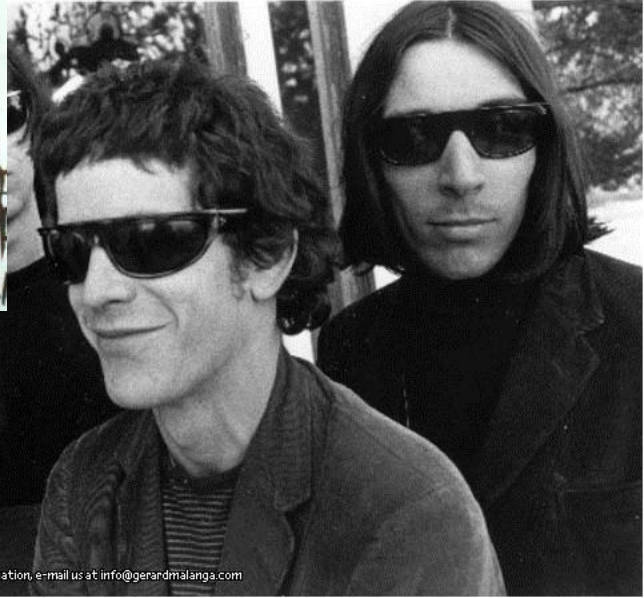


Identiteit in de ICT

Filosofie, identificatie, authenticatie



www.marcdeg



raauw.co

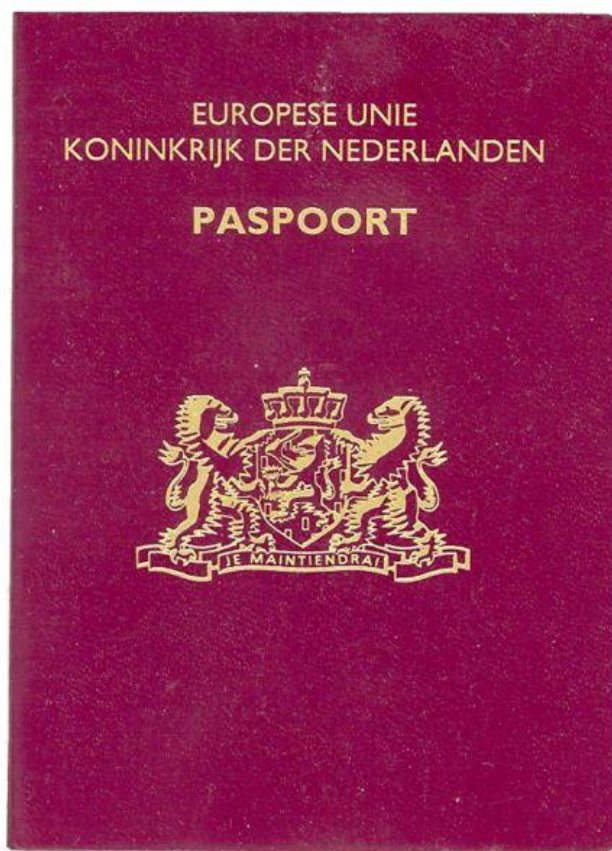


Nieuw-
Halster
Halster
Halster
Steenbe



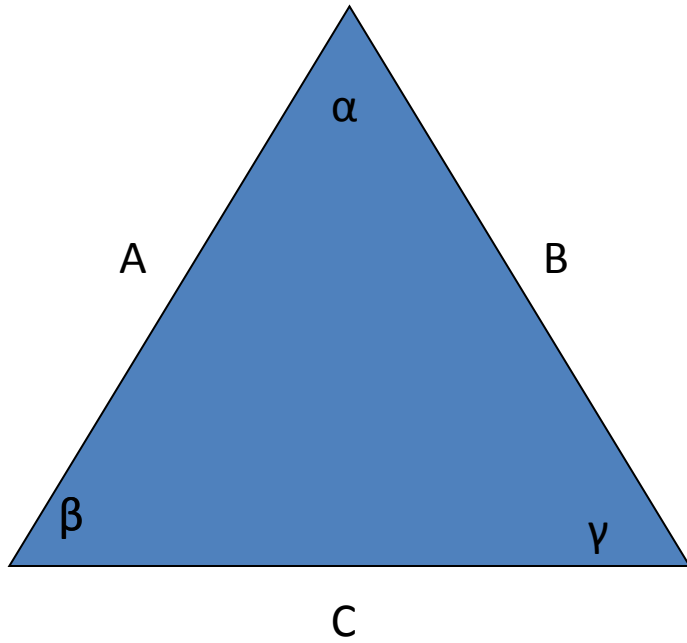
elo	
gen	
gen op Zoom	bevolkingsregister 1900-1920
gen op Zoom	geboren
gen op Zoom	getuige
nbergen	moeder
gen op Zoom	getuige
teren	moeder

Aloysius Petrus]
Aloysius Petrus]
Anna Catharina]



a Cornelia d
a Cornelia d
a Cornelia d
a Cornelia d
a Cornelia d
a Cornelia d
a Cornelia d
a Cornelia d
a Cornelia d





$$x = 2y + 1$$

Parijs is de hoofdstad
van Frankrijk

Wat is identiteit?

- Identiteit is een “lastig: woord
- Associaties:
 - in hokjes verdelen
 - emotioneel / onderbewust
 - je hebt meerdere identiteiten
 - mono-identiteit bestaat niet meer
 - identiteit is een verzameling van zelf-definities
- Meerdere betekenissen

Wat is identiteit?

- “Corporate identity”, branding, marketing
 - IBM wil zich onderscheiden van Microsoft of Oracle. Coca Cola van Pepsi. Nintendo van Sony. BNN van de RTL, RTL van de NOS.
- Op zoek naar je eigen identiteit
 - Wie ben je. Gothic, punk, alto. Romans, films: “coming of age”.
- Een identiteit hebben is een onderscheidend kenmerk bezitten

Wat is identiteit?

- Kun je je identiteit bewijzen?
 - Heb je een rijbewijs meegenomen?
 - Of een paspoort?
 - Sta je in een geboorteregister?
 - Bij vluchtelingen: welk register? Hoe komen we daar?
 - Ayaan Hirsi Ali / Magan
 - Voor een auto: kentekenbewijs
 - Voor vee: een oormerk
- Een bewijs van een eenmalig uitgegeven kenmerk, een teken

Wat is identiteit?

- Euclides: De drie hoeken in een gelijkzijdige driehoek zijn identiek
- Frege: De ochtendster is de avondster
- Parijs is de hoofdstad van Frankrijk
- Een relatie tussen twee verwijzingen
 - reflexief ($a \rightarrow aRa$)
 - symmetrisch ($aRb \rightarrow bRa$)
 - transitief (aRb en $bRc \rightarrow aRc$)

Wat is identiteit (DvD)?

- **identiteit** (de (v.); vgl. –iteit) [*·1824·* <Fr. *identité*] **1** eenheid van wezen, volkomen overeenstemming; *de identiteit van het schrift met dat van de beschuldigde; zijn identiteit bewijzen, bewijzen dat men de persoon is voor wie men zich uitgeeft; van sommige slachtoffers kan de identiteit niet meer worden vastgesteld, men kan niet meer nagaan wie zij waren* **2** eigen karakter, het individuele kenmerk; *hij heeft geen eigen identiteit, hij waait met alle winden mee* **3** (wisk.) vergelijking die voor alle waarden die daarin voorkomende veranderlijke grootheden geldig is.

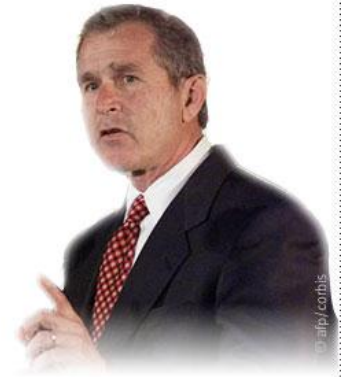
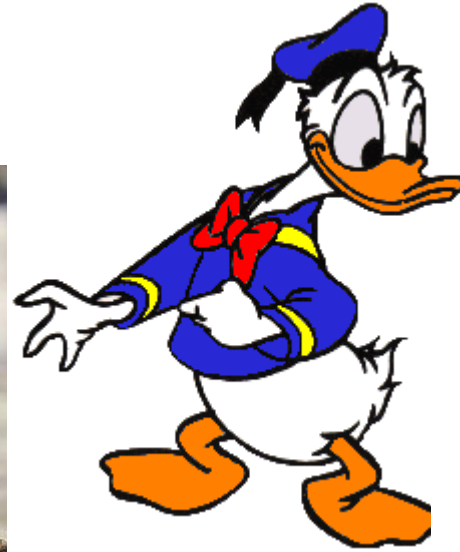
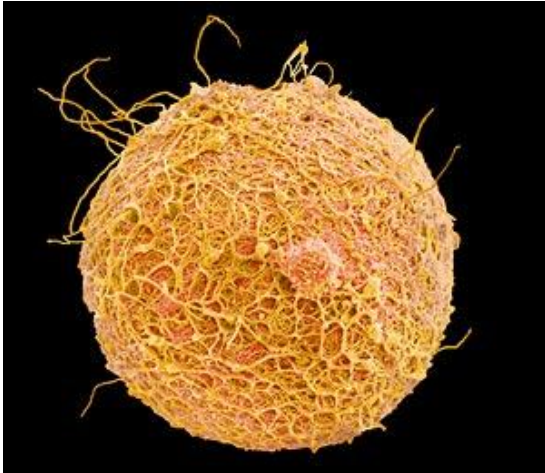
What is identity (OED)?

- **identity** · n. (pl. **-ies**) **1** the fact of being who or what a person or thing is. > the characteristics determining this. > [as modifier] serving to establish the identity of the owner: *an identity card*. **2** a close similarity or affinity. **3** Mathematics (also **identity operation**) an operation that leaves an object unchanged. > (also **identity element**) an element of a set which, if combined with another element, leaves that element unchanged. **4** Mathematics an equation expressing the equality of two expressions for all values of the variables, e.g. $(x + 1)^2 = x^2 + 2x + 1$.
- - ORIGIN C16: from Late L. *identitas*, from L. *idem*, 'same'



Ceci n'est pas une pipe.

Persoon







Gottlob Frege (1848 – 1925)

“De morgenster is de avondster”

“De morgenster is de morgenster”

Gottlob Frege (1848 – 1925)

- Frege onderzocht identiteitsuitspraken:
“De morgenster is de avondster”
- Betekent dit dat ze equivalent zijn, net zoals $a = b$?
- Dan is dit hetzelfde:
“De morgenster is de morgenster”
- Maar: de eerste uitspraak behelst kennis, de tweede is een tautologie

Intensie and extensie

- Intensie (Sinn) is een concept dat we hebben, kennis over een woord of naam
- Extensie (Bedeutung) is het ding waar een woord of naam aan refereert

woord → intensie → extensie

- Een woord bepaalt de intensie
- De intensie bepaalt de extensie

Intensie and extensie 2

woord → intensie → extensie

'avondster' → zeer heldere ster in
de avond → Venus

“De morgenster is de avondster”

- Zelfde extensie, verschillende intensie

“De morgenster is de morgenster”

- Zelfde extensie, zelfde intensie

Bertrand Russell (1872 – 1970)

“De koning van Frankrijk is kaal.”

Bertrand Russell (1872 – 1970)

- Definite descriptions, clustertheorie
- “De huidige koning van Frankrijk is kaal”
 - Is deze uitspraak waar of onwaar? Of onzin?
 - En “De huidige koning van Frankrijk is niet kaal”?
 - Lezingen:
 - Er is een X, zodanig dat X de huidige koning van Frankrijk is, en X is niet kaal: onwaar
 - Er is niet een X, zodanig dat X de huidige koning van Frankrijk is, en X kaal is: waar

Bertrand Russell (1872 – 1970)

“George IV vroeg zich af
of Scott de schrijver
van Waverley is.”

Definite descriptions

- "George IV wondered whether Scott is the author of Waverley."
 - George vroeg zich niet af of Scott identiek is aan Scott
 - George vroeg zich af of een X die ... identiek is aan een Y die ...
 - ... : vul een beschrijving in: "de schrijver van Ivanhoe", "de man die naast de prinses zit"

Ludwig Wittgenstein (1889 – 1951)

inspanning
voetbal
dobbelen
vaardigheid
poker
competitie
patience
winnen
schaken
tegenstander
bal kaatsen
darten

Ludwig Wittgenstein (1889 – 1951)

- Wat betekent het woord “spel”?
- Is er competitie? winst & verlies? vaardigheid? oefening?
- Er is geen vaste betekenis
- Alleen “familiegelekenis”
- “Betekenis is het gebruik in de taal”
- “Concept met schimmige randen”

Causale referentie ('60 – '70)

“Aristoteles is diegenen die
Aristoteles de Grote leerling
Rogier de Sijne geboren in
Stagira ...”

Causale referentietheorie

- Kripke, Putnam, Donnellan, Marcus
- Geen geloof in definite descriptions
 - Aristoteles is de leraar van Alexander, de leerling van Plato, was born in Stagira, etc. etc.
 - Maar: alles wat we van Aristoteles weten, had onwaar kunnen zijn (Aristoteles had als kind kunnen overlijden), en het zou nog steeds Aristoteles zijn (en we zouden niet zeggen: Aristoteles bestond niet)
 - Vergelijk: Odysseus

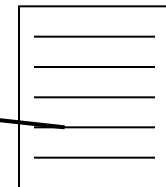
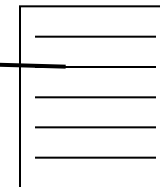
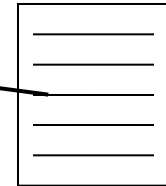
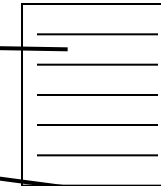
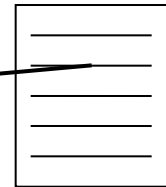
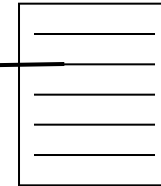
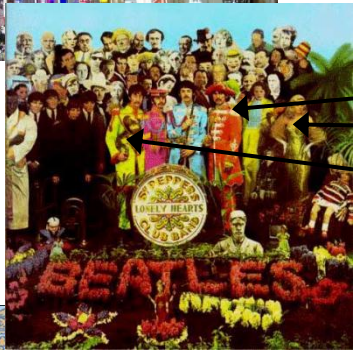
Causale referentietheorie

- Namen zijn “rigid designators”
 - initiele doopgebeurtenis (dit kind het “Aristoteles”)
 - ketting van overleveringen
 - “Aristoteles” verwijst via de ketting naar het kind
 - Ook al is alles wat we van Aristoteles weten, niet waar, het blijft Aristoteles

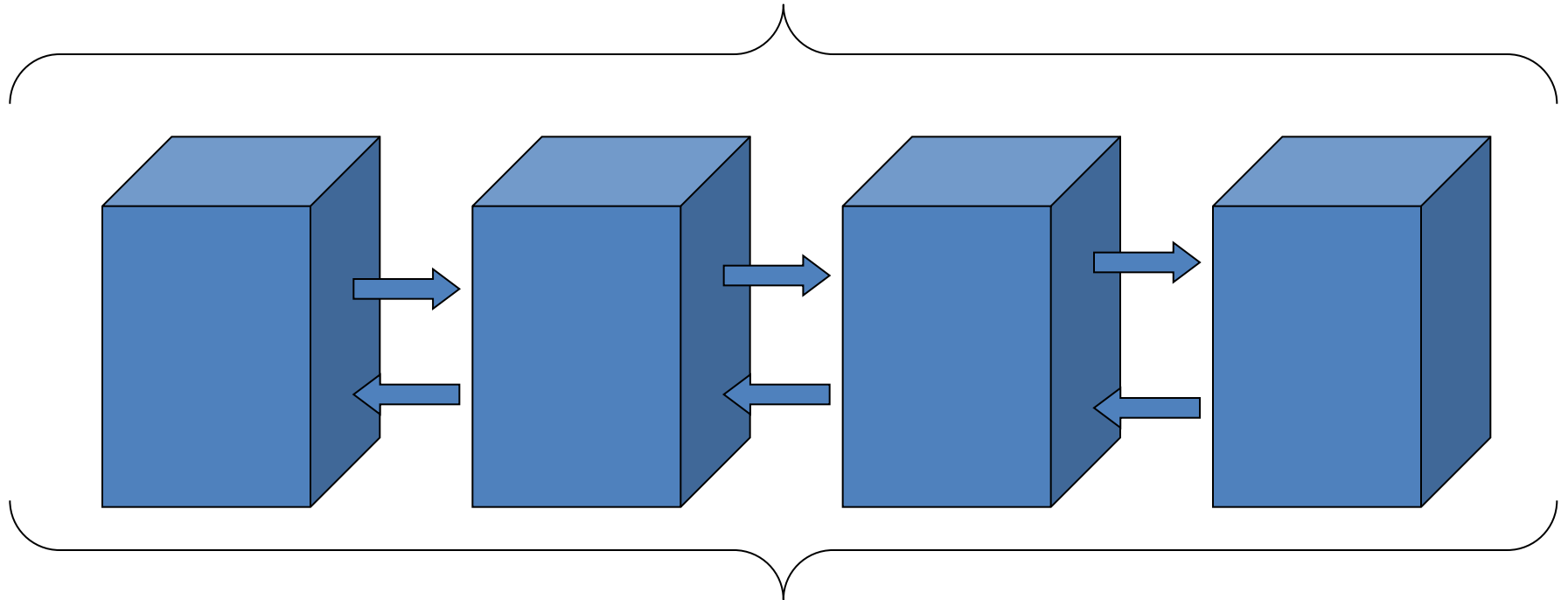
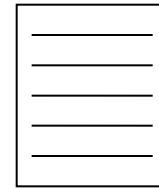
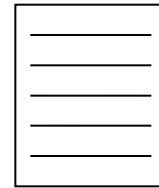
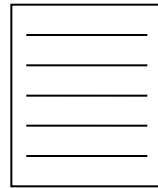
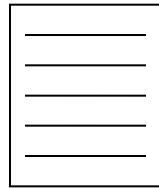
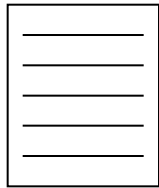
Identiteit en ICT

Echte wereld

ICT



Betekenis in de keten



Identiteit en ICT

- Gaan de documenten die we uitwisselen over dezelfde dingen?
- Data definities
- Identifiers:
 - Records, primary keys
 - Repositories / registries
 - GUID, UUID, OID
 - URI's
 - PKI, Authenticatie
- Identifiers:
 - identiteit van individuals en typen
 - lokaal uniek of globaal uniek

Registries / repositories

- Gemeentelijke BasisAdministratie
Persoonsgegevens
- Nieuwe Handelsregister
- Basis Gebouwen Registratie
- Basisregistratie Kadaster
- Basisregistratie Topografie
- Basis Registratie Adressen
- ... steeds meer

Identifiers in ICT: lokaal

```
<Object>
  <gwb:ID>obj01</gwb:ID>
  <gwb:Rijbewijs>
    <gwb:RijbevoegdheidcategorieCode>B</gwb:RijbevoegdheidcategorieCode>
    <gwb:NummerID>0123456789</gwb:NummerID>
    <gwb:EinddatumGeldigheid>2012-12-12</gwb:EinddatumGeldigheid>
    <gwb:AutoriteitAfgifte>Burgemeester van Groningen</gwb:AutoriteitAfgifte>
    <gwb:EigenaarPartijreferentie><gwb:ID>p01</gwb:ID></gwb:EigenaarPartijreferentie>
  </gwb:Rijbewijs>
</Object>
```

- ePV
- rijbewijs
- lokaal uniek

Globaal unieke identifiers

- contextonafhankelijk
- rijbewijs-id \neq paspoort-id \neq patient-id
- geen conflict mogelijk tussen id's uit verschillende bronnen
 - patient-id uit Waterlandziekenhuis en Elisabethziekenhuis

Identifiers in ICT: OID

- HL7v3 BSN:
 - `<id extension="100197231" root="2.16.840.1.113883.2.4.6.3" assigningAuthorityName="BSN"/>`
- OID: 2.16.840.1.113883.2.4.6.3
 - OID is wereldwijd uniek identificerend
 - deze OID identificeert het BSN nummer
 - OID's zijn hiërarchisch
 - onderdeel ITU-T ASN.1 standaard
 - extension bevat de echte BSN

Identifiers in ICT: UUID

- UUID: Universally Unique Identifier
- 128-bit nummer (32 hex digits)
- b.v.: 550e8400-e29b-41d4-a716-446655440000
- $3.4 * 10^{38}$ UUID's
- algoritme zorgt ervoor dat kans op dubbele UUID's (nagenoeg) nul is
- geen centrale autoriteit
- maar: betekenisloze nummers

Identifiers in ICT: URI

- URI: Uniform Resource Identifier
 - makkelijk verkrijgbaar
 - beter leesbaar dan OID of UUID
 - kan iets retourneren
- <http://www.overheid.nl/bsn/123456789>
- <http://www.marcdegraauw.com/persoon>
- o.a. Dublin Core, RDF, OWL, Topic Maps

Identifiers in ICT: URI

- RDF, OWL
- URI: Uniform Resource Identifier
 - Webarch: By design a URI identifies one resource. We do not limit the scope of what might be a *resource*.
 - RFC 2396: A resource can be anything that has identity... Not all resources are network "retrievable"; e.g., human beings, corporations, and bound books in a library can also be considered resources.
- Resource (b.v. “nu”) ≠ Representation (“2007-10-22 22:45”)

HttpRange-14

- Norman Walsh: “... some folks think `http://example.org/some/path` *must* identify “a document” (what the [AWWW](#) calls an “[information resource](#)”) and some folks think it can identify anything at all.”
- 200 OK: an information resource
- 303 See Other: some resource
- 404 Not Found: the nature of the resource is unclear

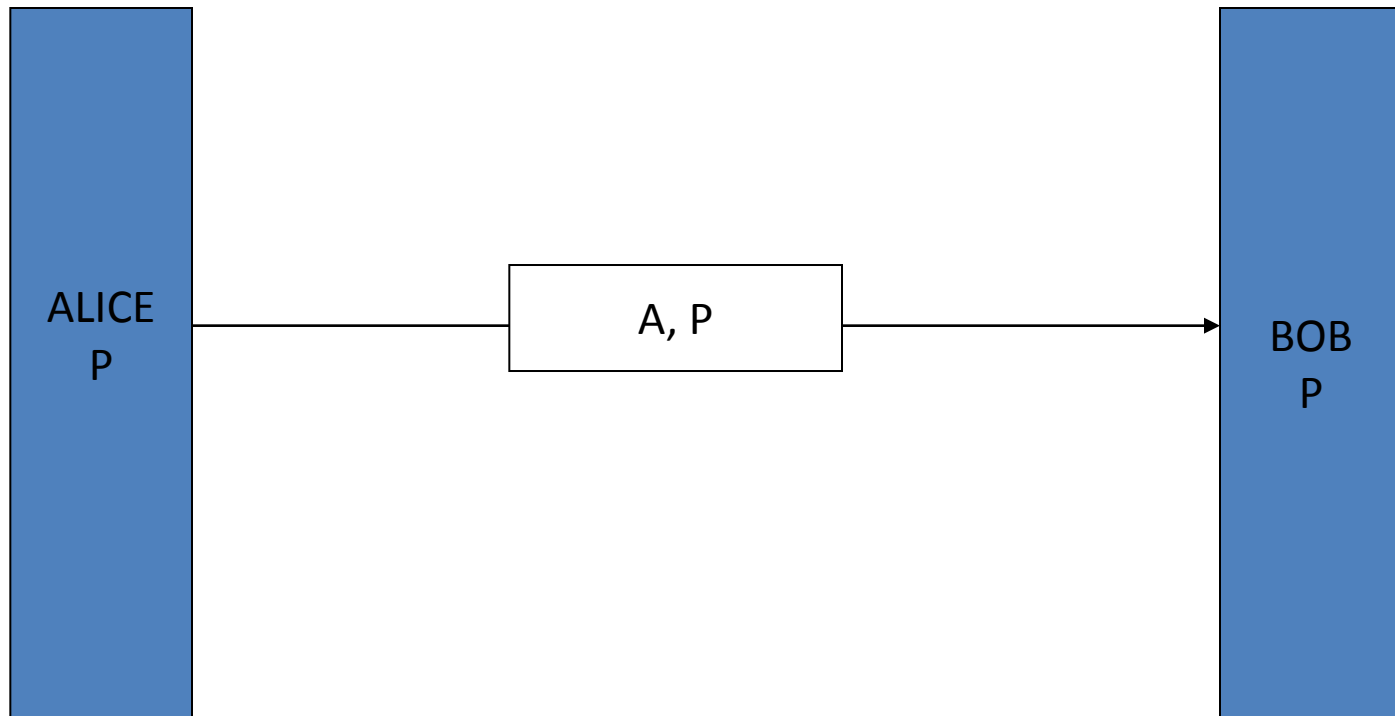
Identifiers in ICT: URI

- Topic Maps
 - [http://en.wikipedia.org/wiki/Praying Mantis](http://en.wikipedia.org/wiki/Praying_Mantis)
 - subject indicator: a web page about a single subject
 - subject identifier: a URI used as to identify a topic
 - addressable subject: [<resourceRef>](#)
 - non-addressable subject: [<subjectIndicatorRef>](#)

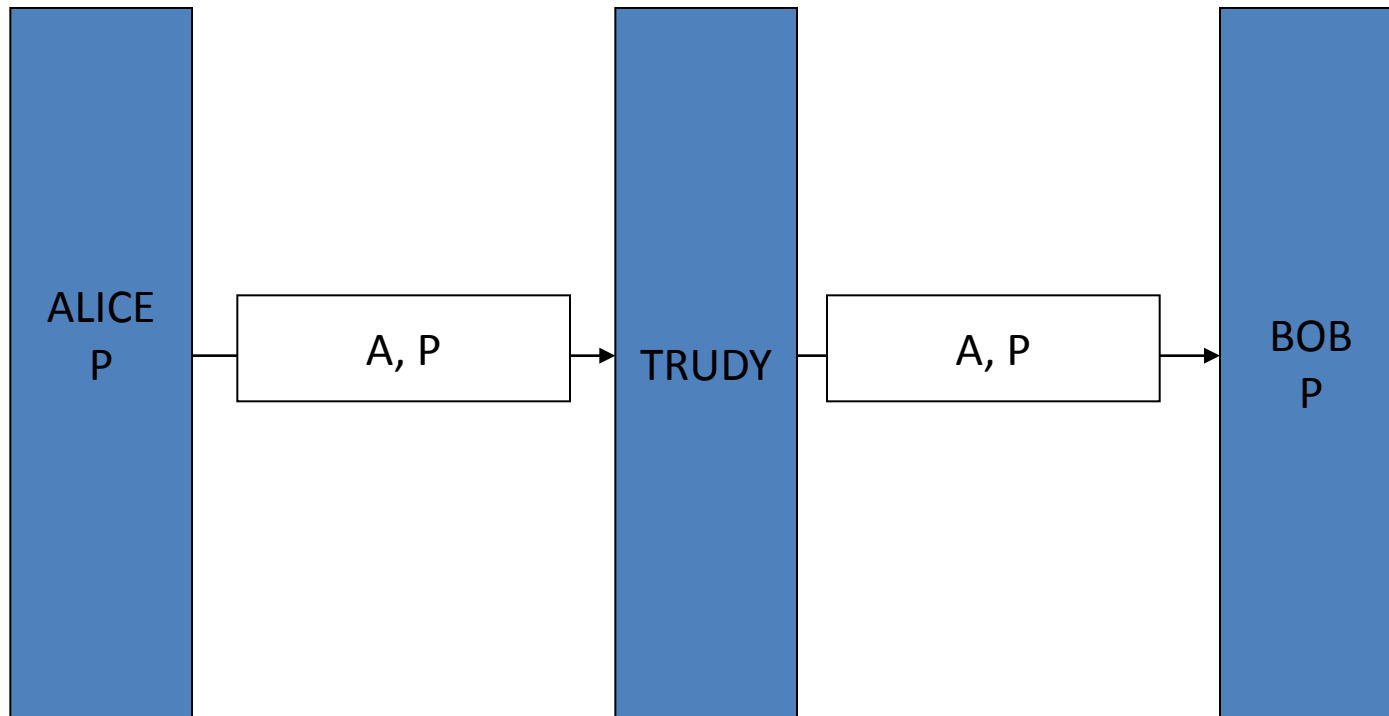
Authenticatie

- Authenticatie
 - username / password
 - shared key
 - private / public key

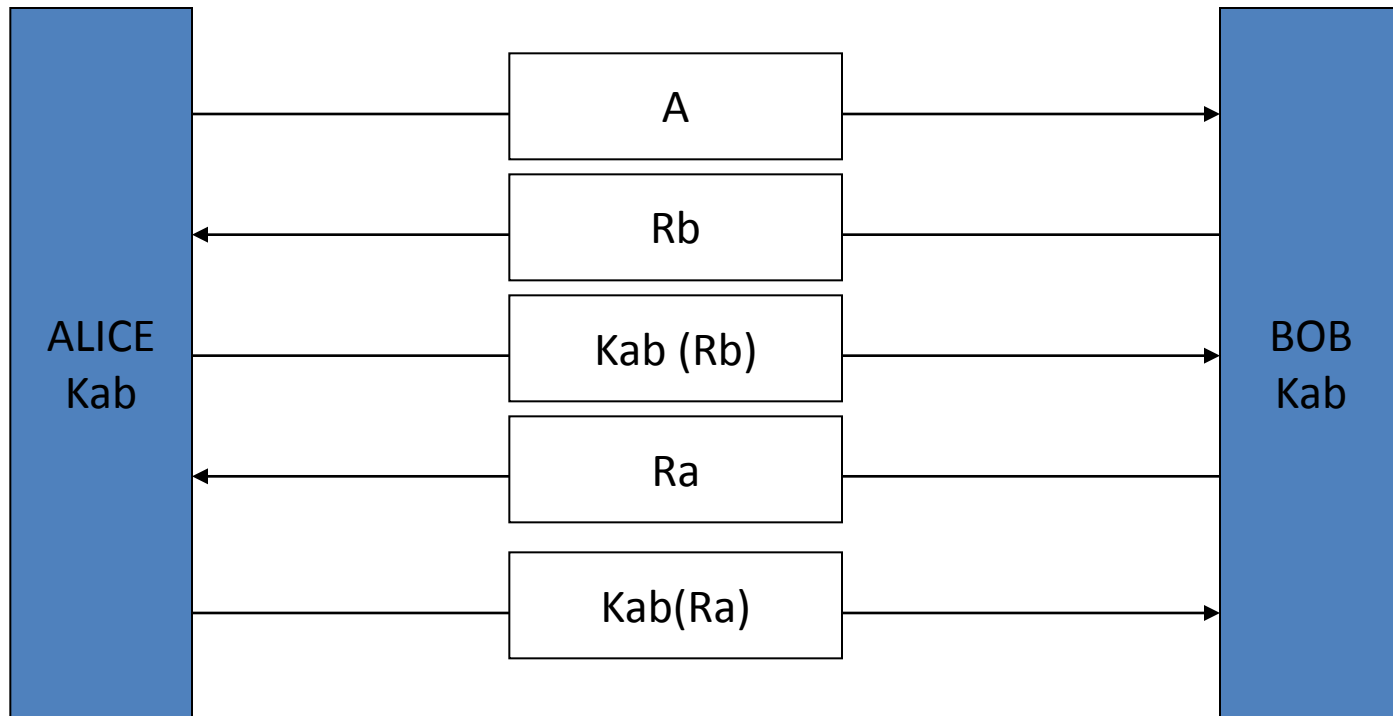
Authenticatie: Username/password



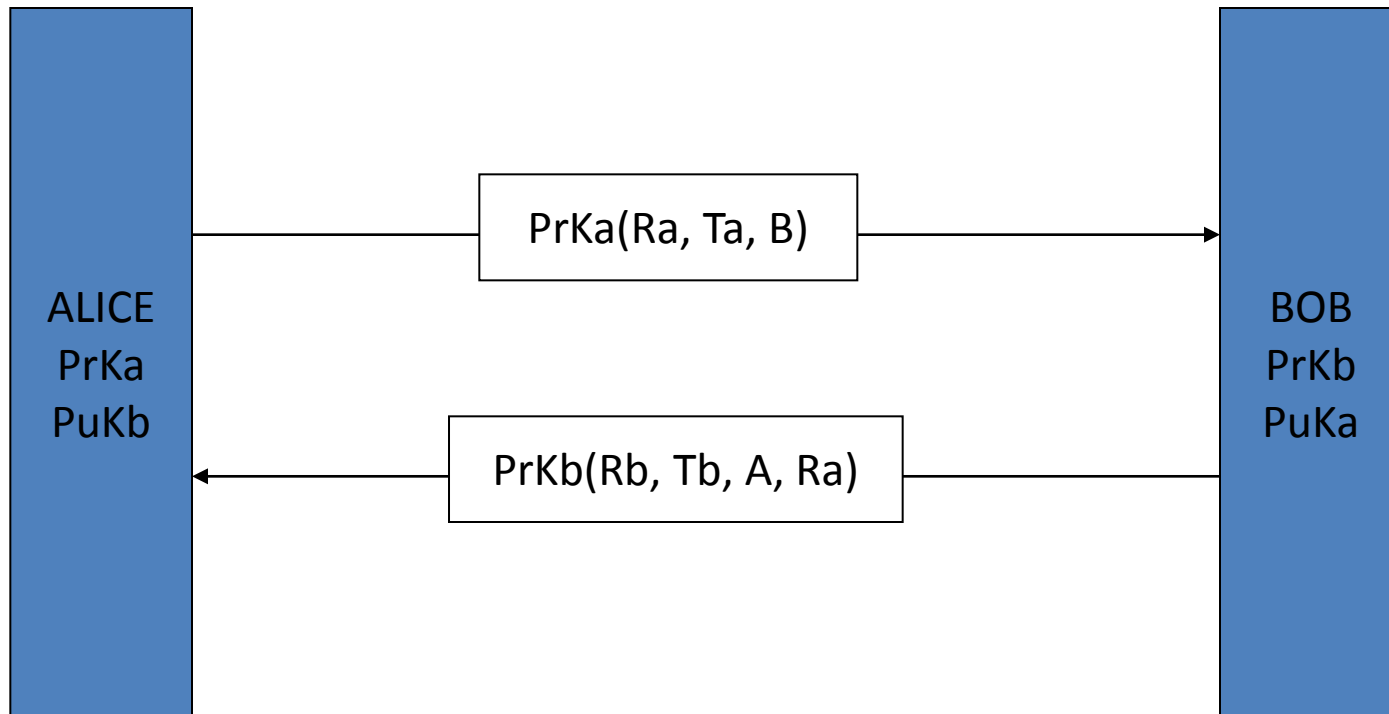
Authenticatie: Username/password



Authenticatie: Challenge-Response Shared Key



Authenticatie: PKI



Authenticatie Zorg

- Landelijk EPD
- Burger
 - BSN
 - BSN registry: opvragen bsn, naw
 - pas of rijbewijs aan balie
- Zorgverlener
 - UZI pas
 - X.509 certificaat
 - PKI-Overheid



Certificaat



Certificaatinformatie

Uitgegeven aan:

Titel	Arts verstandelijk gehandicapten
Naam (CN)	Piet Testzörgverlener2
Organisatie (O)	Piet Testzörgverlener2
Land (C)	NL
Serienummer	000000505

Uitgeversinformatie:

Naam (CN)	TEST UZI-register Zorgverlener CA
Organisatie (O)	agentschap Centraal Informatiepunt Beroepen Gezondheidszorg
Land (C)	NL
Serienummer	00:9E:E9:9B:43:83:B7:95:03:CA:3B:CC:83:98:FC:81:27

Geldigheid:

Geldig van	2005-10-03 10:40:17
Geldig tot	2008-10-02 10:40:17

Dit certificaat is bedoeld om:

Verifiëren van digitale handtekeningen voor onweerlegbaarheid

Kenmerken:

SHA1 Kenmerk	F4:35:DA:69:5C:F5:01:4B:1D:7E:3A:9C:5A:62:E8:9C:2D:75:26:ED
MD5 Kenmerk	51:1D:D5:37:C4:9C:39:BE:02:B0:AA:BF:61:E2:07:CE

Opslaan...

Sluiten

Conclusies

- het is al 2000 jaar niet makkelijk
- intensie = gegevensdefinitie ...
- rigide designator = uuid/oid/uri/cert ...
- denk goed na
- overweeg globale i.t.t. lokale identifiers