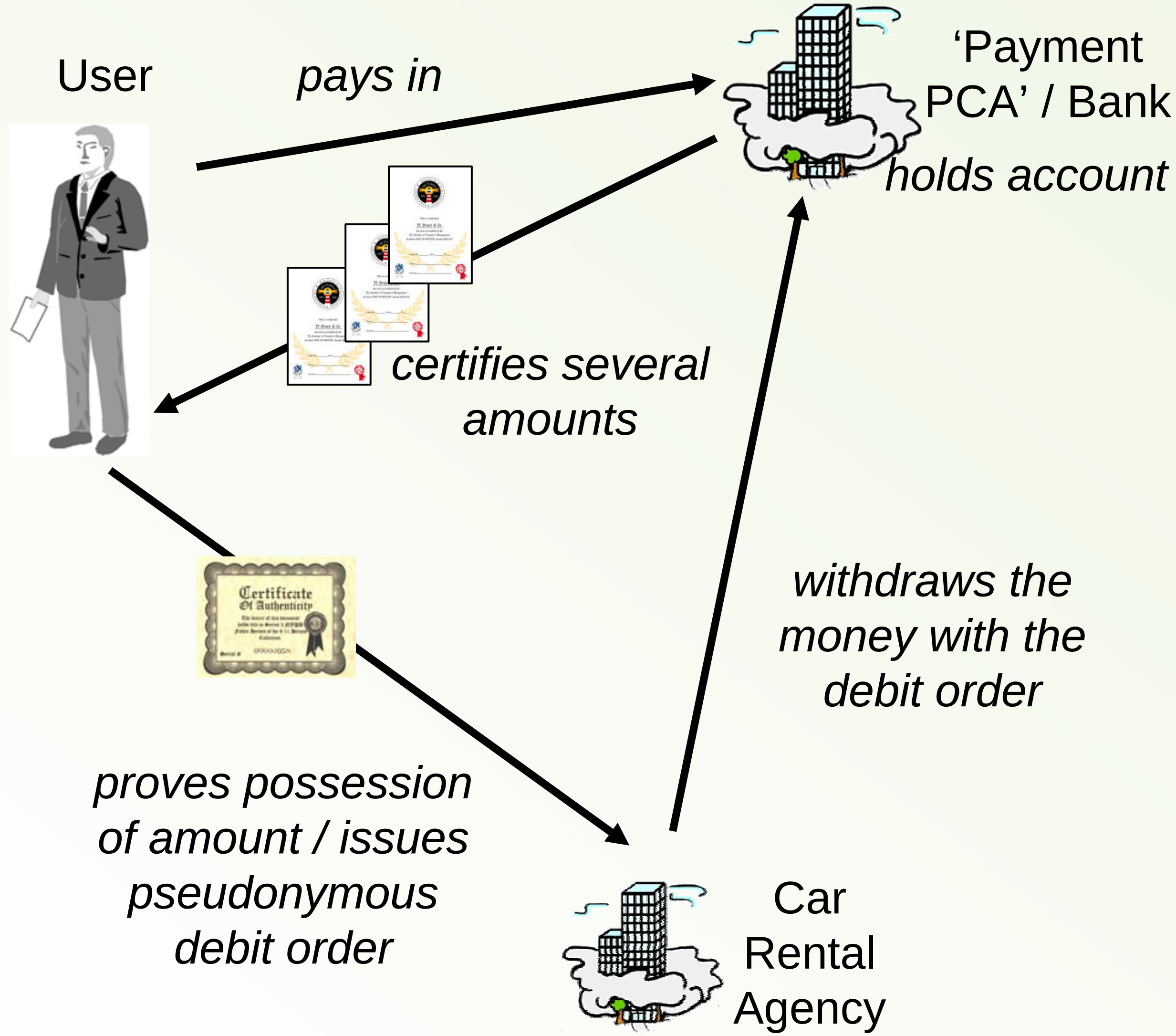


User

discloses all credit card details

service provider gets real name, etc...

Car Rental Agency



User

pays in

‘Payment PCA’ / Bank

holds account

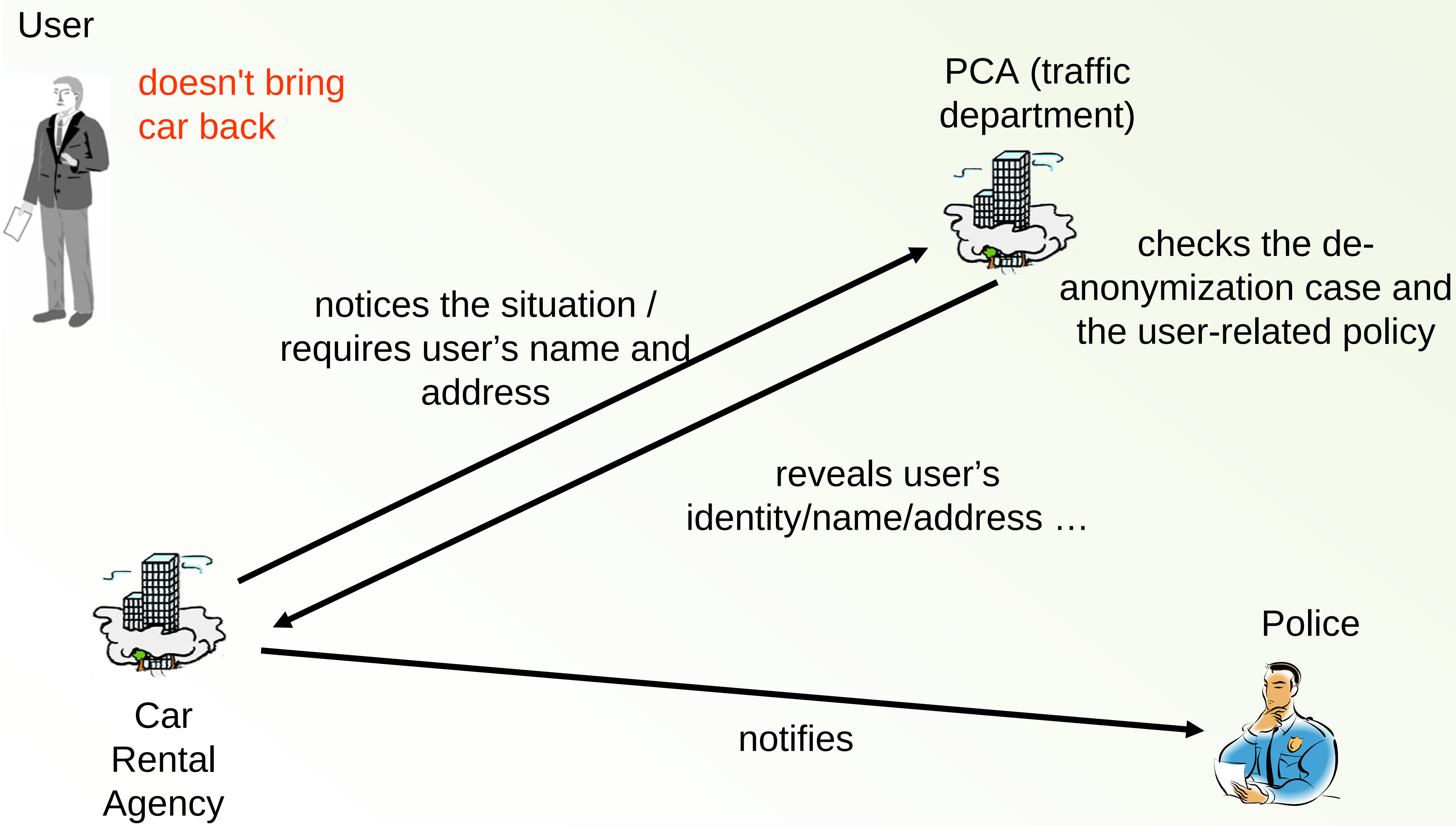
certifies several amounts

proves possession of amount / issues pseudonymous debit order

withdraws the money with the debit order

Car Rental Agency

Example Scenario : Revealing (“global”)



User

doesn't bring car back

PCA (traffic department)

notices the situation / requires user’s name and address

checks the de-anonymization case and the user-related policy

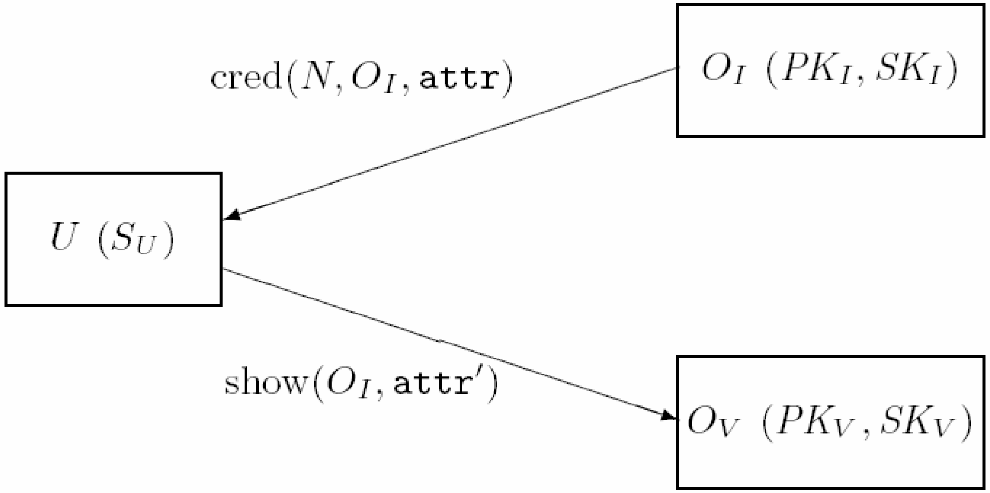
reveals user’s identity/name/address …

Police

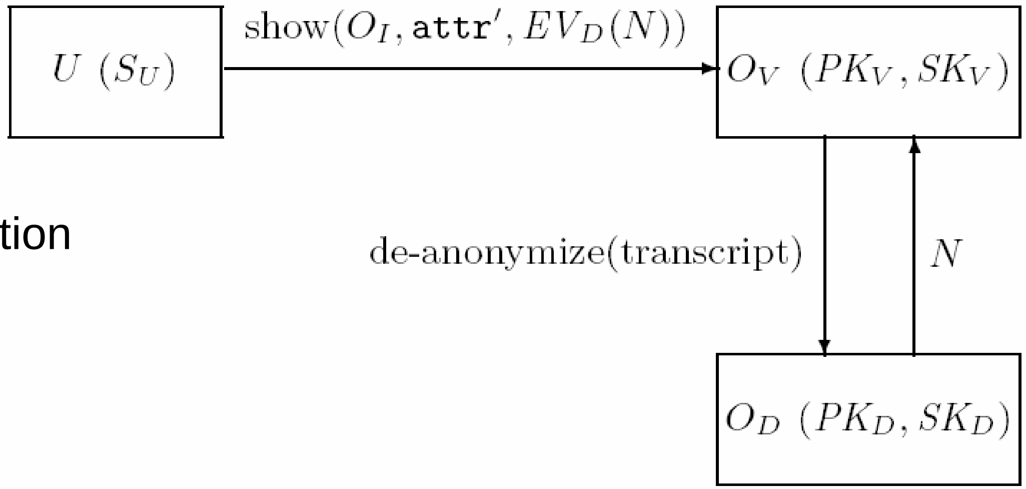
Car Rental Agency

notifies

Idemix Protocol : a small extract


$O_I\ (PK_I, SK_I)$
$\mathrm{cred}(N, O_I, \mathtt{attr})$
$U\ (S_U)$
$\mathrm{show}(O_I, \mathtt{attr}')$
$O_V\ (PK_V, SK_V)$

U	user
O_i	issuing organization
O_v	verifying organization
N	pseudonym
attr	credential's attributes
S_u	user's master secret
PK/SK	public/secret encryption key



O_D	de-anonymizing organization
$EV_D(N)$	with PK_D encrypted N (verifiable)

[KAHE]

Problems :

- general danger of misuse of a pseudonym credential without attention
- you still need 3rd party organizations you and your transaction partner have to trust and give it your identity information
- no development of provider-customer relationship
- no marketing analysis possible

Resume :

- idemix solves problems which weren’t solved before
- practical in use
- but: system must become accepted by the users and especially by the service providers
- service providers may just see the disadvantages for them (information needed for marketing, expenses of system, i.e.)

- Questions? Please, feel free to ask.

- What do you think?

  – Is there a chance for anonymous credential systems like IDEMIX?

References :

- [WES67] Alan F. Westing. Privacy and Freedom. Athenium. New York. 1967
- [PF00] Andreas Pfitzmann, Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology. 2000
- [KOSCH03] Alfred Kobsa, Jörg Schreck. Privacy Through Pseudonymity in User Adaptive Systems. ACM Transactions on Internet Technology. May2003.
- [ISO99] ISO IS 15408, 1999, http://csrc.nist.gov/cc/
- [APN] http://www.apnic.net
- [THAW] http://www.thawte.com
- [CAHE] Jan Camenisch, Els Van Herreweghen. Rüschlikon/Switzerland. Design and Implementation of the idemix Anonymous Credential System
- [LYRISA99] A. Lysyanskaya, R. L. Rivest, A. Sahai. Pseudonym Systems. Cambridge 1999.