

# Privacy - benaderd vanuit de techniek

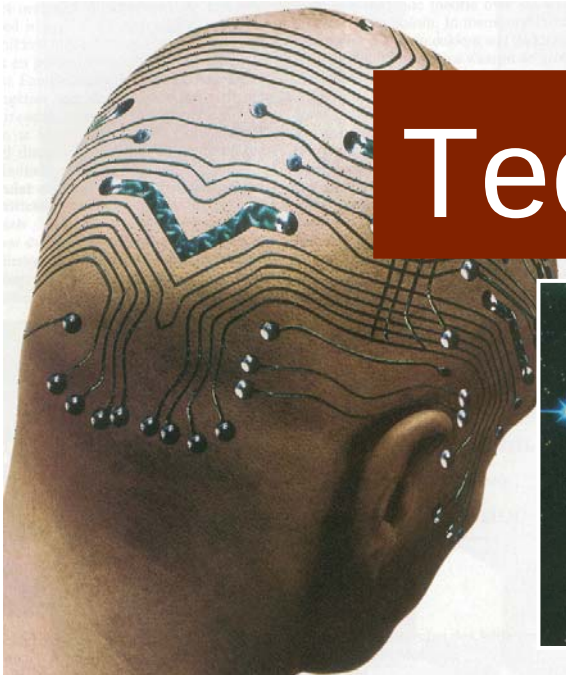
**Rieks Joosten**

**TNO | Knowledge for business**





# Techniek



In elke computer  
zit een 'Avatar',  
of 'Gebruiker'.

Gebruikers voeren  
werkinstructies uit  
(programma's)

Gebruikers en mensen zijn  
enerzijds verschillend:



```

TKP
16514 PUSH HL 229
<130> PUSH BC 197
< 64> CALL NN 205 187 2
LD B H 68
LD C L 77
LD D L 85
INC D 20
JP Z DIS 40 247
CALL NN 205 189 7
LD A <HL> 126
POP
PUS
CP
JP
INC
DJN
POF
JR
POF
POF
LD
RET
KYBD

16544 LD BC NN 1 29 9
<160> CALL NN 205 130 64
< 64> DEC HL 43
LD C N 14 32
CALL NN 205 130 64
INC HL 35
16557 LD A <HL> 126
SUB N 214 28
LD B A 71
LD C N 14 11
XOR A 175

CP N 254 148
JP NC DIS 48 26
CALL STR 205 187 64
CP N 254 2
JP NC DIS 48 19
PUSH AF 245
CALL ALIST 205 141 66
POP AF 241
CP N 254 0
JP Z DIS 40 10
POP BC 193

```

Gebruikers zijn geen mensen



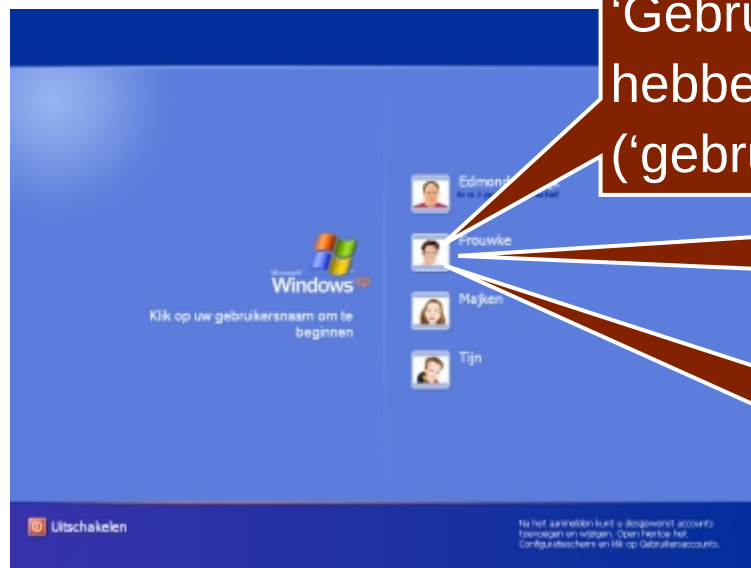
| Mensen | Eigenschap                     | Avatars |
|--------|--------------------------------|---------|
| Traag  | Snelheid van handelen          | Snel    |
| Traag  | Snelheid van verplaatsen       | Snel    |
| Klein  | Geheugen                       | Groot   |
| ✓      | Fouten maken                   | ✗       |
| ✓      | Fouten herstellen              | ✗       |
| ✓      | Vage opdrachten uitvoeren      | ✗       |
| ✗      | Precieze opdrachten uitvoeren  | ✓       |
| ✓      | Creatief, initiatief, flexibel | ✗       |
| ✓      | Geweten                        | ✗       |



In elke computer  
zit een 'Avatar',  
of 'Gebruiker'.

Gebruikers voeren  
werkinstructies uit  
(programma's)

Gebruikers en mensen  
hebben dingen gemeen:



'Gebruikers' (avatars)  
hebben namen  
( 'gebruikersnamen' )

De 'persoonsgegevens'  
van gebruikers  
zijn opgeslagen in  
'(gebruikers)accounts' ...

...en als je hun 'geheim' kent  
(het wachtwoord) ...

... dan kun je met ze communiceren

**Stelling:**

Het is belangrijk om  
mensen van gebruikers  
te kunnen onderscheiden



# Privacy

- Grondwet, art. 10-13:
  - recht op het eerbiedigen van de persoonlijke levenssfeer
  - regels m.b.t. vastleggen, verstrekken, kennisname, gebruik en verbetering van persoonsgegevens gegevens
  - recht op onaantastbaarheid van het lichaam
  - regels m.b.t. het binnentreden van woningen
  - brief-, telefoon- en te
- Met wettelijk geregelde uit
- Wikipedia: the ability of an individual to control themselves or information about themselves and thereby reveal themselves selectively
- Fourth Amendment: the right to be le(f)t alone
- SAA: The right of an individual to be secure from unauthorized disclosure of information about oneself that is contained in documents
- The quality or condition of being free from unsanctioned intrusion
- the existence of conditions which will permit an individual or individuals to carry out an activity commenced without interruption or interference, either by sight or sound by unwanted individuals.



# Wat bedoelen we met 'Privacy'?

- Grondwet, art. 10-13:

Met rust gelaten worden ...

... de persoonlijke levenssfeer ...  
... rekken, kennisname, gebruik  
... persoonsgegevens gegevens

- recht op onaantastbaarheid van het lichaam
- regel
- brief

Met wette

- Wikipedia: ... seclude themselves ...  
... themselves ... tively

- Fourth Amendment

- SAA: The ... unauthorized

- The quality

- the existence of conditions which will permit ...  
... commenced without interruption or interference ...  
... individuals.

... respect voor:

- persoonlijke levenssfeer
- persoonsgegevens
- lichaam
- woonruimte
- communicatie

van fysieke personen

... die zo-doende vrij zijn  
(d.w.z. zich veilig weten)  
om in die rust ('levensruimte')  
te kunnen doen en laten  
wat hen goed dunkt.



# Privacy is gebonden aan 'samenlevingsverbanden'

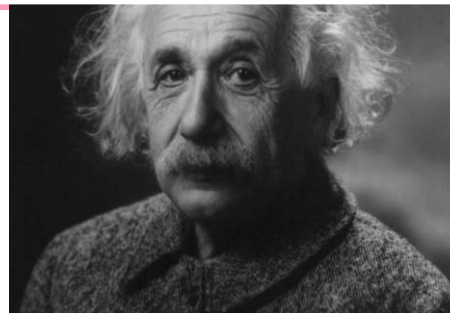


**Stelling:**

'Samenlevingsverbanden'

- jezelf
- huisgenoten
- werk
- clubs
- Nederland

Elk samenlevingsverband  
geeft aan 'Privacy'  
een eigen betekenis





## Identiteit en Persoonsgegevens

Beklaagde  
Harteloos  
Strafblad  
Onschuldig (nog wel)



Uitdrukkingsloos  
Beetje saai  
Klant



Klant  
Wanbetaler  
Onbetrouwbaar  
Ruige chauffeur



Werknemer  
Betrouwbaar  
Controller  
Goed

# Stelling:

Identiteit van Piet =  
alles wat hijzelf en anderen  
van hem vinden

i.e.: samenlevingsverbanden

## Identiteit en Persoonsgegevens



Beklaagde  
Harteloos  
Strafblad  
Onschuldig (nog wel)



**Stelling:**

Persoonsgegevens van Piet =  
'Claim' van iemand over Piet

i.e.: 'Identity Provider'





## Identiteit en Persoonsgegevens

Beklaagde  
Harteloos  
Strafblad  
Onschuldig (nog wel)



Uitdrukkingsloos  
Beetje saai  
Klant



Klant  
Wanbetaler  
Onbetrouwbaar  
Ruige chauffeur



Werknemer  
Betrouwbaar  
Controller  
Goed

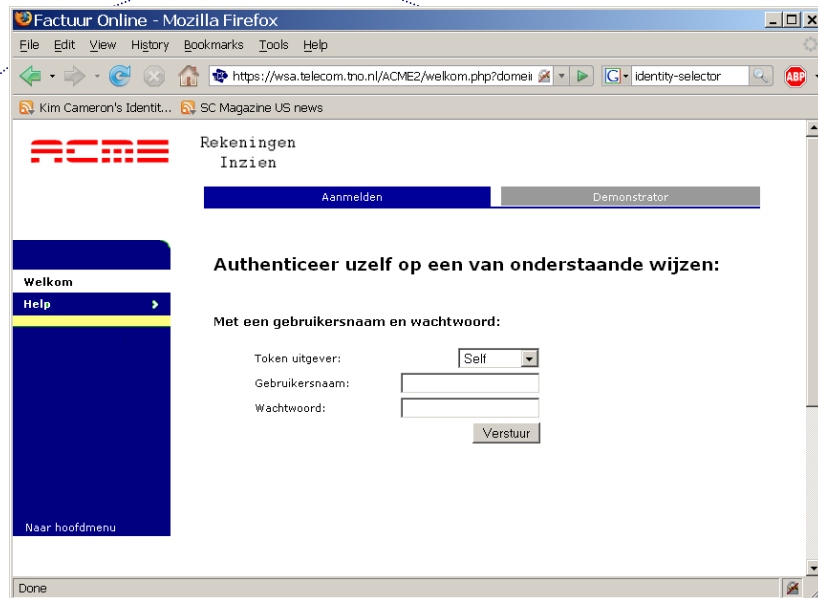
**TIP**

Kijk bij het uitwisselen van  
persoonsgegevens vooral ook  
naar de Identity Provider

## Identity Metasystem (ook wel: InfoCards)

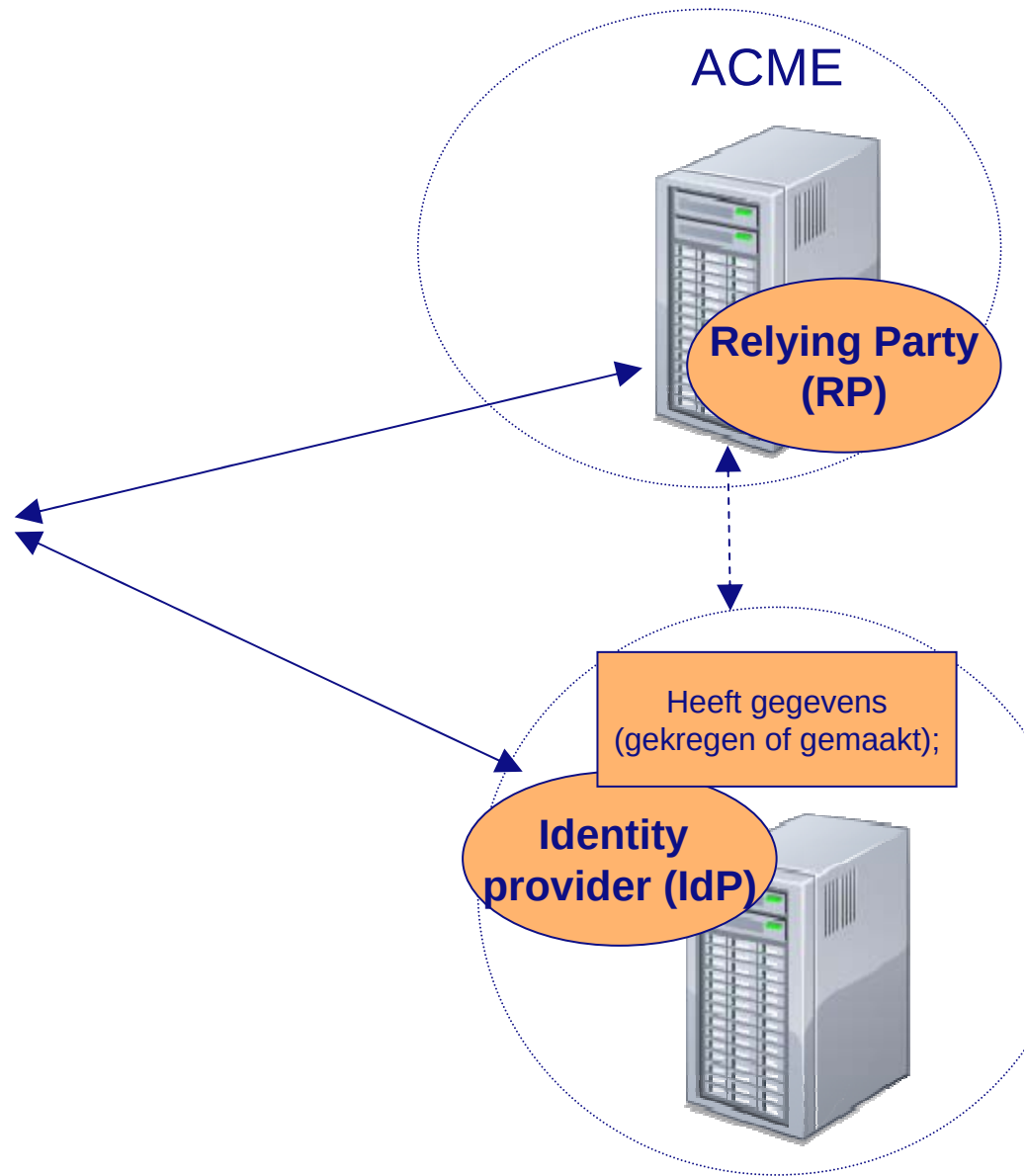


# Klassiek:



Persoon of ding  
waarop gegevens  
betrekking hebben.

**Subject**





# Achtergrond

- Microsoft Passport
  - Identity provider voor MSN (300M+ gebruikers, 1 miljard logins/dag )
  - ~~Identity provider voor Internet~~
- 7 “Laws of Identity”:
  - User control and consent
  - Minimal disclosure for a defined use
  - Justifiable parties
  - Directional identity
  - Pluralism of operators and technology
  - Human integration
  - Consistent experience across contexts



# Identity Metasystem rollen



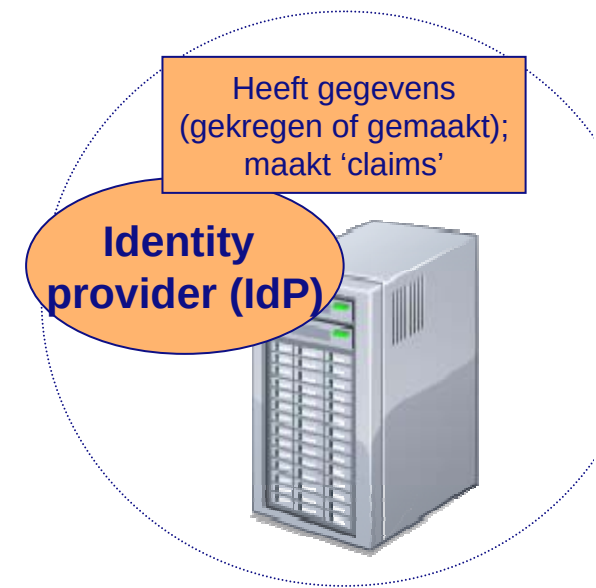
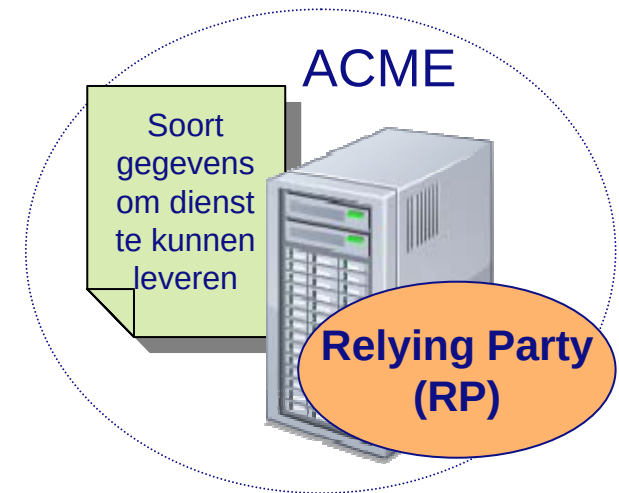
'Infocards' zijn vergelijkbaar met plastic kaarten

Een 'Infocard' bevat alleen meta-data:

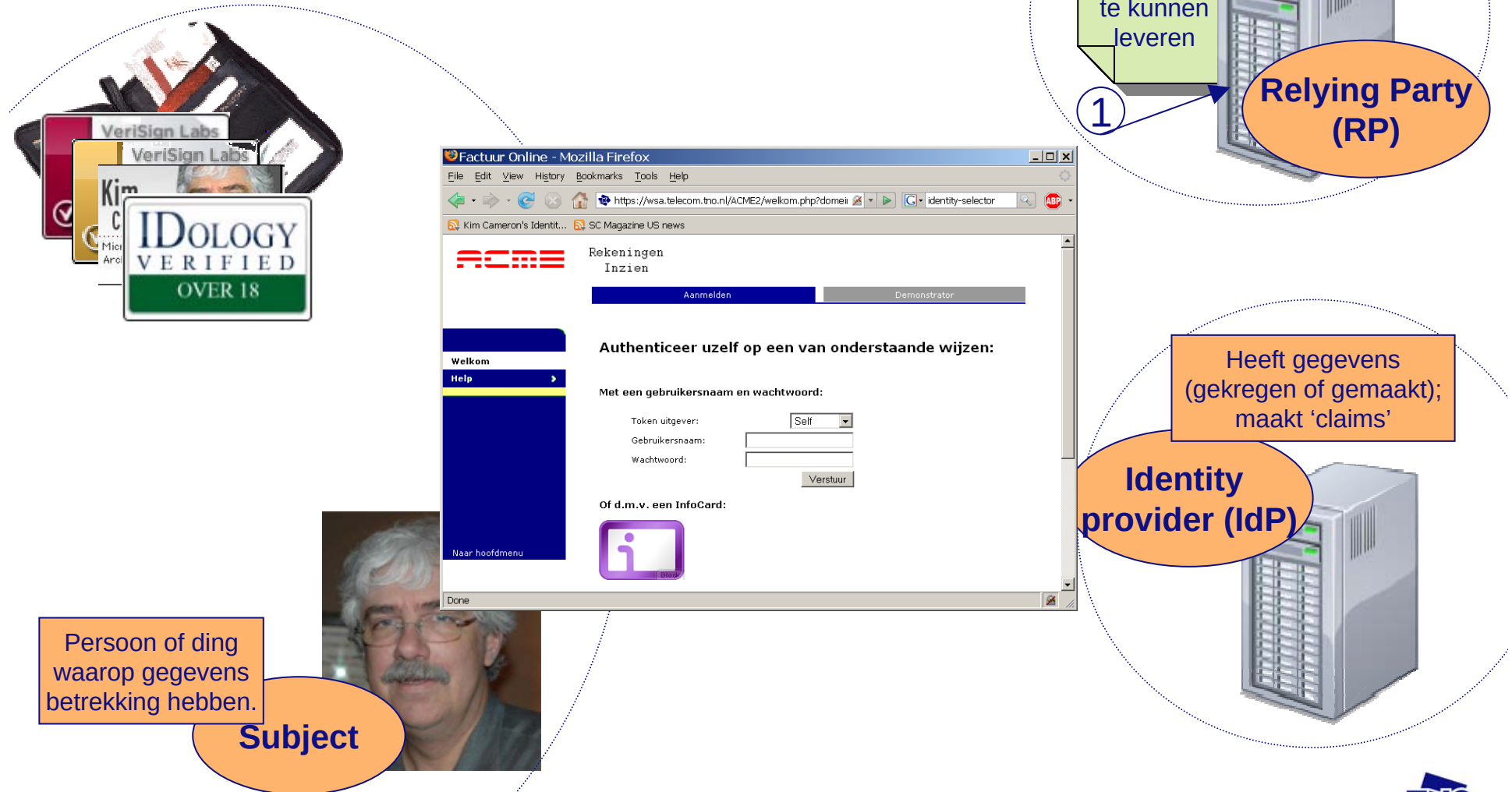
- welk soort data er te vinden is, en
- waar die data dan te vinden is (IdP)

Persoon of ding waarop gegevens betrekking hebben.

**Subject**

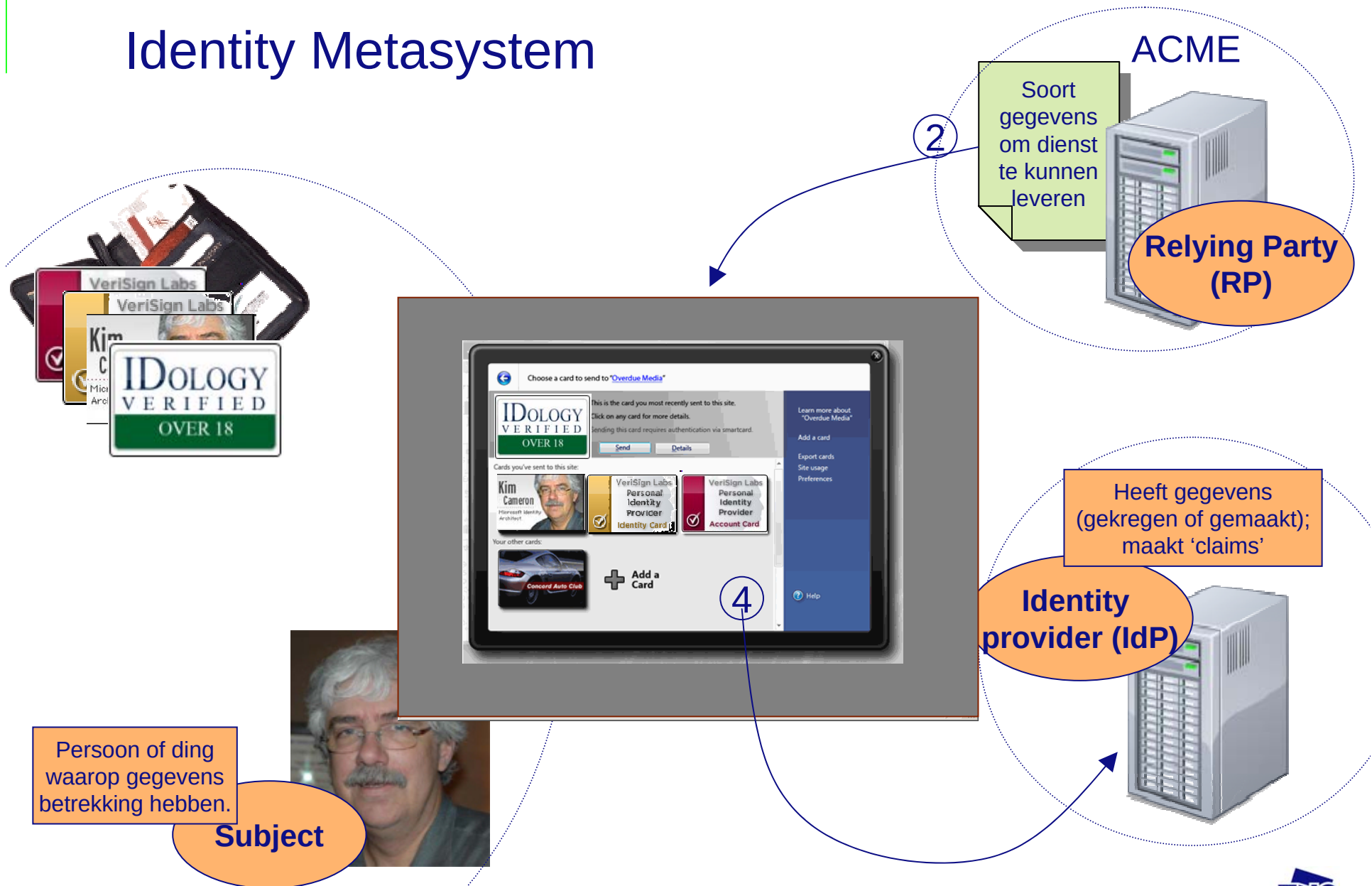


# Identity Metasystem





# Identity Metasystem

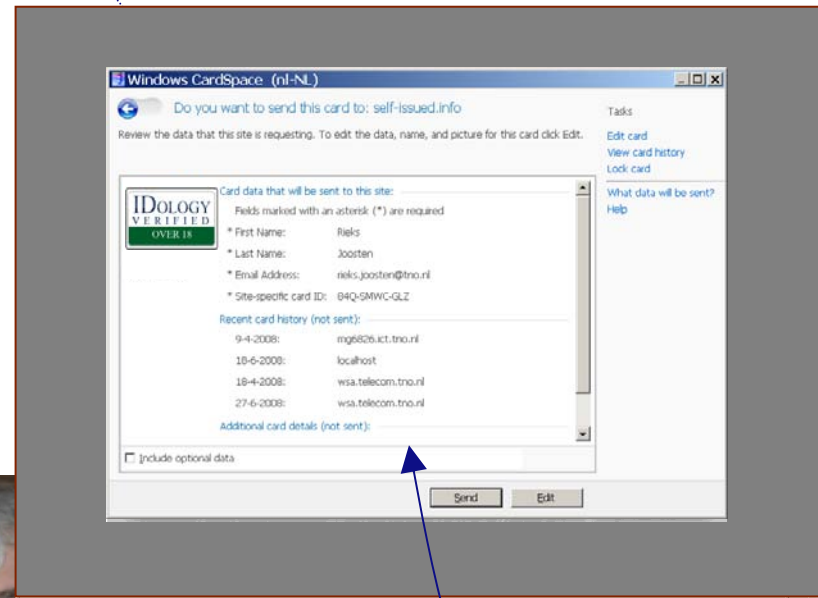


# Identity Metasystem



Persoon of ding  
waarop gegevens  
betrekking hebben.

**Subject**



**ACME**

Soort  
gegevens  
om dienst  
te kunnen  
leveren

**Relying Party  
(RP)**

7

Heeft gegevens  
(gekregen of gemaakt);  
maakt 'claims'

**Identity  
provider (IdP)**

5

# Identity Metasystem



Persoon of ding  
waarop gegevens  
betrekking hebben.

**Subject**

Factuur Online - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://wsa.telecom.tno.nl/ACME2/welkom.php?domei... identity-selector

Kim Cameron's Identit... SC Magazine US news

**ACME**

Rekeningen  
Inzien

Individueel **Totaal**

Welkom  
Facturen  
Lopende gesprekskosten  
Rapporten  
Beheer  
Extra's  
Help

Interlokaal:

| Van        | Naar       | Datum  | Starttijd | Tijdsduur | Kosten |
|------------|------------|--------|-----------|-----------|--------|
| 0703464186 | 0621455066 | 8 Sep  | 15:33:53  | 00:05:34  | € 2,34 |
| 0703464186 | 0621455066 | 8 Sep  | 15:33:57  | 00:05:34  | € 2,34 |
| 0703464186 | 0621455066 | 8 Sep  | 15:55:59  | 00:05:34  | € 2,34 |
| 0703464186 | 0621455066 | 11 Sep | 20:31:58  | 00:05:34  | € 2,34 |
| 0703464186 | 0621455066 | 14 Sep | 10:36:15  | 00:05:34  | € 2,34 |
| 0703464186 | 0621455066 | 14 Sep | 13:20:03  | 00:05:34  | € 2,34 |
| 0703464186 | 0621455066 | 14 Sep | 14:14:53  | 00:05:34  | € 2,34 |
| 0703464186 | 0621455066 | 15 Sep | 16:35:39  | 00:05:34  | € 2,34 |

Done

**ACME**

Soort  
gegevens  
om dienst  
te kunnen  
leveren

**Relying Party  
(RP)**

8

Heeft gegevens  
(gekregen of gemaakt);  
maakt 'claims'

**Identity  
provider (IdP)**

5

# Waarom Identity Metasystem / Infocards?

- Bescherming van persoons-  
c.q. gebruikers gegevens  
staat centraal



- Gegevens binnen 'samenlevingsverbanden' (bedrijven/overheid) kunnen eenvoudig beschikbaar worden gesteld
- Vermindering van het aantal koppelingen tussen systemen voor gegevensuitwisselingen
- Er is, en komt steeds meer, (technische) ondersteuning



# Samengevat:

- Personen zijn geen gebruikers;  
ze kunnen wel met elkaar communiceren.
- Elk Samenlevingsverband geeft 'Privacy' een eigen betekenis,  
die bestaat uit de gevolgen die het heeft voor
  - 'deelnemers' (personen en gebruikers)
  - niet-deelnemers (personen)
- Samenlevingsverbanden die iets vinden van een persoon  
zijn 'Identity Provider' voor die persoon;
- Persoonsgegevens zijn 'claims' van identity providers  
over een of ander persoon (en zeggen niets over de waarheid ervan).
- Technieken zoals Infocards kunnen daarbij helpen.

Techniek is noch positief  
noch negatief  
maar NOOIT neutraal. (Kranzberg)



Rieks Joosten  
+31 622 901 317  
[rieks.joosten@tno.nl](mailto:rieks.joosten@tno.nl)

Techniek is noch positief  
noch negatief  
maar NOOIT neutraal. (Kranzberg)