Public and Private Roles in a National e-Identity Infrastructure

PI.lab yearly event

Bart Jacobs
bart@cs.ru.nl
12 dec. 2014

Outline

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
- Anglosaxon countries lack centralised citizen administrations
  - Eg. 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 in it.

Should the public authorities also be responsible for a *digital* source identity?

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 succesful
- 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

Therefor public authorities must

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