About Self-Sovereignty

PI.lab yearly meeting
Dec. 14, 2018

Bart Jacobs — Radboud University
bart@cs.ru.nl

Outline

About Self-Sovereignty

Where we are, so far

Self-Sovereignty or *Self-Sovereign Identity* (SSI)

- The phrase self-sovereign idenity (SSI) came out of the blockchain community in the 2010s
  - hence somewhat anarchistic and anti-authoritarian undertone
  - strong emphasis on taking back control — after apparent loss
  - influenced by European refugee crisis with many people lacking a (state) recognised identity
- SSI is not well-defined: tech people trying to be philosophers
- e.g. Paul Allen in *Ten Principles of Self-Sovereign Identity* (2016)
  - copied from Kim Cameron's *The Laws of Identity* (2005, Microsoft)
  - things like: "the user is the ultimate authority on their identity"
- In NL "SSI" is used by the Dutch Blockchain coalition
  - in their vision document: "A self-sovereign identity (SSI) is the driving force for a supple interaction in the online economy with a direct impact on the physical world"
  - much of such bla-bla, but no description of SSI

Common elements of SSI

(1) Technological / cryptographical basis
- decentralised blockchain technology for independent persistence
- public key crypto and sometimes also zero-knowledge proofs

(2) The individual him/her-self is the basis for an (electronic) identity
- strong contrast: "national registration destroys that sovereignty"

(3) SSI technology allows people to make claims
- alternative terminology: people can disclose attributes
- these claims/attributes are (cryptographically) verifiable

(4) Much emphasis on user control, access, consent, minimisation, portability
- "the rights of users must be protected!"
- strong GDPR flavour

Blockchain as a SSI-basis I

Recall, the essence of blockchains:

(1) permanent, immutable storage of data, in a "ledger"
- the ledger is public, in principle, and accessible by everyone

(2) No central authority, but distributed guarantees arise
- certainty about what which data was added at what stage

(3) Game-theoretic acceptance of data in the blockchain (ledger)
- some non-sensical riddle needs to be solved
- winner is rewarded
- enormous waste of resources (esp. energy)

Blockchain technology is the underlying mechanism of bitcoins, which became an independent hype. Hundreds of versions now exist.

Blockchain as a SSI-basis II

What to put on the blockchain for identity? Plans vary wildly.
- identity data themselves (claims/attributes) — confidentiality problem
- public keys of people — traceability problem
- hashes of something — same problem

Fundamental show-stopper problem
- All of the above ideas involve storing personal data on a blockchain
- but blockchain data are permanent, and cannot be removed
- this is inconsistent with GDPR's data subject rights of removal

Blockchain as a SSI-basis III

Reactions to the inconsistency between GDPR and "SSI on blockchain"

(1) Switch from public to non-public "permissioned" blockchains
- this undermines the original transparancy goals of the SSI-community
- also: why not use traditional databases then?

(2) Some are even asking for amendments in the GDPR to allow for blockchains
- argument: GPDR is based on the idea of centralised databases
- surrealistic route; better amend your technology

(3) Final retreat: put only public meta-data ("the scheme of claims") on a blockchain
- sure, but why not use simply (one or more) webpages?
- implicit admittance: blockchains were bad idea in the first place

The individual is the basis of SSI

- What does this mean? Self-asserted claims!
  - such claims can be endorsed by other people: "yes, she lives here"
  - ideas going back to early web-of-trust in PKI
  - nice & sympathetic ideas, but they never got off the ground
- People, certainly in continental Europe, see the government as the primary source of (administrative) identities
- Historical detail: Napoleon started registering people's identities
  - he needed these registers to draft people into his huge armies
  - this never happened in Anglo-Saxon countries — which typically have no citizen administration

XKCD intermezzo

What remains of SSI? Data autonomy!

- We have seen: blockchain-basis and self-asserted claims are not very succesful ideas in SSI
  - (after 2 years, blockchain coalition is still stuck on identity)
- What remains of SSI is a high level of user access & control
  - not a new idea of course; but it is taken to a next level
  - I'll use the phrase data autonomy here
- The NL government now also has such a programme Regie op Gegevens
  - it hasn't delivered anything, except paper
  - centralised organisations with big databases don't like this
- Sometimes the discussion gets confused when people start talking about data ownership — in phrases like: "control over *your* data"
  - not very helpful concept, since ownership is often not defined
  - e.g. in NL, neither doctor nor patient owns medical data; they both have rights and obligations (under the WGBO)

Where we are, so far

What is Payment Service Directive (PSD) 2?

- EU directive, in force since 2018 — since 2019 in NL
- It is meant to help the fintech industry by forcing traditional banks to open up their systems — in order to increase competition
  - both for data and transactions
  - banks cannot charge anything for such forced access
- Two new services are foreseen, in practice via third party apps
  (1) "payment initiation services", for new payment mechanisms
  (2) "account information services", for bank-account-info usage
- People need to give explicit consent for access to their bank account
  - this may involve third party data, but it cannot be processed
- "Data autonomy" is part of the PSD2 story line

Own publications about PSD2

(1) **Blog at iBestuur**, sept. 2017
- title: PSD2, a European strategic blunder (in Dutch)
- main point: not fintechs will profit, but US big-IT
- EU should have required reciprocal openness of social media companies, instead of just giving away bank-data-assets for free
- individuals are only weakened *vis à vis* IT-giants
- this blog started / altered the debate in NL

(2) **Publications in law**, 2018 & 2019, with Pieter Wolters
- first in Dutch: *De toegang tot betaalrekeningen onder PSD2*, Ondernemingsrecht.
- then in English: *The security of access to accounts under the PSD2*, Computer Law & Security Review.
- **Main point**: development of the market for payment services has a higher priority than security and privacy

Data autonomy perspective on PSD2

- Appealing motivation: give people more control over their own financial data
  - e.g. collect data from several bank accounts in one app
  - and obtain financial advice from several sources
- **Fundamental question:** will this empower people or weaken them?
- Problematic scenario's; realistic? Abuse of power?
  - you want a mortgage offer? Open your account first!
  - you want an ESTA US-visa waiver? Open your account!
  - you want a new phone subscription? Rent an appartment?

  Credit rating will explode with PSD2, also in Europe.
- Will the GDPR be sufficiently protective?
  - maybe more importantly: will regulators be sufficently active?

Big question

Will more data autonomy make people less autonomous?

Concerns
- IT-giants benefit from individualisation of everything — esp. of consent — and use it for (commercial/political) manipulation
- Who is really being empowered here? How naive are we?
- We are fragmenting the world outside IT-monopolists ...
- and at the same time helping them to become even more dominant

Where we are, so far

Recent data vault initiative in Dutch Parliament

- MPs Kees Verhoeven (D66) and Jan Middendorp (VVD) wrote "initiatiefnota" that was adopted in dec'18
- It asks for one online identity and a personal data vault for each citizen
- About this online identity
  - to be used for authentication to government and for contact
  - and for access to the personal data vault
  - this identity should be regulated by law
- Goals of the proposed personal data vault
  - provide transparancy & control over one's data (*regie*)
  - allow citizens to correct (government) data about them
  - one-source idea: all data exchanges happen via this vault
- "*Met die online identiteit kunnen mensen de controle terugpakken over hun identiteit en persoons-gegevens bij de digitale overheid.*"

Questions wrt. these MP-plans

- What is "one online identity"?
  - a government-provided email address? What about spam?
  - are "polymorphic pseudonyms" an answer? Could work, for authentication
- Secure online contact requires a new communication infrastructure
  - encrypted & authenticated email? Or something else?
- More fundamentally, about the data vault, what if:
  - Google etc. start luring/pressurising people to consent to giving access to the vault, for new, fancy, cool "services"?
  - China demands access to e.g. your medical dossier for visa
- These access abuse issues are not addressed at all
  - rather naive thinking
  - some level of enlightened patronising is needed, to protect people

Protection of citizens?

- Who will protect the "data-autonomous", "empowered" citizen?
- The new vault initiative does not address this matter at all!

What can be done? (difficult)

(1) legal protection: e.g. via increased duty of care (zorgplicht) requirements for parties that access the data vault?
  - just "consent" doesn't work and is too weak
  - forbid *webscraping*, as now practised by uwkluis.nl

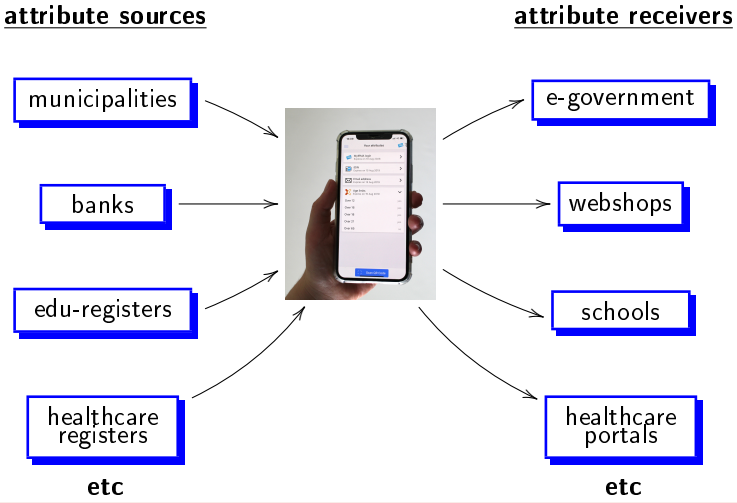
(2) organisational protection: e.g. buddy-approval for sensitive data?

(3) technical protection:
  - temporary disable mode, e.g. when travelling to certain countries
  - require certificate (with conditions) for API-access

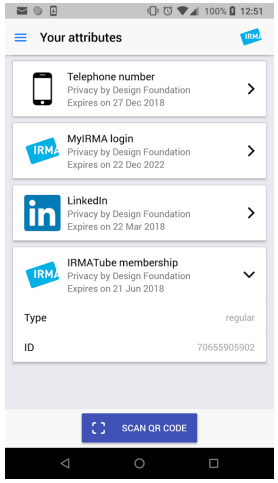
(4) alternatives: ???

Where we are, so far

The IRMA app as everyone's personal hub



IRMA basics: reveal only relevant attributes



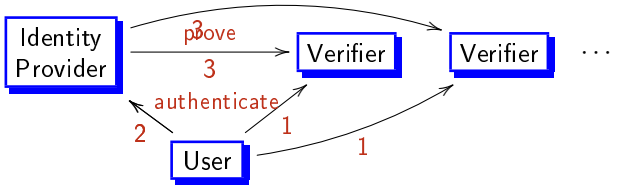
Authentication essentials:

- attributes instead of identities
- collected by user him/herself
- attributes are reliable (digitally signed by source)
- IRMA is free & open source
- decentralised architecture: attributes only on users own phone

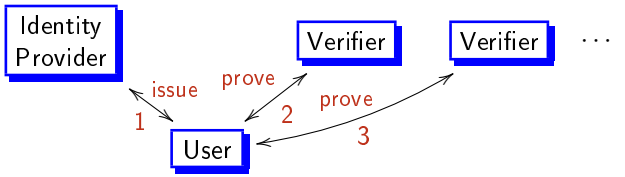
Demo?

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (think iDIN/FB)



Decentralised: everyting goes via the User (think IRMA)



IRMA & SSI

- IRMA involves decentralised storage of attributes, in the user's phone only, with strong cryptographic guarantees
  - it uses zero-knowledge proofs, but no blockchains
- IRMA is a tool for data autonomy: user access & control, transparancy, data minimisation
- But no self-asserted identities with web-of-trust endorsements
- Instead, the foundation behind IRMA is in (cryptographic) control
  - IRMA attributes come from "trusted" sources / registers
  - these attribute-issuing parties need a certificate, for app-access
  - attributes in the app are digitally signed by these sources
  - hence verifiers can cryptographically check the integrity & authenticity (source) of attributes (claims)

IRMA & data autonomy criticism

- The same criticism of data autonomy applies to IRMA
  - giving the individual full control over data invites abuse
- Indeed, this worry is real and appropriate
  - e.g. within the ministery of the interior (BZK)
  - but also within the IRMA team
- but IRMA is only a mini-vault and stands out in some ways:
  - authentication attributes are "small pieces of personal data", very different from e.g. large medical files
  - data obtained from IRMA are "worthless", since not-signed
  - each attribute-request is visible to the user and must be endorsed
  - over-asking violates GDPR's data minimisation — visibly so
  - it is technically possbile (but not implemented yet) to restrict access to sensitive attributes, via a certificate + usage contract

Where we are, so far

Concluding remarks

- Self-sovereign identity (SSI) in the wake of the blockchain hype
  - several aspects of it don't really work, e.g.
  - blockchain storage, self-asserted group-endorsed identities
- SSI did give new momemtum to "data autonomy"
  - giving individuals far-reachting control over "their" data
  - represented as a "return of control", almost Brexit-style
- Predictable power-shift between individuals and IT-giants is ignored
  - giving people more choice mostly empowers the big players
  - very uncomfortable message, to which there is no good solution
- The current data autonomy *discour* is on the wrong track
  - it's about empowering but ignores unpowering
  - it's overly optimistic about personal autonomy
  - we need to organise proper guarantees and counter power to prevent abuse of inidividuals with extensive access.
- There's too much naivety about personal data vaults, as with PSD2!