Outline

Plan

Non-digital situation

DigiD

e-Identity requirements

Towards discussion

Plan for today

Players

- Two people on stage: Bart Jacobs and Jaap Akkermans
  - but one-way communication is not intended!
  - BJ and JA only prepare the grounds
- Hopefully, you as audience take an active role in the discussion!

Topic: e-Identity

- What roles can/should public and private parties play?
- BJ looks at data management issues
- JA looks at economic issues

Background

Context

- NL government wants to upgrade the strength of citizen authentication (currently weak, with DigiD)
- This is a clear struggle, with many competing interests
Traditionally...

- Citizen registrations emerged in continental Europe in Napoleon’s time, primarily for military draft.
  - These registrations are now basis for citizen rights and obligations.
- Anglo-Saxon countries lack centralised citizen administrations.
  - E.g., in US: few people have passports; state-issued driver’s license most used; no reliable carrier for social security number.
- In NL there is BRP (= GBA + RNI) as citizen administration, with national registration number BSN = Burger Service Nummer.
  - BSN is basis for all communication with public authorities (also with education and health sector).
  - BSN is also basis for exchanges between such organisations.

Source identity

Public authorities are traditional providers of the source identity for their citizens.
- Typically as passports, national identity cards, or uittreksel geboorteregister.
- Other identities (bank cards, SIM cards, etc) are derived from it.

High-level view of DigiD

- DigiD is national authentication service for NL public sector.
  - Emphasis on ease-of-use, not on security — now problematic.
  - Widely used (compared to other countries) and successful.
- DigiD works via redirects to the authentication server, returning signed messages of the form:
  “With certainty level X the authenticating person has BSN Y”
- Privacy concerns:
  - Authentication server is a hotspot, knows where you are going (hospital, donor-register, police, social security etc.)
  - All your actions can be traced and connected, via BSN.
- This tracing is not seen as big problem, since it all happens within the public sector.
  - Primarily used for fraud-detection, no commercial exploitation.

Towards an e-Identity

- A public strong authentication solution could be a smart card with BSN (and PKI support).
  - Usage would be restricted to the public sector.
  - Strong authentication is also desirable in the private sector.
- Usage in both public and private sector imposes tough privacy requirements.
  - No traceability, excluding single hubs (like in DigiD).
  - No linkability, excluding single identifiers like BSN, or public keys (in PKI).
- There are strong commercial incentives to make all activities traceable and linkable.
  - Counterbalance is needed.
Contextual authentication

If broad usage, both public and private, is required for an e-Identity system, then it should provide:

- unlinkable, contextual authentication

Two most common solutions

- **pseudonyms**, depending on user and service provider (like in the German identity card nPA)
- **Attributes**, providing selective disclosure and proportional authentication (like in the IRMA project)

Information flow perspective: some bold points

- Information flows determine power relations in modern societies
  - authentication is the basis for informational control
- Authentication mechanisms determine the societal power balance
- Public authorities should empower their citizens, not the information giants

Therefore public authorities must

- extend their role as provider of a citizen source identities into the digital domain
- enforce/introduce mechanisms for contextual authentication