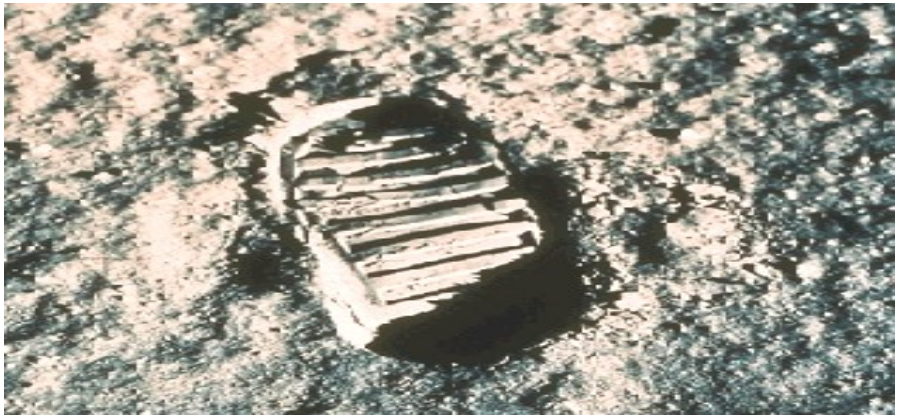
Privatsphäre, Datensicherheit & Überwachung

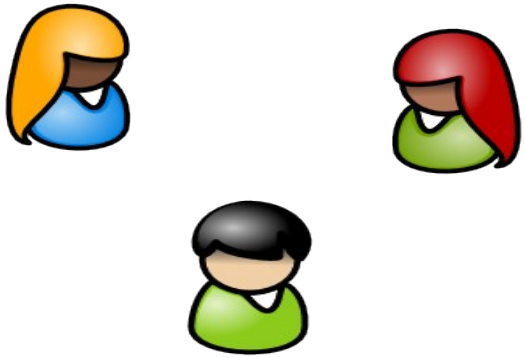
Dr. Jan Camenisch
Projektleiter Security & Privacy
Member, IBM Academy of Technology


Houston, we
have a problem!

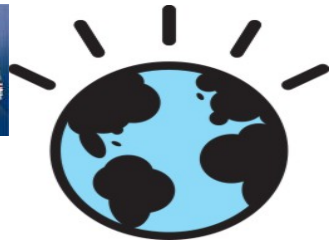

“Neil Armstrongs Fussabdrücke sind noch immer dort oben”
(Robin Wilton, Gartner)

Computer vergessen nicht!





- Speicherplatz immer billiger
- Einfach zu kopieren und zu verbreiten
- Datenverarbeitung immer besser
- Datenauswertung unvorhersehbar
- Zunehmende Digitalisierung



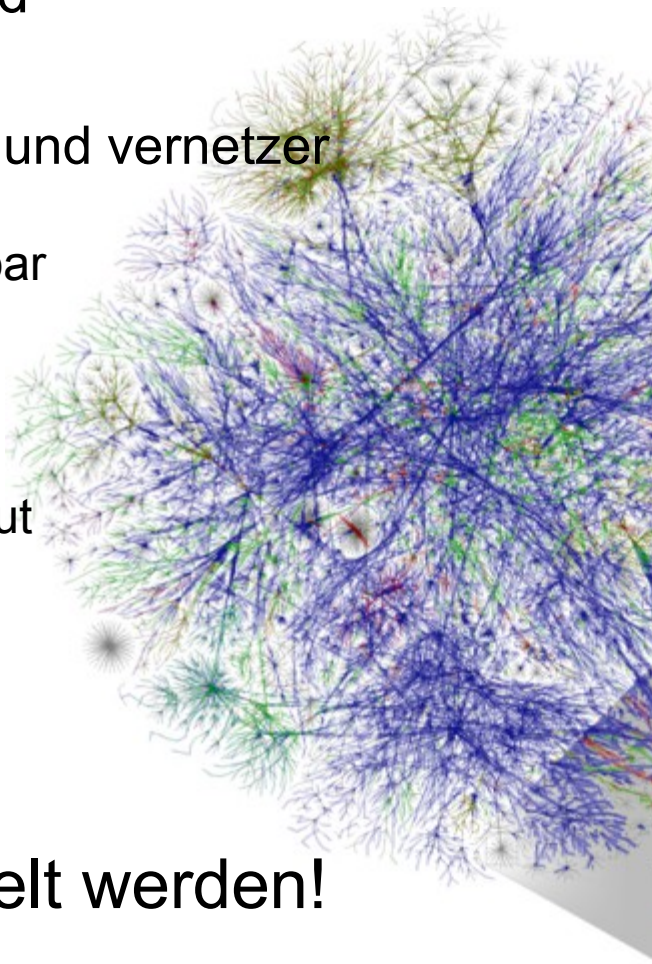
→ elektronische Daten/Welt ≠ Papier-Welt/Daten

Wo sind meine Daten?

Sehr schwierig nachzuvollziehen wo Daten sind

- Geräte, Betriebsysteme, Apps werden komplexer und vernetzer
  - Mashups, Ad networks
  - Nicht sichtbar, für Fachleute kaum noch überschaubar
  - Verarbeitungsprozesse ändern sich im nachhinein

- Netzwerke und Systeme schlecht geschützt
  - Systeme werden “mit der Papierwelt im Kopf” gebaut
  - Wer verschlüsselt schon? Sicherheit kommt zuletzt
  - Jeder kann Apps entwickeln und verkaufen



→ Daten können viel zu leicht gesammelt werden!

You have no privacy, get over it .....?!?

- Riesiges Sicherheitsproblem!
  - Millionen geknackte Passwörter (100'000 followers $115 - 2013)
  - Verlorene Kreditkartennummern ($5 - 2013)
  - Gestohlene Identitäten ($150 - 2005, $15 - 2009, $5 – 2013)

- Schaden schwierig abzuschätzen
  - Kreditkartenbetrug
  - Spam & Marketing
  - Manipulierte Aktienkurse, Zinszätze

- Wenn Geheimdienste so einfach können, können's Kriminelle auch
  - Es geht nicht um zielgerichtete Beobachtung
  - Klar gibt es Grenzen bis zu welchem Grad mach sich schützen kann

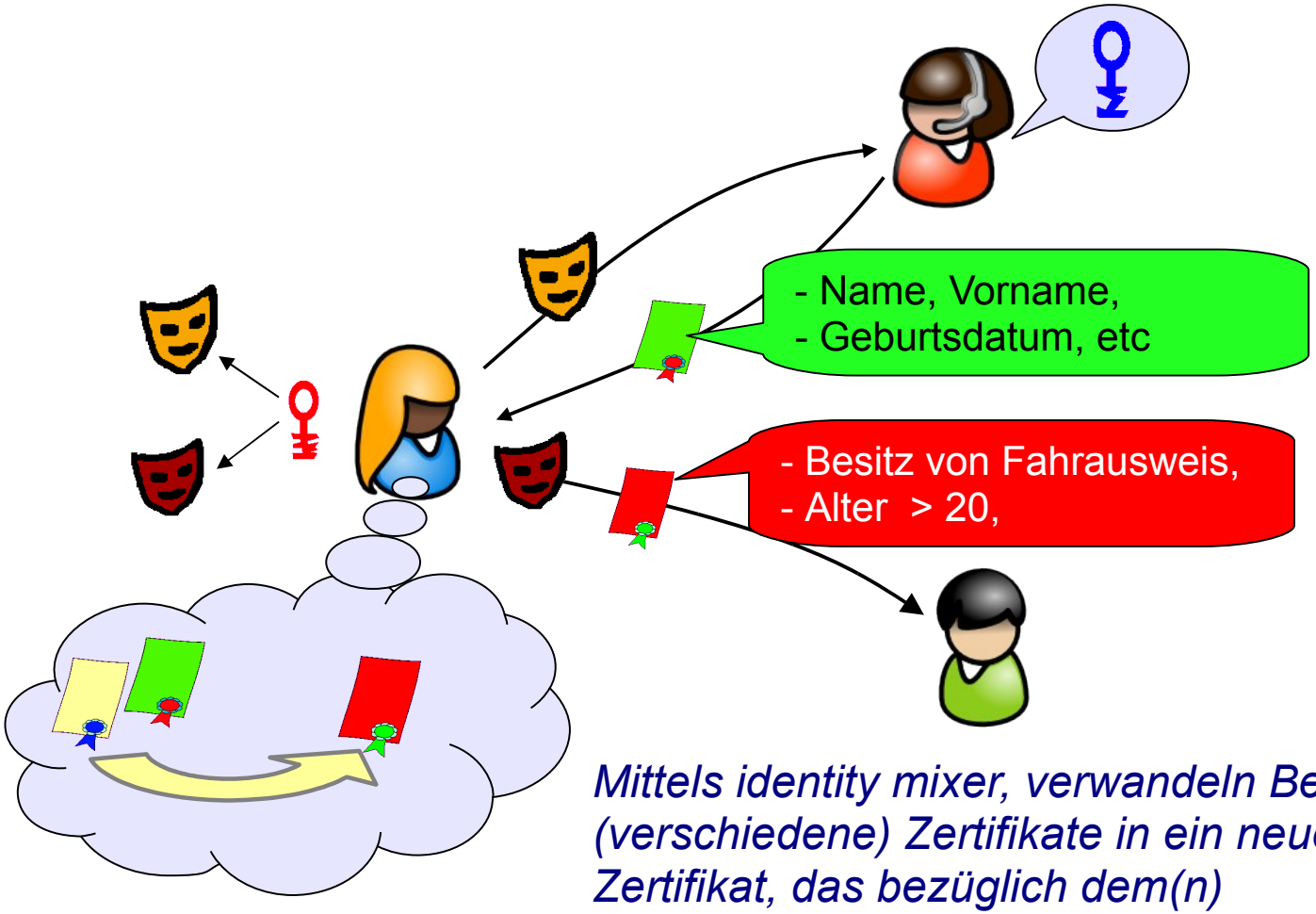
- sozialer Schaden ausser acht (Demokratie, Wahlen,...)

- zuletzt: private Daten sind das neue Geld!

→ Apps und Infrastruktur: Privacy by Design!

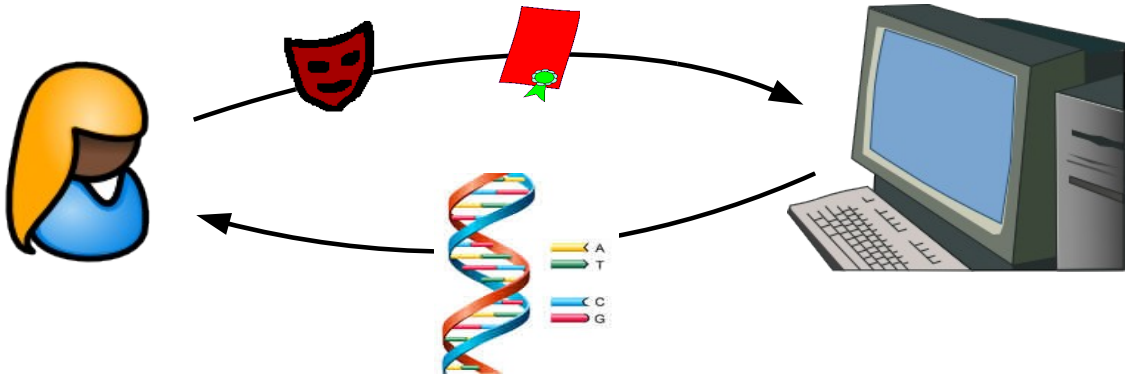
Beispiel: Private Zertifikate zur Authentisierung

(anonymous credentials, attribute based credentials)



Mittels identity mixer, verwandeln Benutzer (verschiedene) Zertifikate in ein neues Zertifikat, das bezüglich dem(n) Signierschlüssel(n) gültig bleibt.

Beispiel: Datenschutzfreundliche Zugriffskontrolle



DNA Datenbank

Einfacher Fall: Datenbank lernt nicht wer zugreift

Besser: Versteckter Zugriff (OT with AC)

- Datenbank lernt nicht *wer* zugreift
- DB lernt nicht auf *welche* Daten zugeriffen werden
- Dennoch kann Alice nur auf Daten zugreifen für welche sie *authorisiert* ist

Besten Dank!

- eMail: jca@zurich.ibm.com
- Links:
  - www.abc4trust.eu, www.futureID.eu, www.fiware.eu
  - www.PrimeLife.eu
  - idemix.wordpress.com
  - www.zurich.ibm.com/idemix